Exploring the Criticality of TARGET2: A Socio-Technical Analysis of Its Role in the Economic Security of the Netherlands

Exploring the Criticality of TARGET2: A Socio-Technical Analysis of Its Role in the Economic Security of the Netherlands

By

Anurag Arora

in partial fulfilment of the requirements for the degree of

Master of Science

in Management of Technology

at the Delft University of Technology,

to be defended publicly on February 15th, 2024.

Thesis Committee:	
First Supervisor:	Prof. Dr Cees van Beers -ETI
Second Supervisor:	Prof. Dr Pieter van Gelder - SSS
Advisor:	Dr Caetano Penna - ETI

An electronic version of this thesis is available at http://repository.tudelft.nl/.

Acknowledgements

I would like to extend my deepest gratitude to a number of individuals whose support and guidance have been invaluable throughout the journey of completing my master's thesis.

First and foremost, I am immensely thankful to my supervisors, Prof Dr Cees van Beers and Prof Dr Pieter van Gelder, for their unwavering support, insightful feedback, and expert guidance. Their expertise and encouragement have been crucial in navigating the challenges of my research. Their dedication to excellence and commitment to fostering a supportive and intellectually stimulating environment have greatly contributed to my personal and academic growth.

I am also profoundly grateful to my advisor, Dr Caetano Penna whose wisdom and mentorship have been indispensable. Dr Penna's perspectives and advice have been a guiding light, helping me refine my ideas and approach my work with rigor and creativity. Dr Penna's patience and understanding have made a significant impact on my journey, and I am truly appreciative of his involvement in my project.

To my mom, dad, and Harshit, your unwavering belief in me and endless love have been the cornerstone of my journey. Your ability to listen, offer wisdom, and provide encouragement during my moments of doubt has been nothing short of remarkable. Your constant support and sacrifices have been my guiding light, infusing me with the strength and confidence needed to pursue my ambitions relentlessly. Thank you for being there through every challenge and triumph, for your unconditional love, and for always believing in my potential with unwavering faith.

I want to express my heartfelt thanks to my girlfriend, Durga, for her love, understanding, and patience. Your encouragement, thoughtful advice, and constant presence have been a beacon of light during the most challenging times. Thank you for standing by me, for celebrating the milestones, and for being my pillar of support.

To my friends Rishabh, Saket, Yash, Divyanshu and Pragalbha thank you for being my support system and for the countless moments of relief and laughter amidst the pressures of research. Your friendship and unwavering support have been a source of joy and comfort, reminding me of the importance of balance and well-being.

A special shoutout to my Spartan Workout group and the SRM Group (Divyajeet, Avi, Shubhang, Tyagi, Usama, Himanshu) for their camaraderie and the unique ways in which they've contributed to my journey. The Spartan Workout sessions provided not only a physical outlet but also mental resilience, teaching me the value of discipline and perseverance. The SRM Group, with its enduring friendship and collective wisdom, has been a constant source of motivation and inspiration. Together, you all have made this journey more memorable and enjoyable, and I am deeply grateful for each one of you.

This thesis would not have been possible without the collective support and encouragement of each one of you. I am deeply grateful for your contributions to my academic journey and personal growth. Thank you all for being part of this journey with me.

Executive Summary

This thesis presents a detailed examination of the role of technology in enhancing economic security, with a specific focus on the Target2 financial transaction system's contribution to the economic stability of the Netherlands. By broadening the traditional scope of national security to include economic stability, environmental sustainability, and technological advancements, this study sets a new context for understanding economic security as a critical component of national well-being.

Focusing on financial technologies, the study examines how the efficiency and security of systems like Target2 can significantly impact a nation's economic stability. Target2 is selected as a prime example of a real-time gross settlement (RTGS) system that is crucial for executing high-value transactions, underlining its significance in the financial infrastructure.

By adopting the socio-technical systems theory, the thesis provides a nuanced analysis that captures both the technical and social dimensions of Target2. This approach facilitates a balanced discussion on the system's components and their implications for economic security.

In addressing the identified gaps within the current academic discourse, this thesis highlights the underutilization of a socio-technical perspective in analysing critical financial systems, the uncertainties surrounding risk pathways, and the absence of framework that effectively link technological systems with economic security.

The report provides detailed cataloguing of Target2's infrastructure, classifying its components into technical and social categories in line with the socio-technical systems theory. This classification differentiates between the system's technical elements, such as interfaces, core platforms, networks, applications, and databases, and its social elements, including governance structures, operational roles, user groups, and communication protocols.

The study outlines Target2's fundamental operations, which constitute the core processes essential for its functioning. Recognized key operations encompass transaction management, risk and compliance mechanisms, system governance, business continuity planning, and user interface administration. This detailed identification of operations serves as a vital framework for exploring the socio-technical interactions within Target2, providing a robust base for understanding the system's operational dynamics and their implications for economic security.

The research into the interplay between Target2's technical and social dimensions uncovers essential synergies critical for its seamless operation. The analysis reveals how the system's core platform reliability is paramount to user operations and how effective communication protocols are crucial for aligning governance decisions with compliance requirements across the user base. This deep dive into the socio-technical intersections of Target2 brings to light significant vulnerabilities, such as gaps in communication, network reliability issues, and gaps in risk management, all of which pose risks to the system's resilience.

Further exploration into Target2 through stakeholder mapping exposes its diversified roles, encompassing real-time settlement, liquidity management, regulatory compliance, and crisis management functionalities. This multiplicity of functions emphasizes the system's indispensable role in safeguarding financial stability. The study also assesses the impact of potential vulnerabilities on stakeholders, identifying how disruptions in settlement processes could impede liquidity flows and how security breaches could diminish trust in the system's operational integrity. This exploration affirms the necessity of addressing identified vulnerabilities to maintain the continuity of economic operations, underscoring the critical nature of Target2 within the financial ecosystem.

This research highlights the potential for identified vulnerabilities within Target2 to evolve into significant threats, including technical breakdowns that jeopardize settlement finality, cyber incidents that threaten data integrity, instances of regulatory non-compliance that introduce systemic risks, and diminishing user trust from continuous operational challenges.

Crucially, the study lays the groundwork for developing effective mitigation strategies. Recommendations include enhancing monitoring systems for the immediate detection of technical issues, establishing cross-functional teams for integrated incident management, implementing stringent access controls to fortify data security, and refining risk assessment methodologies to effectively prioritize system improvements. These strategies underscore the importance of a proactive approach to system maintenance and improvement. Through a detailed analysis of vulnerabilities and corresponding mitigation approaches, the study offers valuable insights into enhancing the robustness of Target2, shedding light on the various risk pathways that could affect economic security. These recommendations emphasize the necessity for an adaptive yet cohesive governance approach, aligning with the thesis's resultant conceptual framework.

This framework, developed from a blend of empirical data and theoretical insights, identifies four key dimensions essential to the management and understanding of Target2: Integration, Reliability, Adaptability, and Networked Value. Integration emphasizes the seamless coordination between the system's technical capabilities and its social constructs, ensuring optimal functionality. Reliability is concerned with operational metrics such as transaction accuracy and system availability, indicative of the system's stability. Adaptability pertains to Target2's ability to anticipate and adjust to emerging threats, demonstrating its dynamic nature. Networked Value highlights the system's strategic role within a globally interconnected financial network, impacting both domestic and international operations. By weaving together socio-technical insights, this framework offers a significant leap forward in the governance of essential centralized systems, with broad implications for security policymakers and financial administrators. It provides a comprehensive model for assessing systemic vulnerabilities, enabling the development of effective policy measures and strategic interventions.

The thesis acknowledges certain limitations, notably its concentrated examination of TARGET2's application within the Netherlands, which may limit the broader applicability of its findings. This focus is complemented by a reliance on official documents, potentially overlooking the nuanced, informal dynamics that also shape system governance. To mitigate these limitations, the study suggests broadening the research scope through comparative studies across multiple countries and adopting ethnographic methodologies, such as embedding within operational teams, to capture a more nuanced view of system governance. Additionally, incorporating viewpoints from outside the financial domain is recommended to challenge and expand beyond existing disciplinary perspectives.

A concrete recommendation is made to the European Central Bank Executive Board: the establishment of a Socio-Technical Integration Function within TARGET2's governance structure. This function is envisioned to foster a holistic approach to technology management, user experience optimization, and the integration of platform policies, embodying the thesis's advocacy for socio-technical cohesion as a cornerstone for resilience in critical financial infrastructure.

Ultimately, the thesis positions TARGET2 at the intersection of technology and social interaction within Europe's financial landscape, asserting that the system's economic security is fundamentally linked to the integrity of both its technical and human elements. By identifying existing coordination challenges and proposing pathways for improvement, the research sets a forward-looking agenda aimed at enhancing financial stability in an era marked by rapid digital transformation.

Contents

Chapter 1 Introduction

1.1 Background and Context

The interrelationship between technology and economic security, central to this thesis, is a multifaceted and evolving phenomenon, shaped by numerous factors and changing societal priorities. The perspectives on what constitutes critical technologies and how they influence economic security have undergone a significant transformation over the years. This thesis seeks to explore and elucidate this complex interplay.

Historically, the concept of 'critical technologies' was primarily associated with military strategic assets, particularly during wartime. This narrow conception, however, has expanded significantly to encompass a broader range of innovations. As noted by Bimber and Popper (1994), and further elaborated by Edgerton (2007), the current understanding of critical technologies includes those driving economic growth, enabling improvements in quality of life, and underpinning critical infrastructure. This expansion reflects a shift in societal values and priorities, recognizing the role of technology not just in warfare but in everyday economic and social life. However, as Clemente (2013) points out, the multidimensional nature of technology criticality presents challenges in systematically evaluating and governing today's technological landscapes.

In parallel, the concept of economic security has also evolved. Traditionally confined to the protection of territorial sovereignty, it now encompasses broader aspects such as environmental sustainability, political stability, and social welfare (Retter et al., 2020). This expansion reflects a growing recognition that threats to national security are not only military but also economic, environmental, and social. Governments worldwide, recognizing this broader scope, have adopted risk-based approaches to frame economic security around vital systems. As Luiijf et al. (2003) discuss, this critical infrastructure perspective considers threats to essential sectors, processes, and technologies as risks to national economic stability.

In the contemporary context, technologies like artificial intelligence, blockchain, and the Internet of Things are transforming operations across critical infrastructure sectors such as finance, energy, and telecommunications (Alcaraz and Zeadally, 2015). These technologies, while driving efficiency, also introduce new systemic interdependencies and vulnerabilities, the implications of which are still being understood (Fåk, 2010). This transformation underscores the need to understand the significance of these technologies for economic continuity and security.

This thesis particularly focuses on elucidating the mechanisms through which technologies confer criticality within infrastructure systems. The implementations of these technologies occur within a nexus of social relationships, regulatory demands, and organizational structures (Hanseth et al., 2004). This complexity highlights the utility of socio-technical perspectives in understanding how human and governance aspects intertwine with technical functionality (Baxter and Sommerville, 2011).

Adopting a socio-technical lens, this study aims to contribute to the economic security literature by examining critical technologies, particularly through the case of Target2. TARGET2 (Trans-European Automated Real-time Gross Settlement Express Transfer System) is a key financial infrastructure of the European Union. It is a payment system owned and operated by the Eurosystem, which comprises the European Central Bank and the national central banks of the Eurozone countries. Target2, employed for high-value bank transactions worldwide, presents an ideal example to evaluate the architectural dynamics and stakeholder relationships that manifest its significance and associated risks.

TARGET2 facilitates real-time settlement of large-value euro transactions, ensuring high-speed and efficient processing of cross-border and domestic payments in the Eurozone. This system is pivotal in

the European financial landscape, serving as a backbone for the settlement of monetary policy operations, interbank payments, and other large-value transfers critical to the stability and functioning of the European economy. Its high-volume, high-value, and real-time capabilities underscore its crucial role in maintaining the liquidity and integrity of the Eurozone banking system.

In summary, this thesis endeavors to bridge the knowledge gap in understanding the socio-technical dynamics of critical technologies and their impact on economic security. Through a detailed exploration of Target2, the study seeks to offer a comprehensive analysis that contributes to both the theoretical understanding of this complex relationship and the practical considerations for managing and regulating these technologies in the realm of national economic stability.

1.2. Research Gap

In the context of this thesis, several significant gaps in the existing literature are identified, setting the foundation for the ensuing research. These gaps, extensively explored in the literature review section 2.4, are pivotal in understanding the socio-technical aspects of financial systems and their impact on economic security.

The literature reveals a limited focus on socio-technical systems, particularly in how they influence a nation's economic security, with a notable absence of studies specific to systems like TARGET2 and their role in countries such as the Netherlands. This gap underscores a need for deeper exploration into how these systems intertwine with economic stability.

Moreover, there exists an insufficient exploration of how TARGET2 impacts economic security, particularly in areas crucial for financial stability, such as trade facilitation, liquidity management, and the transmission of monetary policy. The lack of comprehensive analysis in this domain highlights the need for a more nuanced understanding of TARGET2's role in the broader economic context.

Furthermore, the absence of well-defined, comprehensive conceptual frameworks in the literature addressing the relationship between socio-technical systems and economic security is notable. Such frameworks are essential to grasp the multifaceted nature of economic security and the critical role played by infrastructures like TARGET2.

Additionally, there is a need to clarify the mechanisms through which disruptions in critical infrastructures like TARGET2 propagate risks across interconnected systems, potentially impacting economic stability. The existing literature often lacks specificity in elucidating these pathways, making this an area ripe for detailed investigation.

These identified gaps in the literature form the bedrock of this research, guiding its focus and methodology towards addressing these underexplored areas.

1.3 Scope

This thesis adopts a structured approach to explore the relationship between critical technologies and economic security, focusing on three key dimensions: conceptual, empirical, and methodological. Each dimension plays a pivotal role in constructing a coherent analytical framework that addresses the identified research gaps.

1.4.1. Conceptual Scope

At the heart of this study is the socio-technical systems theory, which forms the conceptual backbone of the research. This theory, as detailed by Hanseth et al. (2004), emphasizes the interdependent nature of technical systems and social structures. Applying this theory enables an in-depth examination of how weaknesses in either technological components or human interactions can lead

to broader systemic disruptions. Specifically, this framework will be employed to scrutinize the manifestations of criticality in Target2, examining how governance structures, user dynamics, and the technical infrastructure interact to shape the platform's role in the economic security landscape. This conceptual focus is crucial in understanding the multifaceted nature of technology's impact on economic stability.

1.4.2. Empirical Scope

Empirically, the thesis zeroes in on Target2, a key real-time gross settlement (RTGS) system used for high-value banking transactions within the Eurozone, with a particular focus on its operation within the Dutch financial ecosystem. Target2 stands as a quintessential example of critical financial infrastructure, making it an ideal case study for this research. The empirical analysis will delve into Target2's operational functionalities, its stakeholder network, and the risk pathways that could potentially affect the Netherlands' economic security. This empirical exploration is aimed at uncovering the specific ways in which Target2 contributes to, and interacts with, the broader economic security context of the Dutch financial system.

1.4.3. Methodological Scope

Methodologically, the thesis employs a qualitative approach, primarily through document analysis and semi-structured expert interviews. This approach is designed to explore Target2's socio-technical aspects. The use of a coding framework and thematic analysis allows for a detailed dissection of Target2's components, their interactions, vulnerabilities, and the consequent economic impacts. This methodology not only supports the linkage of the conceptual framework with empirical findings but also ensures a comprehensive, multi-layered analysis of Target2. The qualitative document analysis provides a deep dive into the existing literature, official reports, and technical documents related to Target2, allowing for a rich understanding of its technical specifications, operational mechanics, and the regulatory landscape it operates within. The semi-structured expert interviews complement this by adding a layer of practical insights and firsthand experiences from those who interact with, manage, or are affected by the Target2 system. This combination of document analysis and expert interviews is crucial for uncovering nuanced details about how Target2 functions within the Dutch financial ecosystem, how it is perceived by its users and regulators, and what potential risks it poses to economic security.

Together, these methods enable linking the conceptual grounding of socio-technical theory with the empirical case analysis to construct an illuminating analytical framework. The methodological rigor applied ensures the reliability and validity of findings, facilitating a detailed examination of how Target2's socio-technical dynamics influence economic security. This thorough methodological approach aims to provide not just descriptive insights into Target2's operations but also prescriptive recommendations for enhancing economic safeguards in an increasingly technology-reliant financial landscape.

In summary, integrating the conceptual, empirical, and methodological scopes provides an aggregative scaffolding to systematically unpack Target2's socio-technical essence and its implications for Dutch economic continuity. The multi-layered analytical approach presented here forms the foundation to bridge vital gaps identified in extant literature, contributing novel insights into the nexus of critical technologies and economic security. Through this detailed exploration, the thesis aims to offer substantial contributions to both academic research and practical applications in the field of economic security and critical infrastructure management.

1.4 Research Questions

The thesis is structured around a series of research questions, each designed to probe a different facet of the TARGET2 system's role in the economic security of the Netherlands. These questions collectively aim to provide a comprehensive understanding of TARGET2, employing a socio-technical lens to examine its technical components, social interfaces, functionality, operational indicators, vulnerabilities, and interdependencies with other financial systems.

1.5.1. Main Research Question

How does the TARGET2 system contribute to the economic security of the Netherlands from a socio-technical perspective?

Relevance: This primary question encapsulates the core investigative focus of the thesis. It resonates with the perspectives highlighted in literature on critical infrastructures and national security (Luiijf et al., 2003). By employing socio-technical theory, as advocated by Geels (2004), this question aims to elucidate Target2's role within the Dutch economic landscape, exploring the intricate interplay between its technical and social dynamics. This approach meets the objective of uncovering the complex mechanisms through which Target2 underscores economic stability.

1.5.2. Sub Research Question 1

What are the key technical components and social interfaces of the TARGET2 system?

Relevance: This foundational question aims to map Target2's architecture, aligning with the socio-technical paradigm mentioned in literature (Sonv & Naik, 2020). Understanding these components and interfaces is crucial for applying the socio-technical perspective to enhance the comprehension of critical systems.

1.5.3. Sub Research Question 2

How does the socio-technical interplay within the TARGET2 system contribute to its functionality and operation?

Relevance: Investigating the socio-technical interplay within Target2 provides valuable insights into its operations. This directly addresses the knowledge gap regarding critical technology manifestations highlighted in existing research (Hanseth et al., 2004).

1.5.4. Sub Research Question 3

What operational indicators can be used to define and measure economic security in the context of the TARGET2 system?

Relevance: Conceptualizing economic security is a crucial step for assessing Target2's influence. Literature suggests that developing a measurable understanding of economic security is important for examining the impacts of technology on a nation's economic well-being (Alcaraz & Zeadally, 2015). This question seeks to identify and define operational indicators that can effectively measure the impact of the TARGET2 system on the economic security of the Netherlands, thereby enabling a more quantitative and objective assessment of its influence.

1.5.5. Sub Research Question 4

What potential vulnerabilities within the TARGET2 system could impact its operation and overall economic stability?

Relevance: Identifying and understanding vulnerabilities within TARGET2 aligns with the broader goal in critical infrastructure literature of assessing points of weakness that could undermine system functioning (Rinaldi et al., 2001). By mapping these vulnerabilities, this research question aims to

reveal potential risk pathways within Target2, providing insights into how such weaknesses could lead to economic impacts. This exploration is key to developing strategies for risk mitigation and enhancing the resilience of the system.

1.5.6. Sub Research Question 5

How does the TARGET2 system's interdependency with other financial systems factor into its impact on the larger financial ecosystem?

Relevance: This question is pivotal in understanding how TARGET2, as a critical component of the financial infrastructure, interacts with and influences the broader financial ecosystem. The rationale for exploring this interdependency is to gauge the extent of TARGET2's impact on other financial systems and the overall financial stability of the Netherlands. This approach is informed by the recognition that financial systems are not isolated entities but are part of a complex network where the functioning of one system can have significant ripple effects on others.

Studying these interdependencies is crucial for several reasons. Firstly, it helps in identifying how TARGET2's operational dynamics and potential disruptions could affect other financial institutions and processes, which is vital for understanding its systemic importance. Secondly, this analysis contributes to a more comprehensive assessment of the overall resilience and vulnerability of the financial sector to technological disruptions or failures within TARGET2. Lastly, by understanding these interconnections, policymakers and financial regulators can better anticipate and manage systemic risks, ensuring the robustness and reliability of the financial infrastructure.

This exploration, therefore, goes beyond the operational aspects of TARGET2, delving into its role as an integral part of the financial network. It aims to provide insights into how changes or challenges within TARGET2 reverberate throughout the financial system, potentially impacting the economic security and stability of the country. Through this analysis, the thesis aims to contribute to a deeper understanding of the interconnected nature of financial systems and the critical role played by technologies like TARGET2 in maintaining the health and stability of the broader financial ecosystem.

1.5 Research Objectives

The research objectives of this thesis are anchored on three interconnected aims, each designed to advance the understanding of Target2's role in economic security. These objectives are critical for constructing a comprehensive analytical model that addresses the complex socio-technical nature of Target2 and its implications for the Dutch financial ecosystem.

1.5.1 Elucidate Target2's Socio-Technical Essence

The first objective is to methodically delineate Target2's components and interfaces, thereby revealing its architecture through a socio-technical lens, as conceptualized by Trist (1981). This involves a detailed categorization of its technical building blocks, such as infrastructure, algorithms, and communication protocols. In parallel, the research will examine the social facets of Target2, including regulatory governance, organizational cultures, and user engagement models, as discussed by Panourgias (2015). The aim is to comprehensively map the symbiosis between Target2's infrastructure capabilities and the human/institutional relationships, providing a foundational understanding of its socio-technical dynamics.

1.5.2 Conceptualize Economic Security Specific to Target2

The second objective focuses on conceptualizing the notion of Dutch economic security, particularly in relation to the risks and resilience of its payment infrastructure as manifested through Target2. This

involves deriving precise operational indicators that reflect the system's critical role in upholding broader financial stability. The conceptualization will be anchored in identifying measurable proxies for risks associated with settling transactions, maintaining liquidity, and ensuring data integrity, as suggested by Alcaraz & Zeadally (2015). This objective aims to render the concept of economic security actionable and specific to the context of Target2.

1.5.3. Analyze Vulnerabilities and Propagation Mechanisms

The third objective leverages the socio-technical mapping of Target2 to systematically identify and trace vulnerabilities arising from weaknesses in its human, procedural, and technical configurations. Drawing on perspectives from literature on common financial infrastructure risks, including work by Cai et al. (2018), this analysis will explore probabilistic pathways of disruption. These pathways include operational bottlenecks, cyber risks, regulatory gaps, and challenges associated with technology transitions. By thoroughly analyzing these vulnerabilities, the research aims to elucidate potential disruptions and their propagation mechanisms that could compromise economic continuity. This objective is crucial for understanding how different types of risks can emanate from or impact Target2, affecting the larger financial ecosystem and, consequently, the economic security of the Netherlands.

The analysis will involve a detailed examination of the points of intersection between Target2's technical and social components and how these intersections might serve as potential vectors for risk propagation. Factors such as the integration of new technologies, the adaptation of regulatory frameworks, and the evolution of user behavior will be considered to understand how they might introduce new vulnerabilities or exacerbate existing ones. This objective goes beyond identifying risks, aiming to map out how these risks could cascade through the financial system, causing broader economic impacts.

1.5.4 Unifying Purpose of the Objectives

The unifying purpose across these detailed objectives is to develop a conceptual framework that captures the intricate socio-technical essence of the TARGET2 system and its role in economic security. This framework is envisioned to provide a comprehensive understanding of TARGET2's operation within the Dutch financial ecosystem, its interdependencies with other financial systems, and its criticality in maintaining economic stability.

The development of this framework involves a synthesis of the socio-technical aspects of TARGET2, the operational indicators of economic security relevant to the system, and an in-depth analysis of its vulnerabilities and potential risk propagation mechanisms. The aim is to construct a model that not only sheds light on the complexities of managing critical financial infrastructures like TARGET2 but also offers actionable insights for enhancing their resilience and reliability.

This conceptual framework is intended to contribute significantly to both academic research and practical applications in the field of financial infrastructure management and economic security. By bridging theoretical perspectives with empirical findings, the framework will serve as a valuable tool for policymakers, regulators, and financial industry stakeholders. It will aid in informed decision-making, guiding strategies to fortify economic safeguards in a financial landscape that is increasingly interlinked and reliant on sophisticated technologies.

1.6 Structure of the Thesis

The thesis is structured across six chapters, each playing a distinct role in unraveling the socio-technical aspects of Target2 and its impact on economic security. The structure is designed to systematically guide the reader through the research process, from foundational concepts to detailed analysis and practical implications.

Chapter 1: Introduction

This chapter sets the stage for the research by presenting the background and context of the study. It identifies the gaps in existing research and outlines the scope and objectives that frame the research impetus, focusing on Target2's significance for economic security in the Netherlands. The introduction provides a clear roadmap for the investigation, establishing the relevance and importance of the study.

Chapter 2: Literature Review

The literature review chapter synthesizes key perspectives from academic discourse that are central to situating this study. It covers a range of topics, including the various definitions of economic security, frameworks for understanding critical technology, and the foundational principles of socio-technical theory. This review establishes the theoretical backdrop against which the empirical study is conducted and contextualizes the research within the broader academic field.

Chapter 3: Research Methodology

In this chapter, the methodological approaches and analytical procedures employed in the study are detailed. It describes the qualitative document analysis and expert interviews that drive the investigation of Target2. The methodology chapter is crucial for understanding how data was collected, analyzed, and interpreted, providing transparency and validity to the research findings.

Chapter 4: Target2 Socio-Technical Analysis

This chapter presents the comprehensive findings from the document analysis, utilizing the frameworks and coding tools proposed earlier. It reveals Target2's socio-technical essence, including its components, interfaces, vulnerabilities, and the impacts these have on economic security. This chapter is pivotal in providing a detailed analysis of Target2's role within the Dutch financial ecosystem.

Chapter 5: Results Validation

The fifth chapter encompasses insights derived from expert interviews to validate the findings obtained from document analysis. It focuses on confirming Target2's critical functioning and identifying potential risks and vulnerabilities that could affect economic continuity. This validation step is crucial for ensuring the reliability and accuracy of the research conclusions.

Chapter 6: Conclusion

The final chapter consolidates the identified dimensions into an integrated conceptual framework. It outlines potential applications of the research findings to policy interventions and strategies aimed at actively safeguarding economic robustness. The conclusion also reflects on the implications of the study for future research and practice in the field of economic security and critical infrastructure management.

Through this structured approach, which bridges theory, empirical analysis, and practical application, the thesis crystallizes the significance of Target2's socio-technical dynamics in reinforcing resilience within the Dutch economic landscape. The structure ensures a comprehensive and coherent exploration of the research questions and objectives, providing a clear pathway through the complex interplay of technology, finance, and economic security.

Each chapter builds upon the previous, creating a cumulative understanding of the subject matter. The initial chapters lay the theoretical and methodological groundwork, enabling a deep dive into the socio-technical analysis of Target2 in subsequent chapters. The results validation chapter ensures the robustness and reliability of the findings, while the concluding chapter weaves together the various threads of the research to present a unified and actionable framework.

Overall, this structured progression of chapters is designed to facilitate a clear, logical, and thorough understanding of the research topic for readers, whether they are academicians, industry professionals, or policymakers. The thesis aims not only to contribute to academic knowledge but also to offer practical insights and recommendations that can inform policy and decision-making in the realm of financial infrastructure and economic security.

Chapter 2 Literature Review

This section initiates the literature review by first establishing a foundational understanding of economic security, a prerequisite for appreciating the role of technology in national development. The review commences by proposing a consensus definition of economic security, setting the stage for an in-depth analysis of 'critical technology.' A significant focus is given to TARGET2, identifying, and justifying its classification as a critical technology within the Dutch context.

The literature review then examines the interplay between critical technology and economic security, underscoring the significance of critical infrastructure in maintaining a nation's economic stability. Using the Netherlands as a case study, this section explores how technology, particularly when embedded in critical infrastructure, becomes essential for economic security.

Furthermore, the review introduces the socio-technical systems framework as a theoretical lens for guiding subsequent research in this domain. Figure 2-1 visually represents the process and structure of the literature review undertaken in this thesis.

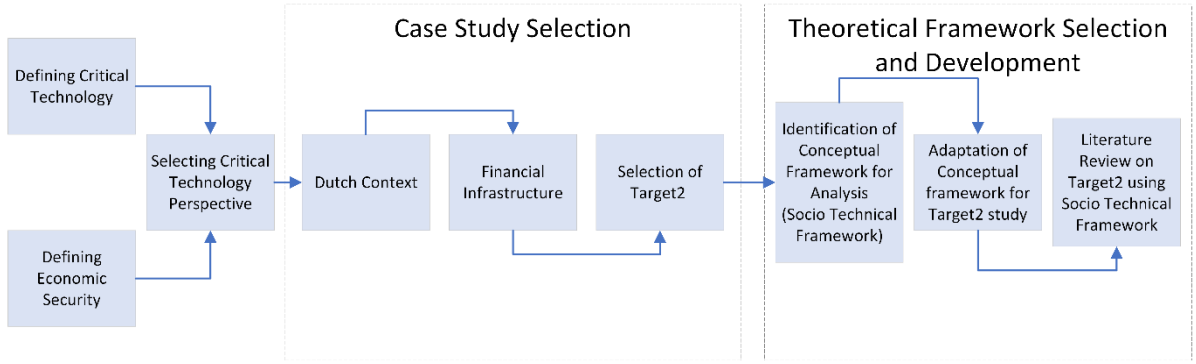

Figure 2-1 Literature Review Flow

2.1 Economic Security

2.1.1 Defining Economic Security

The concept of economic security is inherently complex, characterized by its multi-dimensional nature, conceptual ambiguity, and subjectivity. Influenced by evolving socio-economic contexts, cultural differences, and varying policy and political perspectives, its definition and implications vary globally. Additionally, economic security is interconnected with other forms of security, such as national and environmental security (Newman, 2005). Key factors shaping economic security, which are not mutually exclusive, include employment, income, job quality, health, retirement, housing, food, and financial inclusion. Thus, economic security can be viewed through multiple lenses, dependent on context, scale, and the perspective of those seeking to achieve it.

As we expand our focus, it becomes evident that the concept of national security has evolved significantly over the past century. Historically centered on military threats, it now encompasses a wider range of dimensions, including environmental security, economic security, and social stability/cohesion (Retter et al., 2020). This expansion reflects the growing recognition of the complex and interconnected nature of threats faced by nations, which are unique and prioritized based on each nation's risk assessment processes. In this expanded view, economic security emerges as a critical aspect of national security, underscoring the importance of safeguarding a nation's economic well-being against various types of threats.

Contemporary definitions of national security, as presented in policy and academic literature, often take two distinct approaches. The narrow approach focuses on territorial integrity and sovereignty, while the broader approach, which is our focus, includes economic, environmental, and social well-being, as well as international system developments (Retter et al., 2020). This broader perspective aligns with our understanding of economic security at the national level.

At this macro level, economic security encompasses elements like economic stability (Blanchard et al., 2010), resilience to economic shocks (Hallegatte et al., 2017), trade security (Evenett and Hoekman, 2004), environmental sustainability (Boyce, 2019), and technological capability (Archibugi and Pietrobelli, 2003). It also involves ensuring education and skills (Hanushek and Woessmann, 2008), robust infrastructure (Calderón and Servén, 2010), social cohesion (Putman, 2000), political stability (Alesina et al., 1996), good governance (Kaufmann et al., 1999), inclusive growth (Berg and Ostry, 2011), and sustainable development (WCED, 1987). The cooperative pursuit of economic security, as exemplified by the European Union (Cable, 1995), highlights the interdependence among nations in achieving these goals.

Thus, while our discussion of economic security has considered various individual and societal aspects, the current focus on economic security within the national security framework becomes increasingly vital. We define economic security as the safeguarding of essential physical and virtual systems and assets critical for the functioning of a nation's economy. This includes protecting technological assets like data networks, digital infrastructure, intellectual property, and software systems. This definition situates economic security firmly within the broader context of national security, reflecting its importance in maintaining the stability and resilience of a nation in a rapidly evolving global landscape.

2.1.2 Economic security at the national level

In the context of the nation-state, economic security is a component of larger goal of achieving national security. The concept of national security has transmuted over the past century from consideration of military threats as part of security to including other dimensions such as environmental security, economic security, social stability/cohesion. Every nation prescribes to its own definition of national security, based on their understanding of it, and each nation's security interests are a function of their national risk assessment processes (Retter et al., 2020). Threats faced by a nation are singular to itself, and its security interests are prioritised accordingly. Thus, whether a nation pursues narrow or broad focus of national security depends upon historical trends and current developments, and "national security policy encompasses the decisions and actions deemed imperative to protect domestic core values from external threats" (Leffler, 1990, 143).

Contemporary definitions of national security are often presented in two distinct ways in policy and academic literature. The first approach defines national security in a narrow sense, with a focus on protecting the state's territorial boundaries and sovereignty. This can closely relate to neorealism's tendency to argue that the nation-state remains the principal agent in security in terms of accountability, "despite the advancement of globalization and the proliferation of transnational threats and actors" (Fjäder, 2016, 35). The second approach adopts a broader perspective, which includes factors such as economic, environmental, and social well-being, as well as developments in the international system (Retter et al., 2020). The second approach is of interest in this literature review.

Economic security at the national level includes several macroeconomic-focused elements: economic stability (Blanchard et al., 2010), resilience to shock (Hallegatte et al., 2017), trade security (Evenett and Hoekman, 2004), environmental sustainability (Boyce, 2019), technological capability (Archibugi

and Pietrobelli, 2003), education and skills (Hanushek and Woessmann, 2008), infrastructure (Calderón and Servén, 2010), social cohesion (Putman, 2000), political stability (Alesina et al., 1996), good governance (Kaufmann et al., 1999), inclusive growth (Berg and Ostry, 2011). and long-term economic security dependant on sustainable development (WCED, 1987). Over time there have been calls for a cooperative rather than confrontational pursuit of economic security, a shared goal between states (Cable, 1995), with the project of the EU a key example of this interdependence.

We have defined economic security as safeguarding vital physical and virtual systems and assets that are essential for the functioning of a nation and its economy. Within this definition, economic security also relates to protecting technological assets, including data networks, digital infrastructure, intellectual property and software systems.

2.1.3 Role of technology in economic security

The interrelationship between technology and economic security is intricate, shaped by numerous factors, including how technology evolves within society and its impact on economic structures. To understand this complex dynamic, several theoretical frameworks are useful. Technological determinism (Wyatt, 2008; Drew, 2016) suggests that technological development drives social and economic changes. In contrast, social constructivism (Law and Singleton, 2000; Lynch, 2016) posits that societal factors influence the development and use of technology. Actor-network theory (Hanseth, Aanestad and Berg, 2004) offers a more integrated perspective, viewing technological and social factors as interdependent and mutually influential. These theories provide a foundational understanding of how technology not only shapes but is shaped by economic and societal contexts, which is critical for comprehending its role in economic security.

Historical examples illustrate these theories in action. The advent of the steam engine and mechanized textile production, pivotal during the Industrial Revolution, can be viewed through the lens of technological determinism, where technological innovation directly spurred economic growth (Mokyr, 1990). The 20th century saw further technological milestones like electricity, automobiles, and telecommunications, each playing a determinative role in economic progress. The Information Technology Revolution in the late 20th century, as analysed through social constructivism, highlights how societal needs and structures influenced the development and integration of new technologies into the economy (Brynjolfsson and McAfee, 2014). These technological shifts have fundamentally transformed business models, industries, and lifestyles, demonstrating the intertwined nature of technological and economic evolution.

In the 21st century, the role of technology in economic security has intensified due to the rapid evolution of technological capabilities and their integration into vital sectors. Advancements such as artificial intelligence, big data analytics, and the Internet of Things (IoT) have revolutionized the operational frameworks of critical infrastructures, including energy grids, transportation systems, and financial networks. These technological integrations have enhanced efficiency and connectivity but have also introduced new vulnerabilities. Cybersecurity threats, for instance, pose significant risks to these critical infrastructures, making the protection of digital systems a paramount concern for economic security. The impact of automation, driven by advanced robotics and machine learning, is transforming industries, necessitating a re-evaluation of workforce strategies and economic policies.

Moreover, the digital divide accentuates inequalities in access to technology and economic opportunities, particularly in the utilization and management of critical infrastructure. These

challenges, illuminated by actor-network theory, demonstrate the intricate relationship between technological advancements and economic security. They highlight how technological developments are shaping the resilience and vulnerability of national economies.

Understanding the implications of these technological changes for economic security is crucial, particularly in the context of critical infrastructure. The dependence of essential services on digital technologies means that any disruption, whether due to cyberattacks, technological failures, or inadequate adaptation to new technologies, can have far-reaching economic consequences. Therefore, research into economic security must consider the multifaceted impacts of technology on critical infrastructure, examining both the opportunities for advancement and the challenges of safeguarding these vital systems. This exploration is key to developing strategies that not only leverage technological innovations for economic growth but also mitigate the risks they pose to the stability and security of national economies.

Therefore, maintaining uninterrupted technological operations within essential infrastructure systems, especially in the digital age, is a key aspect of economic security (Tsvetkov et al., 2019). This necessity underscores the importance of technology in national economic security as highlighted by Brynjolfsson and McAfee (2014). The following sections will delve into why technology is crucial for economic security, examining specific technologies that are integral to critical infrastructure and processes. This examination will further elucidate the multifaceted relationship between technology and economic security, showcasing how contemporary technological challenges and opportunities shape and are shaped by economic imperatives.

2.1.4 The Dutch context

In exploring the role of technology in economic security, the Netherlands presents a compelling and relevant case study. The Dutch approach to national security, especially in integrating and safeguarding critical components, offers a distinctive perspective that is particularly instructive. About two decades ago, the Netherlands embarked on a comprehensive critical infrastructure plan. This initiative demonstrates the Netherlands' commitment to understanding and protecting the interdependencies within critical sectors that are fundamental to national security, such as finance, ICT, and energy (Tkachenko et al., 2019).

In 2002, the Dutch government initiated the critical infrastructure protection project ‘Bescherming Vitale Infrastructuur’. The project's objective was to develop a cohesive set of measures for safeguarding the infrastructure of both government and industry, with a special focus on Information and Communication Technology (Luiijf et al., 2003). As part of their national security strategy, the Dutch government identified six vital interests (Clingendael & KPMG, 2019):

- Territorial Security - Protecting borders.

- Physical Security - Safeguarding citizens and infrastructure.

- Economic Security - Ensuring the stability of trade, commerce, and industry.

- Ecological Security - Preserving the environment.

- Social and Political Stability - Upholding fundamental values and rights like the rule of law, democracy, and privacy.

- Functioning of International Rule-Based Order - Maintaining global governance institutions, upholding international law, and safeguarding human rights.

Within this strategic framework, the Dutch national security strategy identifies four critical processes in the financial sector (Retter et al., 2000): retail transactions, consumer financial transactions, high-value transactions between banks, and securities trading. The focus of this study is on high-value transactions between banks due to their significant economic impact.

The selection of the Dutch context for this research is motivated by several factors. The Netherlands' methodical approach to integrating technology within its critical infrastructures, particularly in pivotal sectors like finance and ICT, provides a nuanced perspective for understanding the role of technology in economic security. This approach, characterized by its attention to both technological advancements and comprehensive security strategies, is highly relevant to our investigation into the intricate relationship between technology, critical infrastructure, and economic security. Analyzing the Dutch experience allows this research to draw valuable insights applicable to broader discussions on economic security in the context of a rapidly evolving digital landscape. This choice thus effectively connects with the earlier discussions on the pivotal role of technology in economic security and the critical need to protect infrastructure against contemporary threats.

2.2 Critical Technology/infrastructure

2.2.1 Understanding criticality

Criticality in technology is a multifaceted and context-specific concept. Historically, the term 'critical technologies' was used during the early industrial era, primarily referring to key industrial technologies that drove economic growth and development (Mokyr, 1990). In more recent times, this term has expanded to encompass a broader range of technologies, such as biotechnology and big data (Edgerton, 2007; Brynjolfsson and McAfee, 2014). Today, technologies are deemed critical not just for their economic benefits but also for their impact on various aspects of economic security, including competitiveness, innovation capacity, environmental sustainability, public health, and social well-being (Mazzucato, 2018).

From a strategic perspective, the criticality of technologies remains consistent with their historical role; they have the potential to revolutionize industries, enhance quality of life, bolster national security, and stimulate economic growth. These technologies span a wide range of tools and systems (Moteff et al., 2003). Among the broadly applied critical technologies are Cybersecurity Systems, which protect digital infrastructure, sensitive data, and critical services (Maglaras et al., 2018); Intelligence and Surveillance Tools, including AI, for gathering and interpreting intelligence data (Laplante and Amaba, 2021); Missile Defence Systems and Advanced Aircraft and Military Vehicles, essential for defense against missile attacks (Brown et al., 2005; Moteff, 2007); Biological and Chemical Threat Detection systems; Satellite Technology for military operations and strategic surveillance (Akande et al., 2023); Critical Infrastructure Protection technologies for securing vital resources against threats (Alcaraz and Zeadally, 2015); Biometric and Identity Recognition Systems for security and identification purposes (Štitilis, Laurinaitis and Verenius, 2023); and Advanced Communication Systems, crucial for secure and resilient military communication (Merabti, Kennedy and Hurst, 2011).

This diverse array of technologies serves different purposes, each underlining a different aspect of criticality. The importance of considering diverse perspectives in defining critical technology is evident in its contribution to a more comprehensive, interconnected, adaptable, and policy-relevant understanding of the technological landscape. Adopting this multi-perspective approach is imperative in today's complex and rapidly evolving technological environment, enabling a nuanced examination essential for effective policy and strategic planning. Understanding national economic security through the critical components perspective helps us identify the mainstays of national security through which it can be operationalized, critical infrastructure, critical sectors and critical processes. All critical sectors are built upon critical infrastructures, and the processes governing their working are also critical. It follows from this that changes in these components can have an impact on the national security of a nation (Goodman, 2010).

The selection of critical technologies depends on particular security challenges, geopolitical context, and the military strategy of each country. In terms of prioritising what counts as critical, Clemente (2013, vi) argues that "*it is becoming harder to identify the nodes and connection points whose protection must be prioritized. The result is that in the public debate, at least, critical infrastructure sectors tend to be categorized very broadly, to the extent that they encompass almost every aspect of daily life. The problem, therefore, is that when everything is 'critical', nothing is… The 'critical' label should be used sparingly, and rigorous prioritization encouraged to avoid spending too much or too little on risk management".* These decisions are always political in nature.

In a report for the US Congress, Moteff et al., (2003) set out what makes an infrastructure critical, noting that; "*not all elements of a critical infrastructure are critical. Additional study will be necessary to identify those elements that are the most critical. Other approaches include focusing on vulnerabilities that cut across more than one infrastructure, interdependencies where the attack on one infrastructure can have adverse effects on others, geographic locations where a number of critical infrastructure assets may be located, or focusing on those infrastructure belonging solely to the federal government or on which the federal government depends."*

Moteff et al., (2003) highlight the important need for a better system to identify what is critical, and looking through different lenses is one step in that direction. It also helps us narrow down and justify our selection of a technology that is a part of critical infrastructure.

From a national security viewpoint, the influence of technology on economic security varies, considering there are multiple perspectives determining its critical significance.

2.2.2 Financial systems as critical technology

The economic stability of a nation hinges upon its financial systems (Korol & Poltorak, 2018). Financial systems not only offer intermediation services, but their ambit extends further to credit disbursal, facilitating liquidity, etc. To perform its services, the financial sector is now extremely technology dependent, and the eruption of fintech industry is a testimonial to that (Dorfleitner et al., 2017; Chemmanur et al., 2020). The role of the financial sector in economic security is therefore pivotal, as are its components that come together to make the sector function; ICT being one of them. An IMF paper focused on analysing the relationship between the use of ICT in banks and entrepreneurship provides empirical evidence that young firms that are exposed to ICT-intensive banks have stronger job creation abilities (Timmer, 2021). The paper further states that ICT intensity in banks has strong

implications for entrepreneurship, as it increases startup activity; it also dismisses geographical distance as a factor between lender and borrower (Timmer, 2021).

Notably, the technologies that power core financial processes are gaining prominence in upholding economic stability and security. The efficiency, reliability, and resilience of these technologies can directly impact a nation's economic fortitude (Popelo, Dubyna and Kholiavko, 2021). A de facto critical technology is the real-time gross settlement (RTGS) payment system (Bech and Hobijn, 2006). The RTGS system was introduced to counter Herstatt Risk, named after a German Bank called Herstatt (Kaminska, 2019). Almost all the countries in the world use this complex system to perform high-value interbank transactions (Bech, Shimizu and Wong, 2017). We know about the functionality of the technology, however, the mechanisms through which it associates itself with society are not completely understood.

Money transfers now happen on an instantaneous basis, there are less errors of omission in national accounting. It is less complex now for governments and central banks to discharge their fiscal and monetary policy duties (Khiaonarong and Humphrey, 2022). We are better judges of the current states of our economies, which can be attributed to the multitude of financial data generated in the financial systems (Nanaeva, Aysan and Shirazi, 2021). As already mentioned above however, multiple threats to economic security can arise from potential dysfunction in a critical technology, including financial systems.

Based on our understanding thus far, figure 2-2 depicts the perspective pursued in this research.

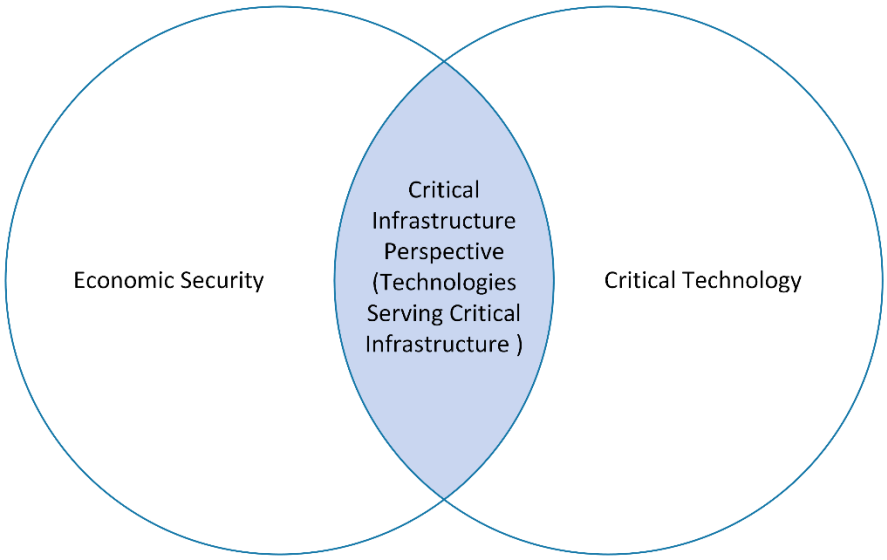

Figure 2-2 Perspective Selection for Economic Security and Critical Technology

2.2.3 Risks and disruption in technology affecting critical infrastructure.

Technology's criticality hinges upon the severity of potential negative outcomes in the event of its failure or disruption. Many research papers explore the impact of technology from the financial sector on the economic well-being/security of a nation (Wijnberg, van den Ende and de Wit, 2002; Shamim, 2007; Dapp, Slomka and Hoffmann, 2014). These impacts are discussed by many authors in terms of risk, which is always associated "*with probabilities (or frequencies) and consequences, often in a*

multiplicative form, expressing expectation values" (Vrijling et al., 2004, 570). In assessing risk criteria for critical infrastructure, three questions must be answered (Vrijling et al., 2004):

- What can happen? Or, what can go wrong?
- How likely is it that that will happen?
- If it does happen, what are the consequences?

The Netherlands is keenly aware of the need to be cognisant of risks and disruption from critical infrastructure. Mennen and Van Tuyll (2015) explore the National Security Strategy approved by the Dutch government which includes both natural hazards and hazards caused by technical failure and malicious threats. The Dutch government has categorised its vital processes as category A and category B. Each category corresponds to a different threshold towards the tolerance of disruption of economic processes. A disruption in vital process causing damages greater than EUR 50 billion or approx. 5% in real income is categorised as category A, while category B corresponds to damages greater than EUR 5 billion or 1% fall in real income (van Justitie en Veiligheid, 2021).

The impact a technology has on the economic security of the nation depends upon how the technology manifests itself within the socio-economic fabric of both organisations and the broader nation (Tohidi, 2011). For instance, disruption in the payment settlements system has the capacity to destabilize the financial sector, creating liquidity and credit risks (McPhail, 2003). Similarly, disruption in telecommunications can severely damage emergency services, hurting the public welfare and emergency healthcare. Several technologies are critical for the economic well-being of a nation, and their criticality is not always mutually exclusive. Many studies have discussed the stability of the financial sector as one of the fundamental dimensions of economic security (Aubert, Patry and Rivard, 2005), it is the facilitator of liquidity, offers a platform for financial intermediation and many more crucial services (Stoneburner, Goguen and Feringa, 2002; Carstens, 2020).

Clemente (2013, vi) argues that the management of risk has become more difficult due to the interdependencies in critical infrastructure which have *"multiplied to the extent that it is difficult, if not impossible, to define defensive perimeters."* Given this level of complexity, societal risks must also be considered; "*for critical infrastructures, however, also societal risks are defined (*Fischhoff, 1990; Slovic et al., 1994).

A structured and systematic approach is needed to analyse and interpret the complex realities surrounding these technologies, their potential risks, and how the social world interactions with the technical. In this light, the socio-technical systems theory emerges as a suitable framework for probing the criticality of technologies for economic security.

2.3 TARGET2 as Critical Technology

2.3.1 Overview

The study of Real-Time Gross Settlement (RTGS) systems, which are crucial for international banking and financial transactions, benefits significantly from the application of the Socio-Technical Systems (STS) framework. RTGS systems are a key component in global finance, as evidenced by their reliance in countries worldwide, a fact highlighted in studies by Furfine and Stehm (1998), Bech, Shimizu, and Wong (2017), Carstens (2019), and D'Andrea and Limodio (2023). The immense transaction value processed through these systems, often exceeding national incomes in major markets as reported in

2012 by High Value Payments Systems (HVPS) ("Statistics on payment, clearing and settlement systems in the CPSS countries - Figures for 2012 - preliminary release", 2013), underscores their critical role in the global economy. The STS framework offers a comprehensive lens to analyze these systems, considering both their technological aspects and their integration within the social and economic fabric. Scholars such as Impenna and Masi (1997), Bradić-Martinović (2011), Bossone, Srinivas, and Banka (2020), and Ahmady (2023) have underscored the reliance of countries on RTGS for both domestic and international banking transactions, making the STS approach particularly relevant for understanding the multifaceted impacts and operations of RTGS systems.

TARGET2 (Trans-European Automated Real-time Gross Settlement Express Transfer System), launched in 2007, is a prime example of such a system used within the Netherlands and across Europe, settling transactions in Euro (Vaes, 2008). Its global counterpart, SWIFT, facilitates interbank settlements worldwide (Jobst, Handig, and Holzfeind, 2012). TARGET2, as a critical RTGS in the Eurozone, is integral for interbank transfers both within and outside the EU. Comprising various unitary technologies, TARGET2 processes payments between banks, revealing a complex interaction between the payment system, banking institutions, and broader societal factors (Bindseil and König, 2011; Whelan, 2014).

The financial system of the Netherlands, considered robust yet not immune to vulnerabilities as seen in the 2008 economic crisis (Chick and Dow, 1997; Chang and Jones, 2013; Vučinić, 2015; Masselink and van Noord, 2009), relies significantly on TARGET2 for critical financial processes. These include retail and consumer financial transactions, high-value transactions between banks, and securities trading (DNB, 2023). The national security strategy underscores the importance of these processes for economic stability.

Applying the STS framework to TARGET2 and the broader RTGS system allows for a comprehensive analysis of how technical components (like the software and hardware of TARGET2) interact with social components (such as regulatory policies, user behaviors, and economic contexts). This analysis is critical to understanding not only how these systems function technically but also how they are embedded in, influenced by, and impact the broader social and economic landscape. In doing so, this approach provides deeper insights into the socio-technical dynamics that underpin the effectiveness, security, and reliability of critical financial infrastructure in the Netherlands and beyond.

2.3.2 Choosing Framework for Target2 Study

In exploring theoretical frameworks to analyse TARGET2, a close comparison was made between Large Technical Systems (LTS) and Socio-Technical Systems (STS), ultimately leading to the selection of STS. Both frameworks offer insightful perspectives on complex systems, yet they differ significantly in focus and applicability.

Large Technical Systems (LTS), as developed by Hughes (1987), provides a historical lens, focusing on the evolution of large-scale infrastructures like electrical grids. LTS emphasizes the interactions between artifacts, organizations, regulators, and user communities, highlighting the technological growth of systems over time. However, as Coutard (1999) notes, LTS tends to prioritize technical aspects, often downplaying the role of social contexts.

Socio-Technical Systems (STS), on the other hand, offers a more balanced approach, giving equal emphasis to both social and technical subsystems. This approach aligns well with TARGET2's structure, which combines advanced technical features such as SWIFT-based architecture, collateral management, and liquidity monitoring modules, with complex social contexts including European financial regulations, inter-organizational relationships between central and commercial banks, and industry cultural norms (Poncelet, 2008; Glowka et al., 2022).

In the analysis, STS emerged as the more suitable framework for several reasons:

Risk Evaluation: Unlike LTS, STS enables a direct examination of risks, including those arising at the intersections between social and technical layers. This aspect is crucial for TARGET2, where understanding and mitigating risks is key to maintaining the financial system's stability (Pasmore et al., 2019).

Conceptualizing Complexity: STS effectively captures the complexity of modern critical infrastructure ecosystems, which include numerous interdependent components and processes. LTS, while valuable, traditionally focuses on historical, self-contained systems and may struggle to represent the intricacies of contemporary, interconnected systems like TARGET2 (Baxter & Sommerville, 2011).

Intervention Alignment: STS is oriented towards actionable improvements, enhancing system performance and economic security. LTS, being more descriptive, primarily explains development trajectories but does not necessarily guide towards constructive interventions. STS's insights are crucial for TARGET2, given its critical role in the financial infrastructure (Appelbaum, 1997).

In summary, although LTS and STS are close competitors in analyzing complex systems, STS was chosen for its comprehensive and balanced focus, its ability to evaluate risks and vulnerabilities, and its potential for guiding practical improvements in TARGET2. This framework's capability to assess both technical components and social dynamics makes it the most appropriate theoretical lens for this thesis.

2.3.3 Socio-technical systems

First introduced by Trist and Bamforth (1951), the concept of a socio-technical system is anchored in the understanding that technology and society are deeply intertwined, rather than existing as isolated entities. This perspective underscores that the success of any system depends critically on the successful interactions between its social and technical elements. It's the harmonious interplay between a system's technical components (like equipment, tasks, techniques) and its social components (encompassing individuals, social structures, and cultures) that determines the overall effectiveness and resilience of the system (Ropohl, 1999).

The socio-technical theory provides a robust framework for analyzing how these two subsystems of technology – the social and the technical – interact with each other (Ropohl, 1999; Ottens et al., 2006). The theory posits that neither the technical nor the social elements can be understood in isolation, nor can their impact be fully realized without considering their interdependencies. This interplay is critical in understanding risks to economic security, which can arise not only from the technological attributes themselves but also from the dynamics of their engagement with various stakeholders. Exploring these interactions, as Baxter and Sommerville (2011) and Sony and Naik (2020) have discussed, can reveal potential vulnerabilities and offer insights into the broader impacts of these technologies on security.

In the context of this study of critical technologies and economic security, the socio-technical perspective is especially relevant. As Coiera (2007, 98) notes, it's about "putting the technical back into socio-technical systems." Critical technologies such as payment systems or cybersecurity infrastructures are limited in their effectiveness if examined solely from a technical standpoint. Whitworth (2011) argues that it's imperative to also consider the social environment in which these technologies are embedded, including regulatory structures, operator skills and attitudes, and the culture of security. The success of these systems, therefore, is contingent upon the synergy between their technical architecture and the social context.

Moreover, the concept of economic security extends beyond traditional economic policies or financial management (Ronis, 2011). It also hinges on how effectively critical technologies are integrated into and interact with our social systems (Cable, 1995; Flechais, Riegelsberger, and Sasse, 2005). This reinforces the importance of socio-technical systems theory, which posits that the successful integration of technology into society is as vital as the technology itself. The theory illuminates the interconnectedness of social and technical aspects, showing that technological risks are not just about the technology itself but also about new dependencies, such as those on cybersecurity and critical materials (Whitworth and De Moor, 2003; Fåk, 2010; Kivimaa et al., 2022).

In essence, the socio-technical systems theory provides a critical framework for exploring the nexus between critical technologies and economic security. By emphasizing the interdependent nature of technological and social elements, this theory sheds light on the comprehensive impact of technology on economic security and underscores the need for a holistic approach in addressing challenges posed by these critical technologies.

The intricate interaction between the social and technical components within technological systems, especially in critical infrastructures like financial systems, has profound implications for economic security. In the realm of financial infrastructure, this interplay can be observed in how technological advancements, such as digital banking platforms, blockchain technology, and automated trading systems, interact with social elements like regulatory frameworks, user behaviors, and organizational cultures. The effective functioning of these technologies hinges not just on their technical robustness but also on how they are perceived, regulated, and utilized within society. For instance, a technically sophisticated digital payment system requires not only robust software and hardware but also user trust, regulatory compliance, and alignment with the existing financial practices and norms.

This research focuses on understanding how the socio-technical dynamics within financial infrastructure impact economic security. For example, a failure in the technical system, such as a security breach in online banking, can have cascading effects on the economy, eroding public trust, disrupting financial transactions, and causing economic instability. Similarly, social factors like non-adherence to cybersecurity protocols by users or insufficient regulatory measures can amplify the vulnerabilities in the technical system, posing risks to the economic security of a nation. Conversely, positive interactions, such as effective regulatory policies that foster innovation while ensuring security, or cultural shifts towards embracing digital financial services, can enhance the resilience and efficiency of financial systems, thereby bolstering economic security.

Therefore, in exploring the financial infrastructure through the lens of socio-technical systems theory, this research aims to uncover the critical points where social and technical elements converge, potentially creating vulnerabilities or opportunities. By doing so, it seeks to provide insights into how these interactions can be managed or leveraged to enhance the economic security of a nation. This exploration is crucial in an era where financial systems are increasingly digitized and interconnected, making the understanding of socio-technical interactions not just relevant but essential for ensuring the stability and security of national economies.

2.3.4 Conceptualizing STS framework for Target 2

Utilizing the Socio-Technical Systems (STS) theory, this framework, grounded in the principles articulated by Trist (1981), provides a comprehensive lens to study the TARGET2 system. The STS theory, emphasizing joint optimization and the interrelatedness of parts, is particularly apt for understanding complex systems like TARGET2, which encompass both technical and social dimensions.

This approach enables us to explore how these dimensions interact and impact the system's effectiveness and resilience.

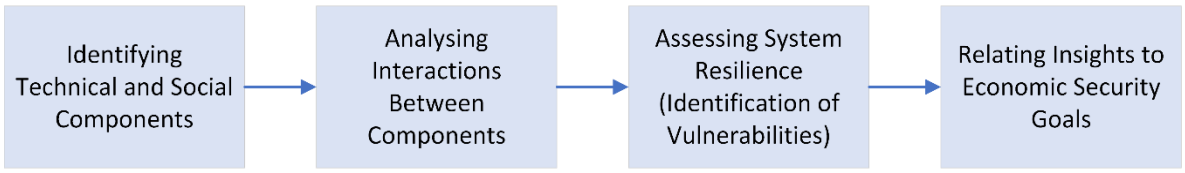

Figure 2-3 Theoretical Framework for Data Analysis

Identifying Technical and Social Components

- Technical Components: The framework first delineates the technical aspects of TARGET2, such as the SSP software, communication protocols, security systems, hardware infrastructure, and interfaces. These components are the backbone of TARGET2, facilitating its core operational functions (Scott & Zachariadis, 2012).

- Social Components: Concurrently, the framework examines the social elements that influence TARGET2. This includes the organizational cultures within the banking sector, the regulatory landscape, professional communities, and the roles of human actors like system operators and managers. These elements play a crucial role in how the system is utilized and governed (Cherns, 1976).

Analysing Interactions Between Components

- The heart of the STS approach lies in analysing the interactions between these technical and social components. It seeks to understand how these elements influence each other and the overall system functionality. For example, how do changes in regulatory policies impact the technical operation of TARGET2? Or, how do the system's technical limitations affect the behaviors and decisions of its operators?

Assessing System Resilience (Identification of Vulnerabilities)

Drawing from sociotechnical systems theory, the framework then assesses TARGET2's resilience. This involves identifying potential vulnerabilities within the system, especially at the points where technical and social components intersect (Pasmore et al., 2019). The goal is to understand how these vulnerabilities could lead to system failures or suboptimal performance.

Relating Insights to Economic Security Goals

Finally, the insights gained from this analysis are connected to the broader goals of economic security. The framework examines how the interplay of social and technical elements within TARGET2 impacts crucial factors like transaction accuracy, fraud prevention, and overall system integrity. This step is vital to understanding how TARGET2, as a socio-technical system, contributes to or detracts from the economic security of the Eurozone.

2.3.5 Key technical components and social interfaces of the TARGET2 system

Building upon the socio-technical framework developed for analysing TARGET2, this section represents a crucial preparatory phase towards an extensive document analysis. By conducting a detailed literature review, we aim to establish a high-level map of the social and technical components integral to TARGET2, as identified in seminal academic works. This review serves as the stepping stone in our journey, laying the contextual groundwork and providing a deepened understanding of the complex interplay within TARGET2. It synthesizes key insights from a range of scholarly sources, offering a

comprehensive perspective on the system's multifaceted nature. This preparatory stage is instrumental in informing our subsequent document analysis, ensuring that our approach is grounded in a robust and nuanced understanding of TARGET2's socio-technical dynamics. By anchoring our analysis in the rich insights gleaned from this literature review, we ensure a more informed, context-sensitive exploration of TARGET2, setting the stage for an in-depth examination of its operational, regulatory, and technological intricacies in the subsequent document analysis phase.

This section draws upon a range of scholarly contributions that shed light on the intricate interplay of social and technical elements within TARGET2. The aim is to construct a high-level map that captures the essence of these components, setting a firm foundation for our document analysis. Panourgias (2015) sought to illuminate the complex causalities between the social and technical aspects of cross-border capital market integration, including TARGET2. Broader academic research on TARGET2 covers the various interdisciplinary themes as outlined below (Vaes, 2008; Chin, 2017; Tarasiuc 2018):

TARGET2 is underpinned by a complex interplay of social and technical components as shown in Table 2.1 below:

Table 2.1 Target2's Socio-Technical Interplay based on Literature Review

Component	Detail	Interpretation
Social Elements		
Regulatory Dynamics	Szécsényi (2015) provides an analysis of TARGET2's evolving regulatory landscape including compliance challenges, offering insights into how regulations shape system operations. Glowka et al., (2022) discuss changing legal norms and regulations impacting TARGET2, highlighting the need for the system to adapt.	Regulations and compliance requirements have a significant influence on how TARGET2 functions, necessitating system adaptations as the legal landscape evolves.
Organizational Cultures	Panourgias (2015) examines organizational culture dynamics in the context of TARGET2 operations, elucidating how institutional cultures influence system implementation and use.	Organizational cultures within TARGET2 institutions impact how the system is put into practice, signalling the importance of cultural factors.
Human Roles and Relationships	Panourgias (2015) also looks at human roles and relationships within TARGET2, shedding light on the complex dynamics between system operators, managers, regulators, and other stakeholders.	There are multifaceted relationships and interactions between human actors that shape TARGET2 operations in consequential ways.
Technical Elements		
System Architecture	Poncelet (2008) provides an architectural analysis of the TARGET2 system, enhancing understanding of its structural design and technological robustness.	The underlying architecture of TARGET2 has a direct bearing on its capabilities and performance.

Data Management	Cecchetti et al., (2012) examine TARGET2's data management features, offering insights into how transactional data is handled to ensure efficiency and integrity.	Effective data management is crucial for TARGET2 to facilitate transactions accurately and securely.
Cybersecurity Measures	Krüger and Brauchle (2021) analyze TARGET2's cybersecurity, assessing the effectiveness of its security protocols in safeguarding against threats. Heijmans and Wendt (2023) also investigate cyber risks and controls, further evaluating TARGET2's cyber resilience.	Ongoing assessment of cyber risks and continuous security enhancement is pivotal for protecting TARGET2.
Interactions and Interdependencies		
Communication Protocols	Martin, Christoph, and Katharina (2019) look at communication protocols in TARGET2, elucidating their role in enabling smooth interbank transactions.	Efficient communication protocols facilitate seamless transactions between TARGET2 participants.
Feedback Loops	Kamps and Heijman (2021) discuss feedback mechanisms in payment systems like TARGET2 that enable adaptive responses to operational disruptions.	Understanding feedback mechanisms allows TARGET2 to adaptively respond to emerging challenges.
Collaborative Decision-Making	Martin, Christoph, and Katharina (2019) also examine collaborative decision dynamics in TARGET2, highlighting the importance of cooperation in system operations.	Collective decision-making is key for effective TARGET2 governance and operations.
Implications and Optimization		
Operational Efficiency	Jobst, Handig, and Holzfeind (2012) assess TARGET2's operational efficiency, providing insights into process optimization and delay reduction.	Optimizing operational efficiency is an ongoing imperative for TARGET2.
Regulatory Compliance	Glowka et al., (2022) analyze regulatory compliance in TARGET2, investigating its impact on adherence to legal and financial norms.	Compliance with evolving regulations ensures TARGET2 aligns with legal standards.
Innovation and Future Development	Bullmann and Pinna (2017) look at innovation potential for TARGET2, shedding light on its capacity to adapt to new technologies. Pezzuto (2019) examines future outlooks for TARGET2, underscoring the need for continued evolution.	TARGET2 must continue innovating and evolving technologically to maintain cutting-edge capabilities.

This literature review and table provide a comprehensive overview of the socio-technical aspects of TARGET2, covering the gamut from regulatory dynamics to system architecture and from data management to collaborative decision-making. The insights garnered here are instrumental in setting the stage for a thorough document analysis of TARGET2, offering a well-rounded perspective on its operation within the broader context of the Eurozone's financial infrastructure.

2.3.6 Factors Contributing to the Criticality of TARGET2 in Economic Security

The criticality of TARGET2 for economic security is rooted in the harmonious integration of its social and technical components. This synergy between different elements ensures the stability, security, and efficiency of TARGET2, thereby making a significant contribution to the economic security within the Eurozone. The application of Socio-Technical Systems (STS) theory offers a comprehensive framework for understanding and analyzing such complex systems.

TARGET2 serves as an invaluable case study for exploring economic security within the realm of critical technology for several reasons. Firstly, as a critical financial infrastructure, TARGET2 is fundamental to the stability and integrity of the Eurozone's financial system. The examination of its security aspects offers insights into securing essential financial systems, which are crucial for overall economic security (Armstrong, 2016). Additionally, financial technologies like TARGET2, which include settlement systems, have dual-use applications. While primarily designed for legitimate financial transactions, they also pose the risk of being exploited for illicit activities, such as money laundering, terrorism financing, or cyberattacks. An exploration of TARGET2's security challenges sheds light on the dual-use nature of critical financial technologies (Martins and Ahmad, 2020).

Moreover, the interconnectedness of TARGET2 with various financial institutions across the Eurozone brings forth systemic risks. Analyzing TARGET2 helps understand the implications for economic security in terms of the stability of the entire financial ecosystem (Cai et al., 2018). TARGET2 also plays a pivotal role in facilitating cross-border transactions within the Eurozone, which are high-value transactions carrying significant stakes. As identified by Hoorens et al. (2000), the vitality of critical sectors in the Netherlands is closely linked to these transactions, underlining the severe consequences for liquidity and foreign exchange if the system falters or fails. Ensuring the security of these transactions is vital for economic security, given their importance in trade, investment, and economic cooperation among member states. Studying TARGET2, therefore, provides valuable insights into securing cross-border financial flows (Kahler, 2004; Sparke, 2006) and understanding the broader implications of high-value transactions in the economic landscape, as further explored by Laugé, Hernantes and Sarriegi (2015) and Rehak et al. (2016).

Another crucial aspect is data security and privacy. TARGET2 processes vast amounts of financial data, and ensuring its security against breaches, unauthorized access, or tampering is paramount for economic security. Researching the data security measures implemented in TARGET2 offers insights into the protection of sensitive financial information, which is a critical aspect of economic security (Koponen, 2012; Coburn, Leverett and Woo, 2018).

Lastly, the security of critical financial technologies like TARGET2 also involves significant policy considerations and international collaboration. Understanding how policymakers address security challenges, implement regulations, and collaborate across borders is essential for enhancing economic security in an interconnected world (Kregel, 2019).

2.3.7 Operational and Security aspects of Target2

The TARGET2 system is designed with several key features to ensure the stability and security of financial transactions. One of the foremost features is its ability to settle transactions in real-time, which guarantees that payments are processed instantly between participating banks, thus enhancing the efficiency of the financial system (Ulbrich and Lipponer, 2012). Another crucial aspect of TARGET2 is its effective liquidity management, ensuring that all participants have adequate funds available to settle their transactions, a vital component for the smooth operation of financial markets (Duca-Radu and Testi, 2021).

In addition to these features, TARGET2 employs a robust collateral management system. This system is essential for securing large transactions and minimizing the associated credit and liquidity risks within the settlement process (Poncelet, 2008). Further bolstering the system's integrity is its comprehensive transaction monitoring capability. TARGET2 constantly scrutinizes transactions for any signs of unusual or suspicious activity, serving as a critical operational indicator of economic security (Glowka et al., 2022).

Data security is also paramount in TARGET2, with all data transmitted through the system being encrypted. This encryption ensures the prevention of unauthorized access and protects sensitive financial information, a necessary measure in today's digital age (Tiberi and Bucciol, 2023). Moreover, the system is equipped with redundancy and disaster recovery mechanisms, which are crucial for maintaining uninterrupted operation, especially in the face of technical failures or natural disasters (Galbiati and Stanciu-Vizeteu, 2015).

Lastly, TARGET2 places a high emphasis on compliance with regulatory standards. This compliance is fundamental to maintaining the security and stability of the financial system, aligning with the rigorous demands of financial regulation and oversight (Glowka et al., 2022)

2.3.8 Potential vulnerabilities

This review now explores how alterations in the socio-technical dynamics of TARGET2 could potentially influence the Netherland's economic security. If the payment system (RTGS) is disrupted, the banks will have no access to liquidity, forcing them to borrow from the markets. In a scenario where a crisis were to materialize, the cost of borrowing will also rise. In a longer term this disruption would be catastrophic for the economy (Ulbrich and Lipponer, 2012). The money and security markets will also slow down, hurting the government's ability to finance its expenditures (SWIFT, 2014). Moreover, Rooj and Sengupta (2020) found that RTGS and economic growth significantly impact each other for good. They have recognized a bidirectional causality between the payment system and economic growth. They were also able to unravel the positive impact of value of RTGS on income and price levels in the economy.

Examining the vulnerabilities of the TARGET2 system from a socio-technical perspective involves understanding the interplay between its social (regulatory dynamics, organisational cultures, human roles and relationships) and technical (system architecture, data management, cybersecurity measures) elements:

- Social Engineering and Cyber Threats: Cyber threats often exploit human vulnerabilities through techniques like phishing and social engineering. Addressing this requires not just technical solutions such as robust firewalls but also social interventions such as training programs to increase awareness about these threats among employees, creating a socio-

technical defence against attacks (Krüger and Brauchle, 2021); Heijmans and Wendt, 2023). Gonzalez-Granadillo et al., (2018) proposed a dynamic risk management response system (DRMRS) consisting of a proactive and reactive management software that aims at evaluating threat scenarios in an automated manner, as well as to anticipate the occurrence of potential attacks)

- Organisational Culture and Compliance: The organisational culture within banks and financial institutions plays a vital role in ensuring compliance with security protocols. A culture that prioritizes security awareness, regular training, and adherence to protocols strengthens the socio-technical fabric. Alternatively, a neglecting these social aspects can weaken even the most advanced technical safeguards (Panourgias, 2015; Glowka et al., 2022)
- User Behaviour and System Usage: Understanding how users interact with the system is crucial. Anomalies in user behaviour, which can be both social (like a change in employment status) and technical (unexpected login locations), can signal potential security breaches. Socio-technical solutions involve continuous monitoring of user patterns and behaviours to detect and respond to deviations promptly (Abad et al., 2013)
- Inter-Organizational Relationships: The TARGET2 system involves multiple banks and entities interacting with each other. Socio-technical vulnerabilities can emerge from these interactions, such as when there is a lack of standardized security practices across all participating organizations. Harmonizing these practices is essential to create a cohesive and secure network (Martin, Christoph and Katharina, 2019)
- Regulatory Dynamics: Socio-technical vulnerabilities can originate from regulatory gaps or inconsistencies. Changes in regulations can create a socio-technical challenge, requiring financial institutions to adapt both their technical systems and social protocols to remain compliant. Failure to do so can result in systemic vulnerabilities.
    - TARGET2 imbalances could be addressed by tightening collateral requirements for central bank liquidity. For the longer term, the evidence that the euro area has been subject to internal balance-of-payment crises should be taken as a strong signal of weakness and as an invitation to reform its structures (Cecchetti, McCauley and McGuire, 2012).
- Public Perception and Trust: The socio-technical dynamics also encompass public perception. If a significant breach occurs, it erodes public trust not only in the affected institutions but also in the broader financial system. Rebuilding this trust requires not just technical enhancements but also social efforts, such as transparent communication about the incident and the steps taken to prevent future occurrences (Lucarelli, 2017). There is also the possibility of default by the indebted, peripheral countries because of the imposition of austerity policies by the European Central Bank (ECB)/European Union (EU)/International Monetary Fund (IMF) with corresponding impact on trust in the system (Lucarelli, 2017).
- Innovation and Emerging Technologies: While technologically progressive, introducing new technologies can create socio-technical challenges. For instance, integrating blockchain technology into financial systems might introduce new social dynamics concerning data privacy and security practices, necessitating a balance between technical innovation and social acceptance and understanding (Bullmann and Pinna, 2017; Pezzuto, 2019). Some like Prewett, Prescott and Phillips (2020) argue that the adoption of blockchain was inevitable, but that barriers and risks remain.

2.3.9 Implications of TARGET2 interdependency with other financial systems for economic security

The interdependency of TARGET2 with other financial systems is integral to economic security. Its smooth operation ensures financial stability, maintains market confidence, facilitates cross-border trade, supports liquidity management, aids in monetary policy transmission, mitigates systemic risks, and upholds international reputation (Hausken, 2017). Safeguarding the integrity and reliability of TARGET2 is paramount for ensuring the economic security of the Eurozone countries, including the Netherlands (Barredo-Zuriarrain, Molero-Simarro and Quesada-Solana (2017).

2.4 Gaps in the literature

The existing body of literature, while acknowledging the increasing reliance on technology within critical infrastructures, reveals notable gaps in understanding the deeper mechanisms of technology's role in economic security. This thesis aims to address these gaps by focusing on several key areas where current research is lacking or insufficient:

2.4.1 Limited Focus on Socio-Technical Perspectives in Critical Infrastructure

Socio-technical approaches have been widely applied in sectors such as healthcare, as demonstrated by Pasmore et al. (2019). However, their application in examining critical infrastructure technologies, especially in the financial sector, remains scarce. Hoffmann (2018) highlights the need for deeper scholarly attention towards the socio-technical dynamics within financial systems. This thesis contends that a socio-technical lens is vital to fully comprehend how technological systems interact with social elements within critical infrastructures, particularly in the financial sector.

2.4.2 Under-Examination of Technology Manifestations in Economic Security

While the literature acknowledges the severe impact of disruptions in critical infrastructure technologies on economic continuity, as noted by Luiijf et al. (2003), there is a lack of granular analysis on how these technologies functionally manifest their significance within economic security frameworks. This thesis seeks to delve into the functional dynamics of how critical technologies, specifically within financial systems, underpin economic stability and security.

2.4.3 Ambiguity in Risk Propagation Pathways

The existing literature recognizes the risks posed by disruptions to critical technologies, especially how these disruptions can cascade across vital systems. However, as Rinaldi et al. (2001) point out, there is an ambiguity in understanding the precise mechanisms through which these risks propagate. This thesis aims to elucidate these mechanisms, offering a clearer view of the pathways through which technological disruptions can impact economic security.

2.4.4 Lack of Comprehensive Conceptual Framework

There is a lack of well-defined and comprehensive conceptual frameworks specifically addressing the relationship between socio-technical systems and economic security. Existing literature has not sufficiently developed multi-faceted frameworks that encapsulate the complex interdependencies between critical infrastructure technologies and the varied aspects of economic security such as financial stability, trade continuity, crisis resilience, and systemic risk management. Constructing conceptual models that capture these nuances can inform evidence-based policy and technology governance.

To address these gaps, this thesis adopts a socio-technical lens tailored specifically to the systemic role and contextual implementation of Target2 within the Dutch financial ecosystem. The chosen analytical approach methodically evaluates the functional dynamics that manifest Target2's criticality and maps

out the potential risk pathways that can undermine economic continuity. By constructing a conceptual model, this study informs dynamic interventions necessary to fortify economic safeguards in a landscape increasingly reliant on complex technologies.

In essence, this research aims to enhance the understanding of the socio-technical interplay in critical financial technologies and provide a nuanced analysis of their role in economic security, thereby contributing valuable insights to the field and suggesting practical approaches for managing and mitigating associated risks.

Chapter 3 Research Methodology

3.1 Research Design

The research design of this thesis is a qualitative approach that utilizes both a coding framework and interpretive analysis to investigate the TARGET2 payment system and its implications for the economic security of the Netherlands. Initially, the study employs a systematic coding framework to analyze the initial sections of TARGET2 documentation. This involves identifying and categorizing the technical and social elements within the system, as well as their operational implications. This phase establishes a detailed understanding of TARGET2's complex architecture and the dynamics of its user interface, laying the groundwork for a more in-depth exploration.

As the study delves into Sections 4.4 and 4.5, it transitions into a qualitative interpretive methodology. This shift is essential to explore the roles and services provided by TARGET2, which are identified through a stakeholder analysis, and to infer potential vulnerabilities that are not explicitly mentioned in the documentation. The interpretive phase, informed by socio-technical systems theory and a comprehensive understanding of financial infrastructures, allows for the identification of latent risks and an assessment of their potential impact on the financial system.

This approach enables a comprehensive analysis, capturing both the explicit operational functionalities of TARGET2 and the more subtle vulnerabilities that may present risks. It facilitates a thorough examination of how TARGET2, as a socio-technical system, affects the economic stability of the Netherlands, particularly in terms of its operational resilience and vulnerability to systemic risks.

To further validate and enhance the credibility of the findings, the research incorporates expert interviews. These interviews are critical for confirming the research outcomes and integrating perspectives from individuals with specialized knowledge and practical experience in the field.

Overall, the research design—encompassing a coding framework, interpretive analysis, and expert validation—ensures a robust, comprehensive, and real-world applicable investigation. The study not only provides a detailed exploration of TARGET2's role within the financial ecosystem but also underscores its significance in the broader context of the nation's economic security.

3.2 Data Collection Methods

Document Selection and Relevance

Selection of TARGET2 Information Guide

The TARGET2 Information Guide is strategically chosen as the primary document for exploration in sections 4.1 to 4.3 of this thesis due to its comprehensive and authoritative depiction of the TARGET2 payment system. This guide is crucial for understanding the socio-technical interplay within TARGET2, offering in-depth insights into both the technical infrastructure and social dynamics of the system.

Justification for the Selection

Comprehensive Technical Details: The TARGET2 Information Guide provides an exhaustive account of the system's technical components, such as core platforms, interfaces, and network structures. This information is essential for understanding the technical architecture of TARGET2, which forms the foundation of the socio-technical analysis in the initial research sections.

Insight into Social elements: The guide is also a valuable resource for understanding the social aspects of TARGET2, including its user base, operational roles, and governance structures. This information is pivotal for examining the interactions between various stakeholders and the governance of the system, enriching the socio-technical analysis.

Relevance: The document is sourced directly from the European Central Bank's website. It is an official and current document. This authenticity ensures the research is based on reliable and relevant data, which is critical for an accurate socio-technical analysis.

Foundation for Interpretive Analysis: Beyond providing data for the coding framework in the initial sections, the guide also serves as a foundation for the subsequent interpretive analysis. It allows for a deeper understanding of the socio-technical dynamics, enabling a nuanced exploration of the system's roles, vulnerabilities, and economic security implications.

Reasoning for Utilizing Document Analysis

Granular Insight: Document analysis was chosen as the primary method for data collection to capture as granular insights as possible into the TARGET2 system. This approach allows for a deep dive into the intricate details of the system's operations, technical specifications, and social interactions, which are richly encapsulated in the documentation.

Specificity and Depth: Unlike other methods such as surveys or interviews, document analysis provides access to detailed and specific information that has already been collated and organized. This is particularly important for understanding complex systems like TARGET2, where every component plays a critical role.

Scope and Feasibility: Considering the scope and feasibility of the thesis, document analysis emerged as the most appropriate method. While supplementary methods could provide additional perspectives, they would extend beyond the practical confines of this research. Document analysis, therefore, offers a focused and in-depth exploration within the set scope.

Authenticity and Reliability: Relying on the TARGET2 Information Guide, an official document from the European Central Bank, adds a layer of authenticity and reliability to the research. This ensures that the analysis is grounded in factual and up-to-date information, providing a robust foundation for the thesis.

The use of document analysis, particularly with the TARGET2 Information Guide, is thus a deliberate and strategic choice, aligning with the research objectives and providing a comprehensive understanding of the TARGET2 system within the constraints of this thesis.

Interviewee Selection and Relevance

In complementing the document analysis from the TARGET2 Information Guide, the research integrates interviews with three professionals for the validation of findings. Each of these individuals contributes distinct expertise and perspectives, vital for substantiating and enriching the research conclusions. A detailed interview protocol is attached in the Appendix A.4.

1. Payments System Expert (Expert in TARGET2)

Relevance for Validation:

Insider Perspective: This expert brings an insider's view on TARGET2, providing insights into its operational nuances and real-world applications.

Technical Expertise: Their deep knowledge of TARGET2's functionalities is crucial for validating the technical aspects highlighted in the document analysis.

Internal Validity: They play a key role in affirming the internal validity of the research findings, ensuring that the interpretations and conclusions are consistent with the actual operational realities of TARGET2.

2. Financial Economist

Relevance for Validation:

Economic Implications: A financial economist can critically evaluate the implications of TARGET2 on economic security, offering a macroeconomic perspective on the system's role.

Systemic Perspective: Their understanding of the broader financial system is essential for assessing TARGET2's impact within the larger economic context.

Theoretical Rigor: They add theoretical depth to the validation process, ensuring that the economic interpretations in the research are grounded in sound economic principles.

3. Policy Advisor

Relevance for Validation:

Policy Formulation and Implementation Insights: The Policy Advisor's role in formulating and implementing institution policies provides critical insights into how TARGET2 is integrated and operationalized within these frameworks. Their perspective is essential for understanding the strategic considerations and decision-making processes influencing TARGET2's use at a policy level.

Regulatory and Compliance Expertise: As a policy advisor, they possess a deep understanding of the regulatory environment and compliance requirements. This expertise is vital for assessing TARGET2's alignment with current financial regulations and its adaptability to evolving regulatory landscapes.

Stakeholder Dynamics and Impact Analysis: Their experience with stakeholder management within the central banking ecosystem enables them to provide a nuanced analysis of how TARGET2 impacts various stakeholders, including financial institutions, regulatory bodies, and the broader economy. This helps in evaluating the system's effectiveness and its role in shaping financial stability.

By incorporating interviews with these three professionals, the research significantly enhances its validation process. The combined expertise of a TARGET2 expert (Payment Systems Expert), a financial economist, and a Policy Advisor ensures a thorough and multifaceted validation, covering technical, economic, and policy-related aspects of TARGET2. These interviews not only corroborate the findings derived from the document analysis but also provide a rich tapestry of insights. This approach enriches the overall credibility and robustness of the research by integrating perspectives from operational, macroeconomic, and policy viewpoints, offering a more comprehensive understanding of the complexities surrounding TARGET2.

3.3 Analytical Approach for Document Analysis

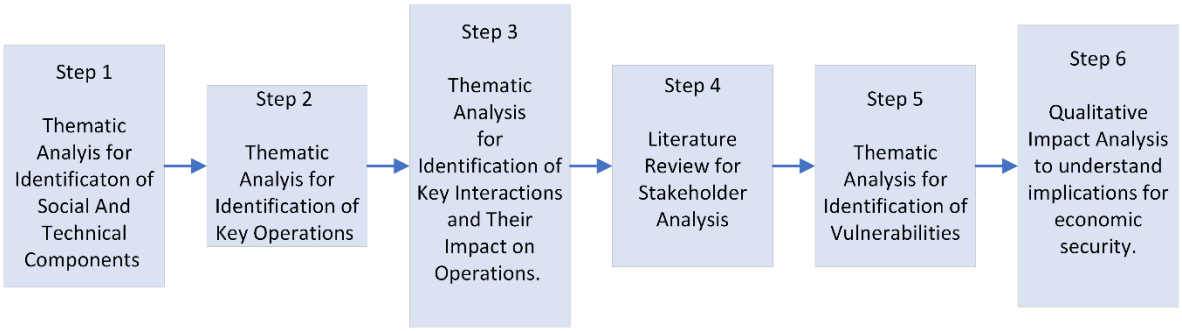

Figure 3-1 Analytical Approach for Document Analysis analytical Approach for Data Analysis

Step 1: Identification of Social and Technical Components

In dissecting the socio-technical fabric of the TARGET2 system, Section 4.1 adopts a thematic analytical approach underpinned by a structured coding and categorization framework. This framework serves to parse out and examine the intricate relationship between technical components and social elements of the system.

Coding Framework Development

Initial Coding: This phase involved an exploratory review of the TARGET2 documentation, wherein raw data points were coded in Atlas Software, meaning codes were derived directly from the text (e.g., "SSP" from "Single Shared Platform").

Focused Coding: After initial coding, focused coding was employed to synthesize and categorize these codes into more substantive and thematic groupings. For instance, the code "SSP" was categorized under 'Core platforms'.

Categorization Process

Technical Components Categorization: Technical elements were categorized by their functionality within TARGET2. For example:

'Core platforms' included the SSP, TIPS, and T2S.

'Interfaces' covered the various points of interaction between the core platforms and ancillary systems.

'Networks' encapsulated communication protocols like SWIFTNet.

Social Elements Categorization: Social elements were categorized by the roles and hierarchical structures within the TARGET2 environment. For example:

'Users' were differentiated into direct participants, indirect participants, and ancillary systems.

'Governance Bodies' were divided into levels reflecting their decision-making hierarchy.

Analytical Approach

Code Mapping: Each code was mapped to its respective category, creating a matrix that highlighted the relationship between technical specifications and user engagement.

Theme Identification: From this mapping, broader themes emerged, such as 'System Accessibility' for users and 'Regulatory Compliance' for governance bodies.

Example of Coding and Categorization

1. **Code:** 'Direct Participants'

Initial Observation: Noted as entities actively engaging with the TARGET2 platform.

Focused Category: Classified under 'Users' in the social elements section.

Thematic Relevance: Represented a key user group whose interactions with the platform are critical for the system's transaction processing and governance.

2. **Code:** 'T2SI'

Initial Observation: Identified as an interface for the TARGET2-Securities.

Focused Category: Placed under 'Interfaces' in the technical components section.

Thematic Relevance: Signified a pivotal point of access and operational connectivity within the system's architecture.

Summarizing the Approach

This approach enabled a systematic breakdown of the TARGET2 system into discernible elements, providing a clear mapping of how each technical component is engaged by various social actors. By categorizing and coding the socio-technical facets, we could articulate the foundational structure of TARGET2, setting the stage for subsequent analysis of key interactions which constitute a higher level of system play. The categories derived here not only clarified the roles and functionalities within the system but also illustrated the potential points of synergy and friction, critical for understanding the overarching socio-technical landscape.

Step 2: Identification and Categorization operations

This step is dedicated to the identification and categorization of the operational processes within the TARGET2 system. It is a foundational step in the analysis, aiming to unravel and classify the intricate web of operations that constitute the system's functionality.

Definition of Operations: In the context of the TARGET2 system, an 'operation' is defined as any sequence of activities or set of procedures that are essential for the system's functioning and service delivery. Operations encompass both automated and manual processes, which facilitate the system's core functions, adhere to compliance standards, manage risks, and ensure effective user interaction. This definition provides a broad yet focused lens to identify and analyze relevant processes within TARGET2.

Analytical Lens for Identifying Operations:

Functional Significance: The primary criterion for identifying an operation was its functional significance within the TARGET2 system. Processes that play a crucial role in the core functions of the system, such as transaction processing and liquidity management, were given priority.

System Impact and Interdependency: Operations that have a significant impact on the system's overall performance or are highly interdependent with other processes were identified as key operational processes. For example, risk control mechanisms are essential for the system's stability and are closely linked with other operational processes.

Regulatory and Compliance Relevance: Processes that are critical for ensuring compliance with regulatory standards and internal governance protocols were also identified as key operations. This includes procedures and protocols that maintain legal and regulatory adherence.

User Interaction and Accessibility: Operations that involve direct interaction with the system's users or affect the user experience were identified. This includes user interface processes, communication protocols, and user support mechanisms.

Process of Identification:

An in-depth review of the TARGET2 documentation was conducted, focusing on identifying mentions and descriptions of operational processes. Operational elements mentioned in the documentation were extracted using a structured coding approach. This involved coding direct references to operational processes and inferencing operational implications from the documented system functionalities and protocols. These processes, identified as the backbone of the TARGET2 system, include transaction processing, liquidity management, risk control mechanisms, compliance adherence, and user interaction protocols.

Categorization of Identified Processes:

The identified operational processes were grouped into coherent categories, based on their nature and functionality. This categorization was grounded in criteria such as process objectives, operational significance, and interaction types. The process grouping led to the formation of distinct categories, each representing a critical aspect of TARGET2's operations.

Examples of Categories:

Transaction Processing: Encompassing all processes related to the handling and execution of transactions within the TARGET2 system.

Risk Management: Including processes aimed at identifying, assessing, and mitigating financial and operational risks.

Liquidity Management: Covering operations that ensure adequate liquidity levels are maintained for smooth system functioning.

Compliance and Protocols: Encompassing procedures and guidelines to ensure adherence to regulatory standards and effective communication.

The completion of this step has resulted in a clear and structured understanding of the operational processes within TARGET2. The categorization of these processes provides a foundation for further analysis, allowing for a targeted approach in evaluating the efficiency, effectiveness, and robustness of the TARGET2 system. The identified categories serve as key pillars in analyzing the operational integrity and performance of the TARGET2 system.

Step 3: Interaction and Operational Impact Analysis

Interaction Analysis

Following the categorization established in step 1, which delineated the socio-technical elements of TARGET2 into functional categories, this step advances the examination to the interactions between these categories. This section explores the engagement between the technical components and social elements identified, assessing their impact on the operational efficacy of TARGET2.

Analytical Strategy for Interaction Analysis

The analytical strategy is methodically structured to follow on from the previous categorization. It revisits the interactions between the functional categories, viewing these as the operational conduits within TARGET2. A detailed investigation deconstructs each interaction into its constituent sub-functions, shedding light on their technical roles and social responsibilities.

Approach in Detail

Interactions as Analytical Units: Each interaction from the table in Section 4.1 is considered an analytical unit, informing the depth of scrutiny required for each sub-function.

Deconstruction into Sub-Functions: The interactions are dissected further, categorizing specific technical and social sub-functions. This deconstruction aids in thoroughly understanding the contribution of each interaction to TARGET2's ecosystem.

Interpretative Analysis: The analysis involves correlating technical capacities with social demands, policies, and feedback to interpret how these shape the functionality and evolution of the TARGET2 system.

Example of Analytical Application

An example is the interaction between **Core Platforms and Users**:

Mapping the Interaction: Identified as a primary interaction, it is pivotal due to the core platforms' role in transaction processing and the users' reliance on these platforms for financial operations.

Sub-Functional Dissection:

The technical aspect focuses on the system's architecture, including modules and connectivity protocols. The social aspect assesses user roles and requirements for seamless transaction execution and liquidity management.

Operational Significance: The interaction is interpreted as a feedback loop where the technical infrastructure's robustness and efficiency are matched by user operations, governed by clear policies and procedures.

Summarizing the Approach

In conclusion, step 2 aims to contextualize and interpret the significance of socio-technical interactions within TARGET2. By adopting this analytical approach, the operational synergies and potential points of friction within the system are elucidated. This analysis is crucial for understanding how TARGET2 maintains its function as a financial infrastructure and suggests improvements to enhance its resilience and adaptability to changing financial conditions.

Operational Impact Study

This step explores how the socio-technical interactions outlined in the previous step manifest in the operational processes within TARGET2. It investigates the practical outcomes and effects of the interplay between TARGET2's technical infrastructure and the user community on its day-to-day functions.

Approach for analyzing operational implications includes:

Identification of Operations: Recognizing the specific operational processes that are influenced by the socio-technical interactions.

Assessment of Impacts: Evaluating how these interactions affect the operational effectiveness, efficiency, and security.

Implication Synthesis: Summarizing the consequences of these impacts on TARGET2's broader operational goals and stability.

Example of Operational Implications:

Transaction Processing is one of the key operations. It is impacted by the reliability of core platforms and user operations. It ensures the timeliness and accuracy of financial transactions, which is critical for the smooth functioning of the European financial markets.

Step 4: Stakeholder Analysis

In this step, stakeholder analysis was performed through a comprehensive literature review to understand the intricate relationship between TARGET2 and the financial system of the Netherlands. The analysis aimed to elucidate the roles, services, and functions provided by TARGET2 to various stakeholders within the Dutch financial ecosystem.

Methodology for Stakeholder Analysis

Literature Review: A systematic review of academic literature, and Grey Literature was conducted to gather information on TARGET2 and its stakeholders. Through the literature, stakeholders were identified, ranging from national regulatory bodies to financial institutions that interact with TARGET2.

Analysis of Roles and Functions of Target2 and its relationship with stakeholders:

The roles, services, and functions of TARGET2 were categorized according to the needs and interactions of each stakeholder group identified. This analysis was grounded in socio-technical theory, emphasizing the role of TARGET2 as a socio-technical system within the financial sector.

Assessment of Relationships

The relationships between TARGET2 and its stakeholders were assessed to determine the system's impact on the operational and strategic levels of the financial system.The nature of these relationships was analyzed to understand the dependency of stakeholders on TARGET2's services.

Step 5: Vulnerability Identification

In this step, the thesis employs interpretative analysis to uncover potential vulnerabilities within the TARGET2 system. This method involves an in-depth review of the system's documentation, identifying not only the explicit content but also the implicit risks and weaknesses inferred from the socio-technical interactions described. The analysis draws upon a combination of theoretical knowledge and practical insights into financial systems and IT infrastructure to hypothesize about potential system frailties. It goes beyond surface-level descriptions to analyze how the technical environment, user behaviors, and governance frameworks coalesce, potentially leading to systemic vulnerabilities.

The process involves scrutinizing TARGET2's infrastructure and operational procedures to pinpoint where disruptions could have widespread consequences, assessing user interactions for operational inefficiencies, and evaluating governance alignment with technical capabilities for signs of ineffective management. Communication protocols are examined for potential coordination issues, while the stability of interfaces and networks is reviewed for failure points that could undermine user confidence. Settlement algorithms and risk management practices are interpreted for their adequacy in maintaining transaction integrity and system stability. The culmination of this analysis provides a

nuanced understanding of TARGET2's socio-technical vulnerabilities, highlighting areas for risk mitigation and system enhancement, essential for the system's robust operation and the economic security of the Netherlands.

Step 6: Implications for Economic Security

In this last step, the interrelation between TARGET2 and the Netherlands' economic security is interpreted using the stakeholder functions identified in step 4 and the system vulnerabilities addressed in step 5. The analysis of stakeholder roles and services underscores TARGET2's integral part in the Dutch financial system's operations, highlighting its influence on national economic stability. Concurrently, the vulnerabilities pointed out in step 5, such as technical disruptions and governance misalignments, elucidate potential risks to this stability. Together, these sections paint a comprehensive picture of how TARGET2's functionality and robustness are pivotal to the economic security of the Netherlands, with its ability to manage and mitigate systemic risks being crucial for safeguarding financial continuity and integrity.

3.4 Analytical Approach for Validation using Expert Interviews

Expert interviews provide essential external review to confirm the main findings of our research. However, these interviews, rich in unstructured qualitative information, need careful analysis to extract valuable insights. By grouping similar comments together, we can form a clear picture of the experts' views on different parts of our research, in line with our study's main interests.

This process involves assigning the feedback to relevant validation categories that we've already set based on the experts' areas of knowledge. By comparing where their opinions match and where they differ, we can identify which parts of our research are well-supported or need more examination by specialists. This way, we can keep the full depth of the experts' varied viewpoints without simplifying them too much.

In short, organizing expert feedback by theme helps us systematically incorporate their practical knowledge into our research, enhancing its usefulness without losing our methodological integrity. Grouping these insights helps us filter out specific recommendations to make our findings more applicable, accurate, or relevant. Thus, the interviews provide systematic validation through their qualitative depth. A detailed Interview Protocol can be found in Appendix A.4

In the analysis of expert interviews for this thesis, a systematic approach was adopted to validate various aspects of the TARGET2 system. The methodology was structured to not only confirm the accuracy of previously identified elements but also to uncover new insights and perspectives. The process involved the application of a detailed coding structure using ATLAS.ti, a qualitative data analysis software, to analyse the transcripts of expert interviews. This approach allowed for a nuanced examination of expert opinions and their alignment with the research findings.

3.4.1 Process Overview

1. Transcript Preparation: All expert interviews were transcribed verbatim to ensure a thorough and accurate basis for analysis.
2. Initial Review: A preliminary review of the transcripts was conducted to gain an overall understanding of the experts' viewpoints and to inform the development of the coding structure.
3. Coding Structure Development: Based on the validation objectives of the research, a coding structure was devised. This involved defining specific codes for each objective, such as "Accurate Identification," "Missing Elements," "Observation Alignment," and others.

4. Open Coding: Using ATLAS.ti, the initial phase of open coding was performed on the transcripts. This phase involved assigning codes to relevant segments of text where experts discussed aspects related to the research objectives.
5. Focused Coding: After open coding, focused coding was conducted to categorize and synthesize the initial codes into more substantive themes. This step helped in organizing the data more meaningfully in relation to the research questions.
6. Qualitative Analysis: The coded data were then qualitatively analysed to extract themes, patterns, and insights relevant to the research objectives.

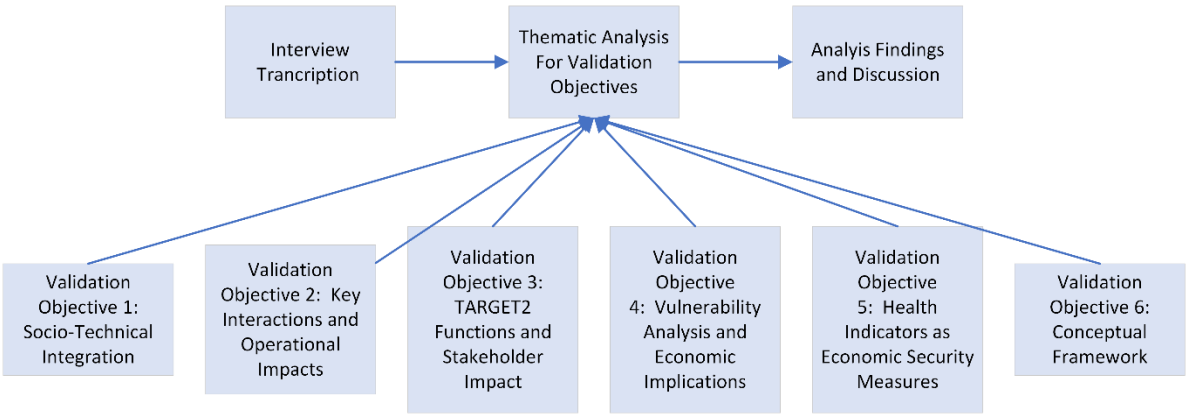

Figure 3-2 Interview Analysis Process

3.4.2 Detailed Coding Process for Each Validation Objective

Validation Objective 1: Socio-Technical Integration

Coding Structure:

- Accurate Identification
- Missing Elements
- Additional Insights

Example Quotes:

"You have accurately captured technical elements like the SSP settlement platform and the TIPS interface." (Accurate Identification)

"The governance structure is missing the Operational Team." (Missing Elements)

Analysis Application:

This approach quantifies expert alignment on identified technical and social components, pinpointing missing elements and gathering additional architectural or procedural details.

Validation Objective 2: Verify Key Interactions and Operational Impacts

Coding Structure:

- Observation Alignment
- Contradictory Operations
- Enriching Perspectives

Example Quotes:

"The core system-user interactions you highlighted reflect what we see in daily operations." (Observation Alignment)

Analysis Application:

This coding confirms if identified socio-technical interactions match expert observances, notes contradictions, and gathers additional perspectives on interaction nuances.

Validation Objective 3: Confirm TARGET2 Functions and Stakeholder Impact

Coding Structure:

- Function Accuracy
- Misaligned Impacts
- Stakeholder Insights

Example Quotes:

"You have correctly highlighted real-time settlement as a key function that TARGET2 provides." (Function Accuracy)

"The impact on corporate treasury operations is not just transaction efficiency but also risk reduction." (Misaligned Impacts)

Analysis Application:

The coding quantifies expert validation on TARGET2 functions, identifies misaligned perceptions of stakeholder impact, and gathers additional insights.

Validation Objective 4: Validate Vulnerability Analysis and Economic Implications

Coding Structure:

- Risk Validation
- Likelihood Assessment
- Severity Evaluation

Example Quotes:

"Technical disruptions are indeed a key vulnerability area." (Risk Validation)

"The likelihood of network issues, in my view, is Possible." (Likelihood Assessment)

"The impact of governance misalignments can potentially be Major." (Severity Evaluation)

Analysis Application:

This coding structure confirms expert alignment on vulnerabilities, assesses their likelihood and severity, and enriches understanding of economic consequences.

Validation Objective 5: Confirm Health Indicators as Economic Security Measures

Coding Structure:

- Indicator Relevance
- Metric Accuracy
- Context Insights

Example Quotes:

"System uptime is definitely a relevant indicator for economic security." (Indicator Relevance)

"The transaction processing accuracy metric correctly signifies the system's operational effectiveness." (Metric Accuracy)

Analysis Application:

The coding assesses the relevance of health indicators, validates technical metric precision, and understands their broader economic implications.

Validation Objective 6: Validate Conceptual Framework

Coding Structure:

- Alignment Confirmation
- Critique and Improvements
- Framework Effectiveness

Example Quotes:

"The dimensions largely resonate with my perspective on TARGET2." (Alignment Confirmation)

"Consider simplifying the framework by consolidating some dimensions." (Critique and Improvements)

Analysis Application:

This approach quantifies expert alignment with the conceptual framework, notes critiques for enhancement, and assesses the framework's effectiveness.

3.5 Ethical Considerations

In our study examining the TARGET2 system, the ethical considerations were adhered to, reflecting the scholarly rigor and commitment to ethical research practices as demonstrated in the entirety of this thesis.

Informed Consent: All participants, especially those engaged in interviews, were comprehensively briefed about the research aims, methodology, and their rights, including the freedom to withdraw at any point. Informed consent was obtained, ensuring voluntary participation under fully transparent conditions.

Confidentiality and Anonymity: Utmost confidentiality and anonymity of participants were maintained throughout the study. Sensitive data was handled with the highest level of security, adhering to strict data protection protocols, ensuring no personal identifiers were disclosed in any publication or report.

Data Handling and Storage: The approach to data management was in strict compliance with current data protection legislation. Detailed procedures were established for the secure storage, access, and eventual disposal of data, emphasizing the safeguarding of participant information against unauthorized access.

Ethical Approval: The research protocol was submitted for and received approval from HREC board, aligning with the ethical standards mandated for research involving human subjects.

Respect for Participants: Our research methodology was imbued with a deep respect for the dignity and rights of all participants. This encompassed not only adherence to legal and ethical guidelines but also a consideration of the impact of our research on participants and the broader community.

Through these comprehensive ethical considerations, it was ensured that the study was conducted with integrity and respect, aligning with the scholarly values and ethical responsibilities that underpin robust academic research.

Chapter 4 Findings from Document Analysis

In the results chapter of this thesis, we dissect the complex socio-technical ecosystem of the TARGET2 system. The study commenced with an extensive document analysis, from which a catalog of social and technical elements intrinsic to TARGET2 was established. These elements were then scrutinized to uncover key interactions, which are posited as the linchpins of the system's success.

These interactions were examined through the lens of their operational implications within TARGET2, highlighting the nexus between social engagement and technical performance. It is within these interactions that the core operations of TARGET2 are executed, serving as conduits to fulfill the system's intended purposes/functions. These functions are not just technical processes but also enablers of social dynamics, ensuring that the system aligns with and supports the requirements of its stakeholders.

Further exploration revealed that the functions derived from the socio-technical interactions are integral to the fulfillment of TARGET2's role within the Dutch financial system. The system's ability to manage real-time gross settlements, maintain liquidity, and ensure the integrity of interbank payments is paramount for the economic security of the Netherlands. The seamless functionality of these operations is crucial in upholding the stability and efficiency of the financial market, thus influencing the broader economic landscape.

The analysis identified vulnerabilities within these socio-technical interactions, recognizing that such weaknesses could pose significant risks to the Dutch economic security. It became evident that disruptions or inefficiencies within the TARGET2 system could have far-reaching consequences, potentially reverberating through the entire financial ecosystem of the Netherlands. These vulnerabilities were categorized based on their potential impact on operations, ranging from transaction delays to compromised data integrity, each with the capacity to erode trust and stability within the financial markets.

The chapter progresses by methodically linking the identified vulnerabilities to their respective stakeholder impacts, mapping out the channels through which economic security could be compromised. In doing so, we delineate a logical progression from the socio-technical foundations of TARGET2 through its operational mechanics to the overarching implications for economic security.

In conclusion, the results presented herein not only underscore the criticality of robust socio-technical interactions within TARGET2 but also articulate the system's indispensable role in safeguarding the economic vitality of the Dutch financial system. The findings serve as a testament to the interconnectedness of social and technical facets within financial infrastructures and their collective significance in national economic security.

4.1 TARGET2's Socio-Technical Elements

This section provides an overview of the socio-technical elements integral to the TARGET2 system, as identified through document analysis. Table 4.1 serves as a guide, enumerating the identified elements integral to the TARGET2 system. This table is instrumental in providing a categorized list of technical and social elements, each playing a pivotal role in the system's operation. As established in our discussion of socio-technical theory in the literature review (section 2.3.3), TARGET2 exemplifies such a system, with deep interdependencies between technical components and social elements. In mapping these components, our analysis helps fill gaps identified in the literature (section 2.4.1) regarding limited focus on explicitly examining TARGET2 as a socio-technical system.

For an in-depth understanding of each element's functionality and relevance, detailed descriptions are provided in the appendix A.1. This comprehensive detailing ensures that the reader can grasp the complexity and nuances of each element and their contribution to the TARGET2 ecosystem. The inclusion of these details in the appendix allows for a focused discussion in the main text while providing a resource for readers seeking more technical or operational specifics.

The technical components listed include the core transaction platforms, the interfaces that facilitate communication between system layers, the networks that underpin connectivity, the applications that manage operations, and the databases that secure transaction integrity. Each of these components is essential for the smooth execution of the system's functions. The identification of these technical elements aligns with the socio-technical framework outlined for TARGET2 (section 2.3.4), validating the relevance of this theoretical framing.

On the social side, the elements encompass the spectrum of users, from direct participants to ancillary systems, the governance structure spanning from the ECB Governing Council to the central banks, and the operational roles that manage daily transaction flows and system oversight. As conceptualized in the broader discussion of socio-technical theory (section 2.3.3), these social components are integral, highlighting the interplay between technical infrastructure and human/organizational elements in systems like TARGET2.

Table 4.1 Identification of Technical and Social Elements (Description in Appendix A.1)

Technical Components	**Social Elements**
Core platforms - SSP (Single Shared Platform) - TIPS (TARGET Instant Payment Settlement) - T2S (TARGET2-Securities)	**Users** - Direct Participants - Indirect Participants - Ancillary Systems
Interfaces - T2SI (T2S Interface) - TIPSI (TIPS Interface) - ASI (Ancillary System Interface)	**Governance Bodies** - Level 1 - The ECB Governing Council - Level 2 - The Market Infrastructure Board - Level 3 - The SSP/TIPS/T2S providing central banks
Networks - SWIFTNet - ESMIG (Eurosystem Single Market Infrastructure Gateway)	**Operational Roles** - Settlement managers - Service desks
Applications - ICM (Information and Control Module) - CRISP (Cost Recovery Information System for Pricing) - GUI (Graphical User Interface)	**Organizational Processes** - Governance - Operations - Testing - Change management

Static Data and Databases - Reference Data - Directories - Account Balances - Transaction Logs	**Communication Flows** - Status updates and notifications - Queries and requests - Broadcasts and circulars - Messaging
Settlement Algorithms	**Operational Procedures** - Normal settlement procedures - Incident response procedures - Contingency/backup procedures
	Governance Rules and Policies - Participation criteria - Access policies - Security controls - Settlement finality rules

4.2 Defining and Identifying TARGET2's Core Operations through Document Analysis

In the context of TARGET2, operations can be defined as end-to-end processes that encompass the entire sequence of activities required to achieve a specific objective within the system. These operations are not just isolated tasks; rather, they represent comprehensive workflows that span from the initiation to the conclusion of a process, integrating various elements of the system's technical and organizational infrastructure.

Understanding these operations is essential to grasp the TARGET2 system's functionality. These end-to-end processes provide the necessary context for any further examination of the system's socio-technical dynamics. This is particularly crucial for TARGET2, where operations are intricately woven with socio-technical elements, forming the foundation upon which the system functions and upon which users, governance, and technology converge.

To identify these comprehensive operations, a detailed document analysis of the Information Guide for TARGET2 users was undertaken. The objective was to extract, from the guide, the quintessential end-to-end processes that define the operational essence of TARGET2. This approach ensured an unbiased and clear comprehension of the system's operational framework, grounded in the specific details provided in the guide.

The analysis revealed several key operations that are central to the functionality of TARGET2:

Transaction Processing and Management: This operation encompasses the entire cycle of payment processing, from the initiation of transactions to their final settlement. It involves steps like transaction execution, real-time settlement, continuous monitoring, and incident management, forming the core workflow of TARGET2.

Risk, Compliance, and Liquidity Management: This operation covers the spectrum from assessing and managing liquidity and risks to ensuring compliance with security standards and integrating robust operational risk controls. It represents a comprehensive process that upholds the system's integrity and stability.

System Governance and Strategic Oversight: Encompassing policy formulation, system oversight, and the execution of strategic roles, this operation outlines the end-to-end process of governing TARGET2, ensuring that it operates within its intended framework and strategic objectives.

Operational Integrity and Business Continuity: This operation involves maintaining system reliability and continuity, including management of transaction interfaces, rigorous monitoring, and performance assessments, ensuring that TARGET2 remains functional and resilient.

Communication and User Interface: This operation focuses on the full spectrum of communication and interaction between the system and its users, ensuring clarity, security, and effectiveness in information exchange.

The identification of these end-to-end operations is a critical step in our analysis, providing a lens through which we can view the socio-technical interactions within TARGET2 (Section 4.3) and explore their operational implications (Section 4.4). Understanding these comprehensive operations is pivotal, as they represent the interconnected workflows that combine to create the operational tapestry of TARGET2.

4.3 Key Socio-Technical Interactions within TARGET2 (Table A.1)

Having established a comprehensive understanding of TARGET2's core operations, we now shift our analytical lens to a critical aspect that underpins these operations: the socio-technical interactions within the system. The significance of these interactions lies in their role as facilitators and enablers of the operational processes we have previously identified. In essence, understanding these interactions is vital because they are the mechanisms through which the operations are effectively realized and managed within TARGET2.

As we discussed in section 2.3.4 of our literature review, our approach is to unravel the intricate weave of social and technical elements using the socio-technical systems framework, specifically tailored for TARGET2. This analysis is key in bridging the gap highlighted in the literature (section 2.4.1) about the limited application of a socio-technical lens in comprehending TARGET2 and its role in economic security.

This section aims to demystify the complex web of relationships connecting the system's infrastructure - encompassing platforms, interfaces, and networks - with the human and organizational dimensions, such as users, governance, and operational roles. These socio-technical interactions are not merely supplementary to the operations; they are integral to their execution, ensuring that TARGET2 functions as a cohesive unit rather than a mere assembly of technical components and user guidelines.

Our exploration, detailed in Table A.1 of the Appendix, delves into how these social and technical aspects synergize to support and enhance the operational functions of TARGET2. The socio-technical systems theory, as outlined in section 2.3.3, provides a valuable framework for this exploration, allowing us to see beyond the technical potential to its practical application in financial operations.

By examining these interactions, we aim to shed light on how TARGET2 achieves its strategic objectives through a harmonious blend of its various elements. This analysis is crucial for understanding the robustness of the financial market TARGET2 serves and aligns with the socio-technical framework's emphasis on identifying vulnerabilities that could arise from the interplay between social and technical components.

Core Platforms and Users Interaction

This interaction is fundamental, as the core processing platforms are the heart of TARGET2, facilitating all payment and settlement processes. The design and functionality of the SSP, TIPS, and T2S must

align with user requirements for efficient financial operations. Users' feedback is crucial for the system's evolution, ensuring that the technical solutions meet their operational needs.

Governance Bodies and Operational Role

Governance bodies set the strategic direction and policies for TARGET2, while operational roles are responsible for the day-to-day management. This interaction ensures that the system operates within the defined regulatory framework and that the technical infrastructure is managed effectively. It's key because it aligns the system's operations with its strategic goals and regulatory requirements.

Communication Flows between Users and Technical Systems

Clear and secure communication channels are essential for the integrity and efficiency of financial transactions. This interaction is key because it ensures that critical information is disseminated accurately and promptly, which is vital for maintaining trust and operational continuity in the financial system.

Interface and Network Reliability Impact on User Operations

Interfaces and networks are the conduits for transaction execution and liquidity management. Their reliability directly affects the users' ability to perform financial operations. This interaction is key as it underpins the operational effectiveness of the entire payment system.

Static Data and Settlement Algorithms Alignment with Governance and Operational Procedures

Accurate static data and effective settlement algorithms are crucial for correct transaction processing. This interaction ensures that the settlement process is fair and efficient, aligning with governance and operational procedures. It is key because inaccuracies or inefficiencies here can lead to financial losses and disputes.

Applications and Operational Procedures

Applications provide the interface through which users interact with TARGET2, and operational procedures dictate how these applications should be used. This interaction is key because it ensures that the system is user-friendly and that the procedures are followed, which is essential for the smooth operation of financial transactions.

Settlement Algorithms and Risk Management

Settlement algorithms determine how transactions are processed, while risk management ensures that operational and financial risks are mitigated. This interaction is key because it directly affects the system's stability and the financial system's resilience to shocks.

User Interaction with Governance Rules and Policies

Users must understand and comply with the governance rules and policies to ensure the integrity of the financial system. This interaction is key because non-compliance can lead to systemic risks and legal issues, potentially compromising the entire system.

Organizational Processes and Technical Reliability

Organizational processes guide the strategic and operational direction, while technical reliability ensures the system's performance and availability. This interaction is key because it ensures that the system remains operational and reliable, which is essential for maintaining confidence in the financial system.

4.4 Operational Implications of Socio-Technical Interactions (Table A.2)

This chapter examines the operational implications of the socio-technical interactions identified within the TARGET2 system. The synergy between the system's technical capabilities and social dynamics plays a crucial role in its day-to-day functions. These functions include settlement processing, liquidity management, and regulatory oversight, which are vital for real-time transaction management and the implementation of monetary policies.

The operational processes are the tangible outcomes of the socio-technical interactions. For instance, the interaction between core platforms and users directly impacts **settlement processing**. The robust infrastructure must facilitate the **rapid processing of transactions**, which is paramount in a real-time gross settlement environment. Users rely on the efficiency and reliability of these platforms to execute financial operations smoothly. Any disruption or inefficiency can have significant repercussions, affecting liquidity management and, consequently, the broader financial market.

Liquidity management, another critical operational process, is influenced by the communication flows between users and technical systems. The ability of users to obtain timely status updates and notifications allows for more informed decision-making regarding liquidity positions. This responsiveness is essential to maintain liquidity levels that meet the requirements of the market and the central bank's policies.

Regulatory oversight is an operational process deeply intertwined with the governance bodies and their interaction with operational roles. The Market Infrastructure Board, together with the ECB Governing Council, defines the regulatory framework within which the system operates. The service desks and settlement managers must ensure these policies are applied consistently and effectively to uphold the system's integrity and compliance.

The effectiveness of these operational processes is contingent upon the real-time management of transactions. The TARGET2 system is designed to provide **immediate finality of payments**, minimizing the risk of settlement failures. This immediacy is a direct result of the well-coordinated interaction between the settlement algorithms and the governance rules, ensuring that transactions are processed accurately and efficiently.

Policy implementation is yet another operational facet shaped by socio-technical interactions. Through these interactions, the TARGET2 system supports the Eurosystem in executing its monetary policy. This support is seen in how the system manages the collateral for central bank credit operations and facilitates the implementation of monetary policy decisions, which are critical for maintaining price stability within the euro area.

In summary, this section highlights how the socio-technical interactions within TARGET2 manifest in operational processes that are integral to the financial ecosystem. These processes are not only vital for the functionality of TARGET2 itself but are also indispensable for the economic security of the jurisdictions it serves. The section emphasizes the importance of these interactions in ensuring the system operates at peak efficiency and reliability, thereby contributing to the overall stability of the financial markets.

4.5 Functions Delivered by TARGET2 to Stakeholders

In Section 4.4, we provide a detailed examination of the functions delivered by TARGET2 to various stakeholders within the Dutch financial ecosystem. This analysis is informed by a comprehensive stakeholder mapping, which identifies the key entities and their interactions with the system. The results are presented in three distinct yet interrelated subsections, each contributing to a holistic understanding of TARGET2's impact on economic security and financial stability.

The first subsection, Results from Stakeholder Mapping in the Dutch Financial Ecosystem, leverages the stakeholder map to outline the intricate web of relationships and dependencies within the ecosystem. Here, we will reflect on the diverse roles of entities ranging from regulatory bodies like the ECB and DNB to commercial banks and individual consumers, and how TARGET2 facilitates and enhances these roles.

In the second subsection, Roles/Services as Functions Performed by TARGET2 for these Stakeholders, we delve into the specific services provided by TARGET2, casting them as essential functions tailored to the needs of the identified stakeholders. This part of the analysis not only describes what TARGET2 does but also emphasizes the significance of these functions for each stakeholder, underscoring the system's versatility and critical importance.

The third subsection, Drivers of Economic Security with Respect to TARGET2 and Economic Security of the Netherlands, focuses on the broader implications of TARGET2's services. It connects the operational functions of TARGET2 to the drivers of economic security, illustrating how the system contributes to the stability and integrity of the financial market and, by extension, to the economic well-being of the Netherlands.

This integrative approach provides a multi-dimensional perspective on TARGET2, revealing how its technical capabilities are interwoven with the economic fabric of society. By referencing the stakeholder analysis and mapping, we aim to provide a comprehensive narrative that captures the essence of TARGET2's role in the financial ecosystem and its contributions to economic security.

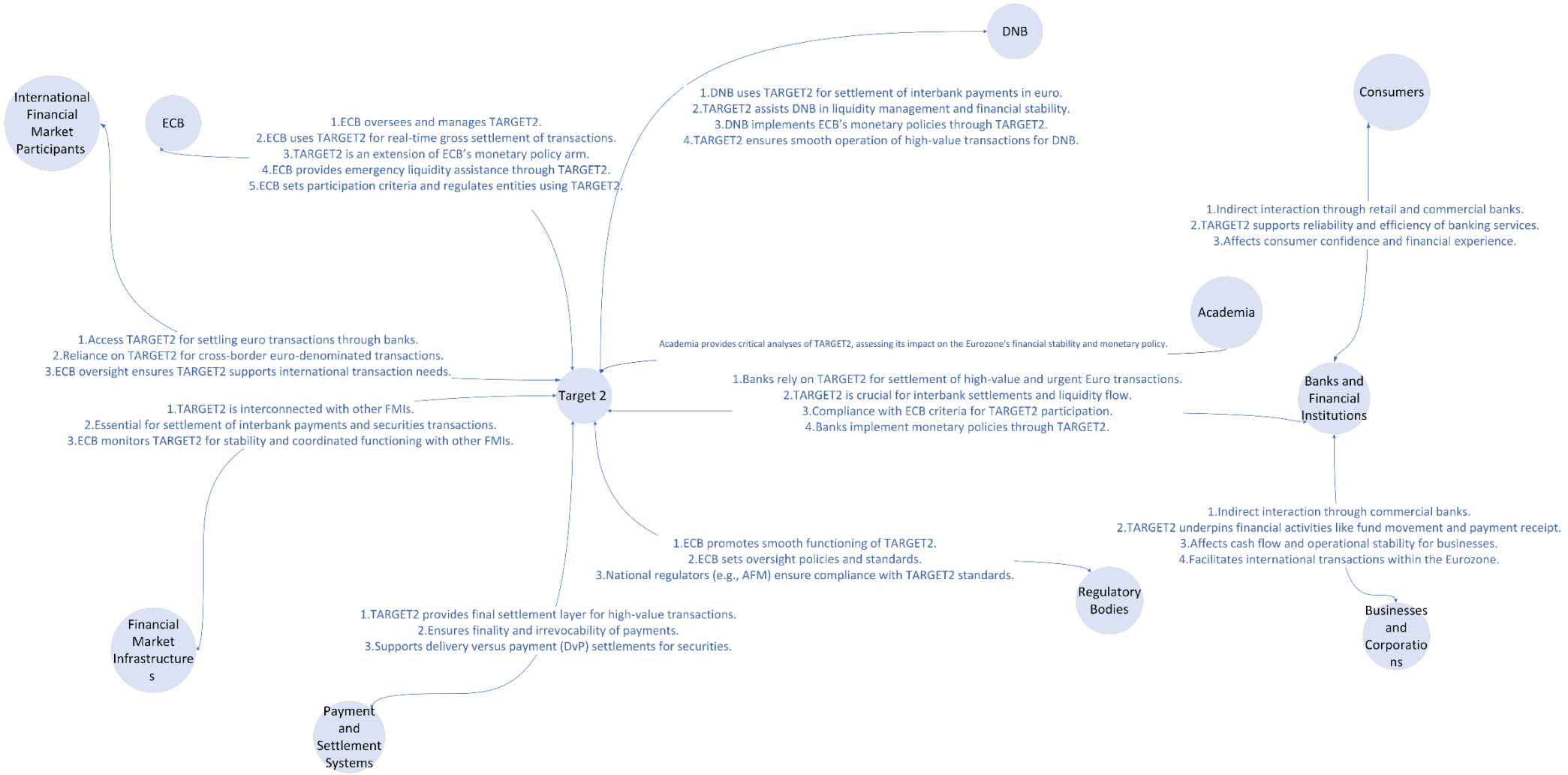

Figure 4-1 Stakeholder Map

4.5.1 Results from Stakeholder Mapping in the Dutch Financial Ecosystem

The stakeholder map of the Dutch financial ecosystem serves as a foundational reference for understanding the roles and interdependencies within the system. It outlines the constellation of entities that directly or indirectly interact with TARGET2 and the nature of their engagements.

Stakeholders such as the **European Central Bank (ECB)** and De **Nederlandsche Bank (DNB)** represent the core regulatory and policy-implementing bodies. TARGET2 serves as an extension of these institutions' operational arms, executing real-time transactions crucial for the Eurozone's monetary stability and policy enforcement. The ECB, in its pivotal role, relies on TARGET2 for its real-time gross settlement operations, which are central to managing liquidity across the Eurozone and implementing monetary policy.

Commercial banks and financial institutions are key operational stakeholders that utilize TARGET2 for interbank settlements. The system's ability to handle high-value transactions efficiently is fundamental to their day-to-day operations, affecting liquidity, credit availability, and ultimately the broader economy.

Businesses and corporations engage with TARGET2 as end-users that benefit from the system's efficiency in transaction processing, which is instrumental in their treasury and liquidity management. This efficiency directly impacts their investment activities and financial operations.

Consumers, while not interacting with TARGET2 directly, are indirect stakeholders whose confidence in the financial system is bolstered by the system's reliability and security. Efficient processing of transactions by TARGET2 ensures that consumer-facing banking services are trustworthy and robust, which is essential for maintaining consumer confidence in the financial infrastructure.

Regulatory and supervisory bodies, such as the ECB and the Authority for Financial Markets (AFM), depend on TARGET2's regulatory oversight functions. The system's compliance and reporting mechanisms support these bodies in their mandate to maintain financial integrity and stability.

The **international financial market participants and financial market infrastructures (FMIs)** use TARGET2 for euro transactions and cross-border settlements, which are vital for the seamless operation of capital markets and the integration of the Dutch financial market with international markets.

Lastly, the Academia, including universities and research institutions, plays an integral role as a stakeholder in the TARGET2 ecosystem. It serves as a center for independent analysis and innovative thinking, contributing significantly to the development and understanding of TARGET2. Academic research offers crucial insights into how TARGET2 impacts central bank balance sheets, its role in the Eurozone's economic integration, and its significance in monetary policy. Furthermore, academic discussions shed light on TARGET2's involvement in broader economic challenges, such as resource allocation and crisis management within the European Monetary Union. Additionally, academia plays a key educational role, shaping the next generation's understanding of and approach to complex financial systems like TARGET2. This not only influences the intellectual discourse surrounding TARGET2 but also plays an indirect yet impactful role in its policy and operational development.

The mapping illustrates how each stakeholder is uniquely served by TARGET2, which is not just a technical platform but a crucial facilitator of financial operations and economic stability. The map underscores TARGET2's integral role in not only supporting the operations of individual entities but also in fostering a coherent and interconnected financial ecosystem. This interplay between

stakeholders and TARGET2 is the bedrock upon which the system's contribution to the Dutch financial ecosystem is built, reinforcing its position as a pillar of economic security.

4.5.2 Roles/Services as Functions Performed by TARGET2 for these Stakeholders (Table A.4)

Stakeholder Mapping

Building on the stakeholder mapping, this subsection delves into the specific roles and services that TARGET2 performs, elucidating how these functions are not just operational features but are custom-tailored to meet the needs of each stakeholder within the Dutch financial ecosystem.

For the **European Central Bank (ECB)**, TARGET2 is the lifeline for operational management. It facilitates the real-time settlement of transactions across the Eurozone, a function that is indispensable for the ECB's management of monetary stability. The system's capability to manage liquidity positions and control money supply is a direct service to the ECB's monetary policy execution.

De Nederlandsche Bank (DNB) leverages TARGET2 for the critical role of liquidity management within the Dutch banking system. By ensuring the efficient settlement of interbank payments, TARGET2 aids DNB in aligning national banking operations with Eurozone-wide policies and standards. This service is pivotal for maintaining the integrity of financial transactions and the overall stability of the Dutch financial sector.

Commercial banks and financial institutions depend on TARGET2 for the settlement of high-value transactions, which is a cornerstone for their interbank settlements and liquidity flow. The system's precision and reliability in processing large volumes of transactions in real time are services that underpin the banking sector's stability. Moreover, compliance with the ECB's criteria, as facilitated by TARGET2, ensures adherence to high standards of technical, operational, and liquidity management.

For businesses and corporations, TARGET2's services extend to facilitating financial operations by underpinning high-value transactions, ensuring transaction finality, and reducing settlement risk. This function boosts confidence in trade and investment activities and supports the corporations' growth and economic activities.

The **consumer** segment, while an indirect beneficiary, relies on the underlying stability and efficiency provided by TARGET2. The assurance of transaction processing, foundational to the reliability of banking services, fosters consumer confidence and influences economic behavior, demonstrating TARGET2's extended service to the public trust.

Regulatory and supervisory bodies are entrusted with the oversight and regulation of the financial market's integrity. Through TARGET2, they are provided with a secure and efficient system that minimizes systemic risk and upholds financial standards—services that are vital for crisis management and maintaining public confidence during uncertain times.

International financial market participants benefit from TARGET2's ability to settle euro transactions essential for global trade. The service provided by TARGET2 in this regard is the facilitation of international economic activities and the seamless integration of capital movement across borders.

Lastly, **the financial market infrastructures (FMIs)** interact with TARGET2 to facilitate the settlement of financial transactions and delivery versus payment in securities settlements. TARGET2's interconnectedness with other systems ensures efficient market processing, a service that maximizes operational efficiency and minimizes systemic risk.

Nested Governance Structure

The extensive stakeholder analysis conducted on TARGET2 has unraveled a Nested Governance Structure, highlighting the complex and layered nature of governance within this critical financial system. This structure depicts how different levels of governance – international, regional, national, and local – are intricately interwoven, each contributing uniquely while remaining interdependent in the broader regulatory and operational landscape of TARGET2.

International Layer:

Global Financial Standard Setters: Organizations like the International Monetary Fund (IMF), the Financial Stability Board (FSB), and the Bank for International Settlements (BIS) play a foundational role in establishing global financial standards. These entities, although not directly overseeing TARGET2, provide the international norms and guidelines that frame its regulatory ecosystem. Their standards on financial stability, risk management, and cross-border financial transactions create a backdrop against which TARGET2 operates.

Influence on Policy and Practices: The policies and best practices developed by these international bodies indirectly shape TARGET2's operational protocols and risk management strategies, ensuring its alignment with global financial principles.

European Union Layer:

Legislative and Regulatory Influence: The European Commission, as the executive body of the EU, crafts the legislative frameworks that impact TARGET2. By developing financial directives and regulations, the Commission sets the legal and regulatory stage within which TARGET2 functions.

Direct Oversight and Alignment with Monetary Policy: The European Central Bank (ECB) holds the pivotal role of directly overseeing TARGET2's operations. The ECB ensures that TARGET2 is not only aligned with the monetary policies of the Eurozone but also adheres to the principles of financial stability and efficiency critical for the entire Eurosystem.

Eurosystem Layer:

Technical and Operational Management: The central banks of the larger economies within the Eurozone, often referred to as the Four Central Banks (4CB), are tasked with the technical management and operational oversight of TARGET2. These banks ensure the system's technical robustness, security, and operational efficiency.

National Implementation and Integration: National central banks, such as De Nederlandsche Bank (DNB) in the Netherlands, play a crucial role in integrating TARGET2 within their respective national financial infrastructures. They ensure that domestic financial institutions are compliant with TARGET2's standards and facilitate the implementation of Eurosystem monetary policies at the national level.

National and Local Layers:

Policy Implementation and Regulation: Local governments and national regulatory authorities like the Authority for the Financial Markets (AFM) in the Netherlands are responsible for the domestic implementation of EU and ECB policies. They ensure that local financial operations are in alignment with TARGET2 standards and the broader regulatory framework set by the European Commission and the ECB.

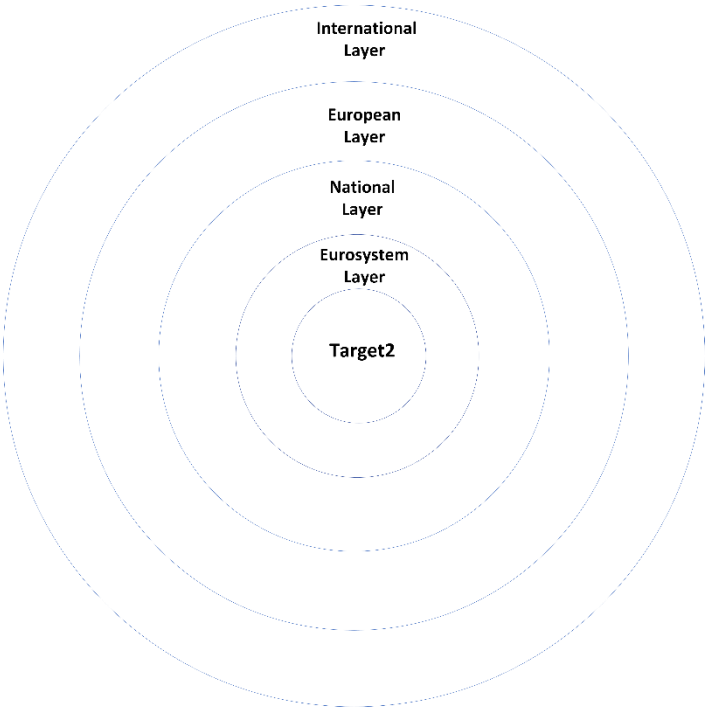

Figure 4-2 Nested Governance Structure

4.5.3 Drivers of Economic Security with respect to TARGET2 and Economic Security of the Netherlands (Table A.5)

This final subsection focuses on the broader economic implications of TARGET2's operations, particularly how it drives economic security within the Netherlands. The roles and services provided by TARGET2 are not only operational functions but also critical components that safeguard the stability and integrity of the Dutch financial system.

The European Central Bank's (ECB) reliance on TARGET2 for real-time gross settlement underlines the system's centrality in ensuring the Eurozone's financial stability. TARGET2's swift and reliable processing of transactions across Europe directly contributes to the efficient execution of monetary policy and the maintenance of financial market integrity. These are key drivers of economic security as they facilitate stable economic conditions, control inflation, and manage interest rates, which are fundamental to the health of the Dutch economy.

For De Nederlandsche Bank (DNB), the management of liquidity is a prime concern, with TARGET2 playing a vital role in ensuring the operational integrity of the Dutch banking system. This function is critical for the stability of the Dutch banking system, as it aligns with Eurozone strategies and compliance with TARGET2 standards, fostering a secure and resilient financial environment.

Commercial banks and financial institutions in the Netherlands depend on the secure and efficient interbank settlements provided by TARGET2. This service is essential for stabilizing the banking sector and ensuring the availability of credit, which in turn supports lending activities and economic growth. By adhering to ECB criteria through TARGET2, these institutions can operate within a trusted framework that upholds financial stability and consumer confidence.

Businesses and corporations benefit from TARGET2's efficient transaction processing and reduced settlement risk, which enhances their ability to engage in trade and investment activities confidently. This confidence in the financial system is a crucial driver of economic security, as it supports business operations and growth, which are key components of a healthy economy.

From a consumer perspective, TARGET2 indirectly supports economic security by ensuring the reliable banking services they depend on. The system's efficiency and security influence consumer confidence and economic behavior, which is vital for the sustained health and growth of the Dutch economy.

Regulatory and supervisory bodies, including the ECB and AFM, utilize TARGET2's stringent oversight and regulation capabilities to minimize systemic risks. In crisis situations, TARGET2's robust framework is instrumental in maintaining market stability and public confidence, key drivers of economic security.

International financial market participants and financial market infrastructures (FMIs) interact with TARGET2 to facilitate efficient cross-border transactions and settlements. This interconnectivity is essential for the Netherlands, as it ensures the country's financial integration with the global market and mitigates risks associated with international financial activities.

By elucidating these roles and services, subsection 4.3 highlights TARGET2's comprehensive impact on economic security. It showcases how the system's functions are integral to maintaining the stability, integrity, and resilience of the Dutch financial landscape, ensuring that the Netherlands remains a competitive and secure player in the global financial market.

4.6 Vulnerabilities and Operational Indicators of Economic Security

4.6.1 Vulnerability in Socio Technical Interactions (Table A.3)

This section delves into the vulnerabilities within the socio-technical framework of TARGET2, evaluating the risks inherent in these interactions. As discussed in section 2.3.4 of the literature review, alterations in the socio-technical dynamics of systems like TARGET2 can influence economic security. This analysis aims to uncover precisely such risks.

These vulnerabilities have the potential to disrupt the operational efficiency of TARGET2 and could have ripple effects throughout the Dutch financial system if not properly mitigated. Section 2.2.3 reviewed academic perspectives on assessing the criticality of infrastructure based on the potential consequences of failure. This discussion aligns with that risk assessment perspective.

Specific vulnerabilities highlighted later in this section, including issues with usability, governance alignment, and communication channels, connect directly to vulnerabilities and risks identified in section 2.4.5 of the literature review. Our analysis provides empirical investigation of these identified risks.

Additionally, section 2.3 positioned socio-technical systems theory as crucial for illuminating points of weakness and interconnectedness related to human, organizational and technical factors. This section applies that theoretical positioning, evaluating vulnerabilities emerging from socio-technical interactions.

In essence, this vulnerabilities analysis firmly aligns with and builds upon the risk- and security-focused discussions in the literature review, providing an evidence-based assessment of potential weaknesses in TARGET2's socio-technical dynamics that could undermine economic stability for the Netherlands.

Core Platforms and Users

Usability Issues: If the system is not intuitive, users may struggle with daily operations, leading to a decline in transactional efficiency and an increase in error rates. In a high-stakes financial environment, these usability issues can significantly delay financial processes, affecting the broader market and eroding user confidence in the system.

Technical Disruptions: TARGET2 operates as a nerve center for critical financial transactions. Any technical disruptions, whether due to system outages or software glitches, can halt or delay transactions. The consequences of such disruptions are severe, potentially leading to substantial financial losses and undermining the stability of the financial infrastructure.

Transaction Processing Bottlenecks: In the high-volume transaction environment of TARGET2, bottlenecks have the potential to cause systemic slowdowns. This can affect not only the efficiency of the payment system but also the timeliness of financial transactions across the market, which could have far-reaching implications for liquidity management and market confidence.

Governance Bodies and Operational Roles

Misalignment Between Governance and Technical Capabilities: A disconnect between the governance policies and the technical capabilities of TARGET2 can lead to mismanaged system operations. This misalignment can hinder the implementation of policies, potentially causing operational challenges that ripple through to end-users.

Ineffective Operational Roles: The effectiveness of operational roles is crucial in maintaining system integrity. Inefficiencies or inadequacies in executing these roles can lead to non-compliance with governance decisions, opening up vulnerabilities related to security risks and potential financial fraud or losses.

Low Compliance Rates: Compliance with governance decisions is a cornerstone of system integrity. Non-compliance can expose the system to various risks, including legal penalties and operational disruptions that may lead to financial losses or fraud.

Communication Flows between Users and Technical Systems

Miscommunication and Coordination Issues: Effective communication is pivotal in complex systems like TARGET2. Miscommunication can lead to misunderstandings and coordination issues among users, potentially disrupting the entire payment process and affecting market operations.

Security Breaches in Communication Channels: The security of communication channels is paramount, given the sensitivity of financial transactions. Any breach could lead to significant data leaks, damaging the confidentiality and integrity of financial transactions and eroding trust in the system.

Underutilization of Communication Systems: If users are not fully engaged with the communication systems, critical updates may be missed. This underutilization can lead to reduced operational efficiency and a lack of synchronicity in system-wide updates or responses to emerging issues.

Interface and Network Reliability Impact on User Operations

Unstable Interfaces and Networks: The stability of interfaces and networks is essential for transaction execution. Instability can lead to transaction failures, causing financial losses and damaging the system's reputation.

High Incident Rates: A high rate of incidents related to network issues can diminish user confidence and lead to a decline in system usage. Such a trend is detrimental, as it may signal underlying vulnerabilities within the network infrastructure.

Negative User Experience: A negative user experience can have far-reaching consequences. Current and potential system participants may be deterred, reducing the reach and impact of TARGET2, and by extension, affecting the overall user base and transaction volume within the system.

Static Data and Settlement Algorithms Alignment with Governance and Operational Procedures

Inaccurate Static Data: Accurate static data is the bedrock of correct transaction processing. Inaccuracies can provoke disputes, incorrect transaction processing, and potential financial losses — all of which threaten the integrity of the financial market.

Inefficient Settlement Algorithms: The performance of settlement algorithms is directly tied to the settlement process's efficiency and fairness. Inefficiencies can induce delays and undermine trust in the system, affecting the timeliness and reliability of settlements.

Misalignment with Governance and Operational Procedures: Any discrepancies between the algorithms, static data, and governance or operational procedures can lead to non-compliance issues, resulting in legal challenges and operational inefficiencies.

Applications and Operational Procedures

Application Usability and Functionality Issues: Applications that are not user-friendly or lack critical functionalities can lead to daily operational inefficiencies. In a system as critical as TARGET2, this can increase the risk of operational failures and affect the system's ability to respond to unexpected events, thus impacting its overall resilience.

Non-Adherence to Operational Procedures: Strict adherence to operational procedures is vital in TARGET2. Deviations from these procedures, especially during high-stress periods or incidents, can amplify the risk of operational failures, potentially causing system-wide disruptions.

Ineffective Applications for Contingency Scenarios: Applications must be robust enough to handle contingencies. If they are not, it may compromise the system's ability to respond effectively to unexpected events or crises, ultimately affecting the stability and reliability of the TARGET2 system.

Settlement Algorithms and Risk Management

Inadequate Settlement Algorithm Performance: Algorithms that are not robust or efficient could lead to delays and inefficiencies in transaction settlement, potentially causing financial instability.

Ineffective Risk Management: The lack of effective risk management strategies may result in unmitigated risks materializing, leading to system disruptions and a loss of confidence among stakeholders.

Poor Integration of Risk Management in Algorithms: Proper integration of risk management principles into settlement algorithms is crucial. Without this, the system could be more vulnerable to emerging threats, compromising the stability and security of the entire financial ecosystem.

User Interaction with Governance Rules and Policies

Lack of Awareness and Unintentional Non-Compliance: Users who are not fully aware of the governance rules and policies might inadvertently violate them, affecting the system's legal and regulatory standing.

Systemic Risks Due to Low Compliance Levels: Low compliance with governance rules can introduce systemic risks, potentially compromising the entire financial system.

Ineffective Governance Communication: Poor communication of governance rules can impede the system's ability to enforce policies and maintain order, leading to operational inefficiencies and vulnerabilities within the financial infrastructure.

Organizational Processes and Technical Reliability

Misalignment of Organizational Processes with Technical Needs: When organizational processes do not align with the technical needs of the system, it can result in increased downtime and inefficiency, hindering the overall effectiveness of TARGET2.

Inadequate System Performance Metrics: Without appropriate metrics to monitor system performance, it becomes difficult to assess and ensure the reliability and availability of the system, which is crucial for continuous operation.

Ineffective Testing and Change Management: Inadequate testing and poor change management practices can leave the system vulnerable to unaddressed issues and outdated practices, affecting its ability to conduct transactions reliably and efficiently.

These vulnerabilities represent key areas where TARGET2's socio-technical interactions could be compromised, leading to a cascade of operational issues. Addressing these vulnerabilities is critical to safeguarding the financial stability and security of the Dutch financial ecosystem.

4.6.2 Identification of Threats Arising from Vulnerabilities in TARGET2

Building upon the previously validated vulnerabilities within the TARGET2 system, we now shift our focus to the identification of specific threats. These threats represent the potential negative outcomes that could materialize if the identified vulnerabilities were to be exploited. It is crucial to establish a clear logical connection between each vulnerability and its corresponding threat to prioritize risk management efforts effectively.

System Component Failures

The vulnerability of outdated or inadequate system components creates a risk for system component failures. This threat materializes when critical parts of the technical platform malfunction, potentially causing payment processing disruptions and settlement delays, directly impacting financial transaction integrity.

Procedural or Operational Failures

Operational vulnerabilities, such as lapses in standard procedures or execution of processes, can lead to procedural or operational failures. This threat emerges from the potential for human error, process inefficiencies, or inadequate control mechanisms, which collectively degrade the system's operational reliability.

External Events

The system's exposure to environmental and external threats is accentuated by vulnerabilities in disaster preparedness and infrastructure resilience. Natural disasters or power outages could exploit these weaknesses, severely disrupting TARGET2’s operational capabilities.

Security-Related Incidents

Vulnerabilities in data security, such as weak encryption or inadequate access controls, can be exploited, leading to security-related incidents. These incidents compromise the confidentiality and integrity of data and communication, threatening the system's reputation and trustworthiness.

Vulnerability to Malicious Code

Software security vulnerabilities offer a gateway for malicious code. The threat of viruses, worms, or Trojan horses infiltrating the system could corrupt data and disrupt operations, undermining the security and functionality of TARGET2.

Unauthorized Access

Weaknesses in authentication and authorization mechanisms can lead to the threat of unauthorized access. This threat is characterized by individuals gaining access to system files and source code without authorization, risking data integrity and potentially leading to malicious activities.

Supplier-Related Security Incidents

The reliance on third-party suppliers introduces vulnerabilities in the supply chain, which can manifest as supplier-related security incidents. These incidents could stem from breaches or failures in the suppliers' infrastructure, impacting TARGET2's service provision.

Participant-Related Events

Vulnerabilities related to participant management and oversight could result in participant-related events. This threat category includes the risks that arise from the actions or operational disruptions of the participants themselves, which could compromise the system's stability.

Cybersecurity Incidents

Inherent vulnerabilities in cybersecurity measures could lead to a range of cybersecurity incidents. This broad threat encompasses hacking, data breaches, and various cyber-attacks, each representing a significant concern for the system's overall security posture.

4.6.3 Operational Indicators of Economic Security

After establishing a link between socio-technical vulnerabilities and economic security threats in the TARGET2 system in Section 4.5, we turn our attention to operational indicators that can serve as quantifiable measures of these vulnerabilities. These indicators not only signify the system's performance but also provide a gauge for the broader economic security of the Netherlands.

Operational Indicators as Reflections of Vulnerabilities:

Each vulnerability identified in the socio-technical assessment of TARGET2 translates to an operational indicator. For instance, usability issues and technical disruptions, which could affect real-time gross settlement and liquidity management, could be measured by indicators such as transaction delay times and system downtime frequencies. These indicators provide tangible evidence of risks to economic security and the efficiency of monetary policy execution.

Governance and Compliance as Economic Barometers:

Misalignments and inefficiencies within governance structures manifest as low compliance rates and governance-policy misalignment metrics. These indicators serve as barometers for the economic security of the financial system, reflecting the ability of the Dutch banking system to maintain stability and confidence.

Communication Integrity and Network Reliability:

Communication flaws and interface instabilities are captured by indicators such as the number of communication failures and network reliability scores. These are critical for ensuring that high-value transactions and securities settlements are conducted without disruption, directly influencing consumer confidence and economic behavior.

Data Accuracy and Algorithmic Alignment:

Inaccurate static data and inefficient settlement algorithms can be measured by the accuracy of transaction data and the performance efficiency of settlement algorithms. These indicators are crucial

for the integration and efficiency of financial markets and FMIs, which underpin the economic security of the Netherlands.

Operational Procedures and Application Effectiveness:

The adequacy of operational procedures and application effectiveness is reflected in operational reliability metrics and the robustness of contingency applications. These indicators are vital for all financial transactions and are indicative of the system's capacity to handle unexpected events, which is essential for the continuous operation of payment systems.

Risk Management and User Compliance:

The effectiveness of risk management strategies and user compliance with governance rules are indicated by the system's ability to withstand financial shocks and the degree of adherence to governance rules. These indicators are significant for the prevention of systemic risks and for ensuring the enforcement of the legal and regulatory framework.

Technical and Organizational Process Alignment:

Finally, the alignment of organizational processes with technical needs is indicated by metrics such as system performance and change management effectiveness. These indicators are crucial for maintaining the system's functionality and, by extension, the economic security of the Netherlands.

Conclusion:

In conclusion, the vulnerabilities within TARGET2's socio-technical framework, as highlighted in Section 4.5.1, are closely aligned with operational indicators that monitor the economic security of the Netherlands. These indicators are critical for understanding the potential impact of socio-technical vulnerabilities on the nation's economic stability and provide actionable insights for system enhancement and policy formulation.

4.7 Impact of Identified Vulnerabilities on Economic Security

The analysis of TARGET2's socio-technical system has identified specific vulnerabilities that, if triggered, could potentially affect the roles, services, and functions that TARGET2 provides to stakeholders within the Dutch financial ecosystem. This section delineates the logical progression from these vulnerabilities to their conceivable impact on the economic security of the Netherlands, highlighting the transmission channels through which these vulnerabilities could cascade into systemic risks.

Vulnerabilities in the socio-technical interactions could directly undermine the functionality of TARGET2, leading to service disruptions. Such service disruptions would then adversely affect the various functions that TARGET2 performs for its stakeholders—ranging from real-time gross settlement and liquidity management for the ECB to the facilitation of high-value transactions for commercial banks. By affecting these critical functions, the vulnerabilities have the potential to propagate through the financial system, thereby impacting the economic security of the stakeholders and, by extension, the economic stability of the Netherlands.

Core Platforms and Users

Usability issues, technical disruptions, and processing bottlenecks could severely impact TARGET2's ability to offer real-time settlement and liquidity management, compromising the ECB’s capacity for

operational management and policy implementation. This could result in inefficient monetary policy execution and regulatory oversight, undermining financial stability and efficiency across the Eurozone, and directly affecting the economic security of the Netherlands.

Governance Bodies and Operational Roles

Misalignments and inefficiencies within governance structures and operational roles may lead to inadequate enforcement of compliance, eroding the robustness of interbank settlements and the execution of monetary policies. This can destabilize the Dutch banking system, hinder commercial banks and financial institutions' lending and economic activities, and ultimately impair the stability and confidence required for a resilient financial sector.

Communication Flows between Users and Technical Systems

Issues such as miscommunication, security breaches, and the underutilization of communication systems can disrupt the final settlement layer for high-value transactions and securities settlements, pivotal to businesses and corporations. This disruption could lead to transactional uncertainty and settlement risks, affecting consumer confidence and the economic behavior essential for a thriving banking system.

Interface and Network Reliability Impact on User Operations

Unreliable interfaces and networks could lead to high incident rates and negative user experiences, thereby diminishing the irrevocability and finality of payments. This could also weaken the settlement of interbank transactions, impinging upon the liquidity management of banks, and by extension, the stability of the Dutch financial ecosystem.

Static Data and Settlement Algorithms Alignment with Governance and Operational Procedures

Inaccurate static data and inefficient settlement algorithms could lead to disputes and financial losses, compromising the efficiency and integration of financial markets which are fundamental to FMIs. Any inconsistency with governance and operational procedures could result in non-compliance, legal challenges, and operational risks, affecting the economic security of the Netherlands.

Applications and Operational Procedures

Non-adherence to operational procedures and ineffective applications could hinder TARGET2's ability to maintain operational reliability and security, vital for all financial transactions. Such deficiencies could result in delays or failures in payment processing, affecting the smooth operation of payment systems and the integration and stability of international financial markets.

Settlement Algorithms and Risk Management

Suboptimal settlement algorithms and inadequate risk management practices can lead to financial instability and loss of confidence in the settlement system. This would jeopardize the seamless operation of payment systems, affecting the economic activities across the international financial market participants and FMIs. The Dutch financial system could suffer from increased systemic risk, with potential global implications given its integral role in international trade and finance.

User Interaction with Governance Rules and Policies

A lack of user awareness and unintentional non-compliance could induce systemic risks, potentially leading to a widespread crisis within the financial system. Poor governance communication could

result in operational inefficiencies, disrupting the legal and regulatory framework's enforcement and undermining the economic security of the Netherlands.

Organizational Processes and Technical Reliability

Misalignment of organizational processes with technical needs could result in system downtime and inefficiency, affecting critical transactions and the overall functionality of TARGET2. This would directly impact the system's performance, reducing its reliability and availability, essential for maintaining confidence in the Dutch financial system.

Chapter 5 Findings from Interview Analysis

This section presents a synthesized overview of insights derived from expert interviews, encompassing themes such as Socio-Technical Integration, Operational Dynamics, Functions Delivered by TARGET2, and the Impact of Vulnerabilities on Economic Security. Each theme is an amalgamation of diverse expert viewpoints, ensuring the retention of their depth while aligning with the established logical framework.

The objective of this section is to validate the research findings using practical knowledge from field experts. The systematic grouping and analysis of interview data not only corroborate the initial research but also provide specific recommendations to enhance its relevance and applicability. The insights extracted from this detailed process significantly contribute to a comprehensive understanding of the TARGET2 system. They affirm the validity of the research findings and highlight areas that merit further exploration and study.

Incorporating these expert perspectives, the section underscores the integration of academic research with practical field knowledge, enriching the overall findings and narrative of the thesis.

5.1 Socio-Technical Integration in TARGET2: An In-Depth Synthesis of Expert Perspectives

The collective insights from the Payment Systems Expert, Policy Advisor, and Financial Economists provide a rich tapestry of analysis on the socio-technical integration of TARGET2, emphasizing the complex interplay between its technical and social dimensions.

The Payment Systems expert lays the foundational understanding of TARGET2 as a socio-technical system. Their affirmation that "looking at TARGET services as socio-technical systems is a good way to look at any business," positions TARGET2 within a broader conceptual framework that transcends traditional technical analysis. They underscore the importance of recognizing the system's dual nature, stating “is of course a technical system. But the most important part...is that it has a purpose” - highlighting its role in facilitating secure bank transactions. This expert's analogy of TARGET2 to an organic, synchronized system sheds light on the delicate balance required between technical infrastructure and social dynamics, illustrating the systemic risks that arise from imbalances in either area.

Building upon this, the Policy Advisor delves deeper into the socio-technical fabric of TARGET2. By differentiating between the technical platforms and the banks as direct users, this expert clarifies the pivotal role of human interaction within the system. They detail the system’s technical configuration, including interfaces and operational procedures, enriching our understanding of its inner workings. The emphasis on human factors as a critical yet vulnerable component, as highlighted in their statement “human interaction is always the weakest link for whatever project or system we talk about," resonates with the need for a balanced socio-technical approach.

The Financial Economist further broadens the narrative by addressing a significant gap in the economic literature concerning socio-technical systems. Their endorsement of a detailed approach, as encapsulated in their remark, "I think it sounds like a very valuable approach that you really go into the details of the different elements and to understand them," validates the research’s thorough exploration of TARGET2. This expert brings to light the limited scope of traditional analyses and acknowledges the socio-technical perspective as one among several valuable lenses for examining complex systems.

The expert views reveals TARGET2 as an intricate socio-technical ecosystem. It is portrayed not just as a confluence of technology and business processes but as an entity where technical efficiency and social purpose are inextricably linked. This comprehensive analysis underscores the importance of an integrated socio-technical lens in capturing the full spectrum of TARGET2's operations and purpose. The experts collectively advocate for a multifaceted approach to understanding TARGET2, one that appreciates the system's technical sophistication while acknowledging the critical role of its social and organizational context. This nuanced understanding is vital for a complete assessment of TARGET2, revealing its operational intricacies and the broader implications for the financial ecosystem it serves.

5.2 Operational Dynamics in TARGET2

The Payment Systems expert provides a pragmatic view of TARGET2's operations, emphasizing the system's automated nature balanced with manual interventions. The expert's statement, "day-to-day is the system is fully automatic...if there's incidents then there is manual interventions," highlights the seamless integration of technology and human oversight. This reflects a coordinated oversight model where technical efficiency is complemented by active human involvement. Further, the expert frames TARGET2 within a business context, describing it as "a business and we have clients and the clients are the commercial banks." This perspective adds a service-oriented dimension to the analysis, focusing on fulfilling stakeholder needs through a blend of social interests and technical capabilities. The expert also mentions, "there is a whole cascade of testing phases which is usually manual work," pointing to the process behind technical upgrades and the integration of these upgrades with essential social elements like user preparedness and policy guidance.

The Policy Advisor explores TARGET2's various operational responsibilities, including settlement processing, liquidity monitoring, and regulatory oversight. They shed light on the system's components, such as collateral management platforms and risk mitigation applications, which underpin these processes. The expert discusses how socio-technical dynamics directly influence operational effectiveness, with efficient communication protocols playing a key role in the system's functionality. However, they also point out the vulnerabilities inherent in such a system, citing instances of technical glitches and miscommunication that can compromise operations. The Policy Advisor's statement about past incidents, "database access failures temporarily stalled auto-collateralization sweeps," and coordination issues around participant notification chains underscore the risks associated with the interplay of people and system interactions.

The Financial Economist highlights the critical operation of settlement within TARGET2, asserting its central role in the system's functionality. They state, "Settlement is really at the essence of Target2," underscoring its importance in executing system operations and its critical implications in facilitating transactions. This emphasis on settlement positions it as a foundational operation, central to TARGET2's socio-technical configuration. The expert acknowledges the complexity of roles in the system, suggesting that while settlement is a core function, other mechanisms also contribute significantly to operations like liquidity management.

Combining these insights presents a comprehensive view of TARGET2's operational dynamics, where technical automation, human intervention, and business-oriented service delivery are intricately interwoven. The Payment Systems expert's focus on the automated yet responsive nature of the system, the Policy Advisor's detailed exploration of operational responsibilities and the associated risks, and the Financial Economist's emphasis on the centrality of settlement function, collectively illustrate a complex operational ecosystem. This integrated perspective reveals TARGET2 as a system where technical efficiencies are harmonized with socio-technical interactions, highlighting its critical

role within the financial ecosystem and the importance of robust operational management to ensure its stability and effectiveness.

5.3 TARGET2's Functions and Their Impact on Stakeholders

The insights from the Payment Systems , Policy Advisor, and Financial Economists collectively provide a nuanced understanding of the diverse functions delivered by TARGET2 and their significant impact on various stakeholders in the financial ecosystem.

The Payment Systems expert's perspective offers a focused view of TARGET2's primary function in the realm of interbank funds transfers. They succinctly state, “TARGET2 in effect only does one function...transferring money funds from one account to the other,” highlighting the system's streamlined efficiency in executing secure bank transactions. This perspective is enriched by the expert's analogy of “a whole Christmas tree of correspondent banking relations,” which vividly illustrates TARGET2's role in simplifying and systematizing intricate funds transfer arrangements between banks. This metaphor not only conveys the complexity of banking relations but also underscores TARGET2's value in bringing clarity and efficiency to these processes through its technological and oversight capabilities.

Complementing this, the Policy Advisor broadens the scope, delving into TARGET2's role in facilitating liquidity management. They clarify, "Liquidity management is not a function of target 2 but the liquidity management function of banks is really helped and supported by Target 2,” thereby underscoring the system's supportive role in enhancing banking operations. The expert further expands on the range of ancillary functions facilitated by TARGET2, including settlement processing, regulatory oversight, and policy implementation. This breadth of functionality underscores TARGET2’s extensive reach as a facilitator of critical financial workflows, deeply embedded within the wider socio-economic fabric. The Policy Advisor's insights reveal how TARGET2's operations impact not only the internal mechanisms of financial institutions but also extend to influence commercial banks, consumers, and broader continuity in the financial sector.

The Financial Economist, meanwhile, emphasizes the foundational role of settlement in TARGET2, stating, "Settlement is really at the essence of Target2...it's fundamental." This assertion places settlement at the core of TARGET2’s operations, highlighting its critical role in facilitating transactions across the financial landscape. The expert also points to the complexities surrounding TARGET2's involvement in liquidity management and monetary policy transmission, noting areas that require deeper exploration. Their remarks on the interconnectedness between TARGET2's operations and broader functions, such as monetary policy signaling by the ECB, uncover layers of complexity and interdependencies that are crucial to understanding the system’s full impact.

In synthesizing these expert perspectives, TARGET2 emerges as a multifunctional system central to the financial ecosystem. It is portrayed not just as a facilitator of high-value transaction settlements but also as an integral component supporting a range of banking operations and contributing to financial stability and economic security. The system's role goes beyond mere transaction processing, encompassing critical aspects of regulatory oversight and policy implementation, thus influencing a broad spectrum of socio-economic activities. This comprehensive analysis underlines the importance of TARGET2 in the financial landscape, highlighting its pivotal position in ensuring smooth monetary transactions and effective financial management across multiple levels of the financial ecosystem.

5.4 Analysing Vulnerabilities within TARGET2's Socio-Technical Framework

The collective insights from the Payment Systems Expert, Policy Advisor, and Financial Economist offer a nuanced understanding of the vulnerabilities inherent in TARGET2's socio-technical framework, highlighting the multifaceted nature of risks and the critical role of resilience.

The Payment Systems expert provides a calibrated assessment of vulnerabilities, acknowledging the varying likelihood and impact of different threats within TARGET2. Their analysis underscores that "Technical disruptions are quite likely. Usually impact is usually low...but it can be high as well," reflecting a balanced perspective that recognizes infrastructural risks while emphasizing the importance of mitigating protocols. This approach is crucial in understanding the complex risks stemming from socio-technical asymmetries, especially in crisis situations that lead to "miscommunication and misalignment." The expert's insights into these vulnerabilities offer a clear pathway to tracing system perturbations back to coordination deficiencies between interdependent components, thus evolving the theoretical arguments around financial stability. Importantly, the focus is not solely on vulnerabilities but also on the system's resilience, with a note that security breaches are "very unlikely" due to robust protection mechanisms.

Complementing this view, the Policy Advisor sheds light on communication as a significant problem area, arising from complex human coordination needs within TARGET2. They note, "the biggest problems were all in the field of communication about informing not informing everybody," pinpointing the human element as a critical vulnerability. Additionally, the expert highlights the risks posed by technical disruptions in databases and interfaces, which can lead to significant operational challenges. The evolving threat of authorization management, necessitating constant updates to access controls, is also underscored, particularly in the context of mitigating risks like social engineering. This analysis extends the understanding of vulnerabilities, emphasizing both human and technical aspects and their interplay in creating risks within the system.

The Financial Economist adds a broader dimension by identifying significant political risks, particularly the potential impact of a Eurozone member country's decision to exit. Their statement, "when one country decides to leave the euro...that can lead to really stress in the system and even lead to a collapse," illuminates the interconnected nature of the Eurozone's financial systems and the profound implications of political decisions on TARGET2. This perspective goes beyond mere financial losses, underscoring the systemic nature of the risks involved and the potential for cascading effects across the European financial fabric.

A comprehensive picture of TARGET2's vulnerabilities emerges from the experts' perspectives. The insights reveal a system where operational, technical, human, and political factors intertwine, creating a complex landscape of risks that require a multifaceted approach to management and mitigation. The emphasis on both preventive resilience and effective response strategies highlights the need for a comprehensive approach to safeguarding economic security and ensuring the system's stability. This analysis underscores the importance of considering all dimensions of vulnerabilities within TARGET2's socio-technical framework, from the operational level to the broader socio-political context, to effectively anticipate and manage potential risks and disruptions.

5.4.1 Risk Assessment

Vulnerability Severity Analysis

The robustness of financial transaction systems is paramount to maintaining the integrity and stability of modern economic structures. This section presents a detailed risk assessment of the TARGET2

system's vulnerabilities, which were elucidated through a methodical analysis of documentation and bolstered by insights gathered from interviews with domain experts.

Through engaging with seasoned policy advisors and payments systems expert, this study has illuminated the likelihood and impact of various vulnerabilities that were initially identified in the document analysis phase. The interplay between these two dimensions—likelihood and impact—forms the crux of the vulnerability severity analysis, providing a nuanced view of the potential risks. The likelihood and impact matrices are presented in table 5.2. The table also includes a resultant/ synthesized matrix that combines the risk assessment from both the experts.

The ensuing discourse synthesizes the expert opinions into a comprehensive risk matrix. This matrix serves as a strategic tool to prioritize vulnerabilities based on the severity of their potential impact and the probability of their occurrence. It reflects a consensus on certain vulnerabilities that experts agree pose a significant risk to the system, as well as divergences that highlight areas requiring heightened attention or further investigation.

This assessment is instrumental in guiding the strategic allocation of resources toward mitigating the most critical risks and fortifying the system against potential vulnerabilities. By integrating expert judgments, the analysis ensures that the identified vulnerabilities are not only theoretically grounded but also validated through professional experiential knowledge, culminating in a robust and actionable risk mitigation strategy.

Table 5.1 Likelihood and Intensity of Impact of vulnerabilities

	Impact / Likelihood	Rare	Unlikely	Possible	Likely	Almost Certain
Policy Advisor	**Catastrophic**					
	Major	E, F, G, I, N, S, T	D, M	C, H, R		
	Moderate	B, J, K, L, O, P, U	A, Q			
	Minor					
	Insignificant					
Payment Systems Expert	**Catastrophic**					
	Major	I, R, S, T	G, H, M		A, O	
	Moderate		K, P, U			
	Minor	B		D, F	C	
	Insignificant	E, L, N	J			
Synthesized Matrix	**Catastrophic**					
	Major	I, S, T	G, H, M, R		O	
	Moderate				A	
	Minor	E, N	B, D, F, J, K, L, P, Q, U		C	
	Insignificant					

Table 5.2 Legend for Vulnerabilities

List of Vulnerabilities	Code
Technical Disruptions	A
Transaction Processing Bottlenecks	B
Unstable Interfaces and Networks	C
Inaccurate Static Data	D
Misalignment Between Governance and Technical Capabilities	E
Ineffective Operational Roles	F
Low Compliance Rates	G
Miscommunication and Coordination Issues	H
Security Breaches in Communication Channels	I
Underutilization of Communication Systems	J
Usability Issues	K
Negative User Experience	L
Lack of Awareness and Unintentional Non-Compliance	M
Inadequate Settlement Algorithm Performance	N
Ineffective Risk Management	O
Poor Integration of Risk Management in Algorithms	P
Non-Adherence to Operational Procedures	Q
Ineffective Applications for Contingency Scenarios	R
Ineffective Testing and Change Management	S
Misalignment of Organizational Processes with Technical Reliability Requirements	T
Inadequate System Performance Metrics	U

The synthesized Risk Matrix presented here offers an integrated view of risk assessments from two different experts. The synthesis is attained by erring on the side of caution which means that between the two inputs from the two experts for likelihood and impact, the score which represents higher probability or higher impact is chosen. It is designed to help prioritize risks based on the likelihood of occurrence and the potential impact on the system. Here is an interpretation of the table:

Catastrophic Impact: There are no vulnerabilities assessed as having a catastrophic impact by either expert. This suggests that, while there are significant risks, none are expected to be systemically catastrophic under the current analysis.

Major Impact:

Vulnerabilities Security Breaches in Communication Channels, Ineffective Testing and Change Management, and Misalignment of Organizational Processes with Technical Reliability Requirements have been identified as having a major impact with a rare likelihood of occurrence. These represent significant risks that are not expected to happen often but would have serious consequences if they did.

Vulnerabilities Low Compliance Rates, Miscommunication and Coordination Issues, Lack of Awareness and Unintentional Non-Compliance, and Ineffective Applications for Contingency Scenarios are also assessed to have a major impact but are considered unlikely to occur. These might represent areas where risk mitigation could be targeted to reduce their likelihood even further.

Vulnerability Ineffective Risk Management is deemed likely to have a major impact, indicating a high-priority risk that warrants immediate attention.

Moderate Impact:

Vulnerability Technical Disruptions is seen as likely to have a moderate impact. This risk is viewed as something that could occur with reasonable frequency, but the consequences would be manageable rather than severe.

Minor Impact:

A cluster of vulnerabilities (Transaction Processing Bottlenecks, Inaccurate Static Data, Ineffective Operational Roles, Underutilization of Communication Systems, Usability Issues, Negative User Experience, Poor Integration of Risk Management in Algorithms, Non-Adherence to Operational Procedures, Inadequate System Performance Metrics) are assessed as unlikely to happen but would only have a minor impact if they did. These are lower priorities compared to those with major impacts.

Vulnerability Unstable Interfaces and Networks is rated as likely to occur with a minor impact, suggesting a frequent but not particularly damaging issue that requires routine management rather than urgent action.

Vulnerability Misalignment Between Governance and Technical Capabilities and Inadequate Settlement Algorithm Performance, while assessed as having a minor impact, are rare and therefore might be deprioritized in favor of addressing risks with greater likelihoods or impacts.

Insignificant Impact: No vulnerabilities are identified in the combination of high likelihood and insignificant impact, which would indicate frequent occurrences with negligible consequences.

This matrix illustrates a risk landscape where the most critical vulnerabilities to address are those with a likely occurrence and major impact, as they pose the most immediate and significant threat to the system. Vulnerabilities with major impacts but lower likelihoods are still serious but may be addressed with longer-term strategies. Minor impacts are less of a concern but should not be ignored, as they may still affect system performance or user experience. The absence of catastrophic risks may indicate that while the system has vulnerabilities, there are no single points of failure that would result in total system collapse.

Analytical Interpretation of Target2's socio-technical vulnerabilities

It emerges from the analysis that TARGET2 is enmeshed in a complex interplay of technical robustness and human-oriented operational challenges. The vulnerabilities identified—ranging from user interface issues to governance misalignments—are indicative of a system where technical infrastructure is deeply intertwined with human operational dynamics. Significantly, these vulnerabilities are not static entities but evolve in response to the system's adaptive engagements with user feedback and operational exigencies. This dynamic nature of the vulnerabilities underscores the necessity of a resilient framework capable of iterative refinement.

Expert evaluations, contextualizing the likelihood and impact of these vulnerabilities, reveal a landscape wherein high-impact risks are balanced against their lower occurrence probability. For instance, the potential for security breaches in communication channels, though rare, necessitates vigilant safeguards due to their substantial impact. Conversely, technical disruptions, while more frequent, are perceived as less impactful, suggesting a need for routine, yet robust, management protocols.

This nuanced risk matrix serves not merely as a theoretical construct but as a strategic blueprint for prioritizing system enhancements. It propels a bifocal approach wherein immediate resources are allocated to fortify the system against high-severity vulnerabilities, irrespective of their lower likelihood. Simultaneously, it advocates for an ongoing refinement process to mitigate more frequently occurring risks, even if their individual impact is moderated.

The analysis further accentuates the significance of governance and communication as pivotal in mitigating risks. It becomes evident that vulnerabilities are exacerbated when the human element—manifested through miscommunication or coordination lapses—is not adequately addressed. Therefore, a systemic approach that transcends technological fixes and encompasses procedural and policy reforms, coupled with human capacity building, is imperative.

Remarkably, the absence of vulnerabilities with catastrophic impact reflects a system that, despite its complexity, is resistant to complete systemic failure. However, it is important to note the systemic interdependencies, particularly the profound implications of macro-political events, such as a Eurozone member's exit, which could trigger cascading effects across the financial landscape.

In conclusion, the TARGET2 system embodies a robust yet intricate architecture with multifaceted vulnerabilities requiring a comprehensive risk management strategy. This strategy must integrate the socio-technical facets of the system and leverage expert insights to preemptively curtail potential disruptions. The inclusion of user feedback mechanisms not only exemplifies the system's adaptability but also highlights the role of users as pivotal stakeholders in the evolutionary trajectory of TARGET2's socio-technical framework.

Threat Severity Analysis

In the preceding chapters, we have identified and validated the array of vulnerabilities inherent within the TARGET2 socio-technical system. Building upon this foundation, this chapter transitions into a critical examination of the severity of potential threats. This threat severity analysis is instrumental in quantifying and qualifying the risks, thereby enabling the formulation of a calibrated risk management strategy. The analysis is anchored in the creation of a threat severity matrix—a tool that categorizes each threat by its likelihood of occurrence and the magnitude of its potential impact.

The threat severity matrix serves as a pragmatic guide for risk prioritization, informing the strategic direction of TARGET2's risk mitigation efforts. By assessing the threats against two critical dimensions—likelihood and impact—the matrix illuminates the areas where resources and attention should be concentrated to bolster the system's defenses and maintain its integrity.

Table 5.3 Threat Severity Analysis

Impact / Likelihood	Rare	Unlikely	Possible	Likely	Almost Certain
Catastrophic					
Major		System Component Failures, Procedural or Operational Failures, Vulnerability to Malicious Code, Unauthorized Access	External Events, Security-Related Incidents, Cybersecurity Incidents		
Moderate		Participant-Related Events	Supplier-Related Security Incidents		
Minor					
Insignificant					

With the expert-informed threat severity matrix before us, we now turn to unpack the practical significance of each threat category. The insights from a policy advisor enrich our analysis, bridging the gap between abstract risk assessment and tangible mitigation planning.

Here is an analytical interpretation of the matrix:

Major Impact and Unlikely Likelihood:

System Component Failures, Procedural or Operational Failures, Vulnerability to Malicious Code, and Unauthorized Access: These threats are considered to have a 'Major' impact, meaning their occurrence could cause significant disruption to TARGET2's operations and compromise the system's integrity. The 'Unlikely' likelihood suggests these are not expected to happen frequently under normal circumstances. However, due to their high impact, they warrant considerable attention in the system's risk management plan, with robust mitigation strategies and contingency plans.

Major Impact and Possible Likelihood:

External Events, Security-Related Incidents, and Cybersecurity Incidents: These threats are not only severe in their consequences but also more probable than the previously mentioned ones. They require an active and layered defense mechanism, including both preventive measures and rapid response plans. Given their 'Possible' likelihood, these threats should be part of regular risk assessment exercises, ensuring that the system's resilience is maintained and that stakeholder awareness is heightened.

Moderate Impact and Possible Likelihood:

Supplier-Related Security Incidents: This threat has a 'Moderate' impact and a 'Possible' likelihood, indicating that while the threat is not as severe as those in the 'Major' category, it is still likely enough to occur that it cannot be ignored. Effective supplier risk management and due diligence are vital, as well as ensuring that suppliers' security practices align with TARGET2's standards.

Moderate Impact and Unlikely Likelihood:

Participant-Related Events: These threats are less likely to occur but could still have a moderate impact on TARGET2's operations. This suggests a need for clear communication protocols and rigorous training for all participants to minimize the risk of such events. It also underlines the importance of regular audits and compliance checks to reinforce adherence to operational procedures.

Analytical Interpretation of Threats

The distribution of threats across the risk matrix indicates a concentration in the 'Major' impact category, which underscores the critical nature of TARGET2 as a financial infrastructure. The absence of threats in the 'Catastrophic' impact category is a positive indicator of the system's underlying strength and existing risk controls. However, the presence of several threats in the 'Major' impact category with a 'Possible' likelihood requires ongoing vigilance.

Furthermore, the matrix reveals that while some threats are less likely to occur, the consequences of such events would still be significant, justifying the need for a proactive risk management approach. The existence of threats with a 'Possible' likelihood across both 'Major' and 'Moderate' impact categories calls for a dynamic and adaptive risk management framework capable of addressing both imminent and potential risks.

In conclusion, the analysis of this risk matrix should inform the prioritization of TARGET2's risk mitigation efforts. While the system exhibits robustness against the most severe threats, the identified risks demand a structured approach to risk management that includes both prevention and response mechanisms. The goal should be to reduce the likelihood of these threats materializing and to minimize their impact should they occur, thereby ensuring the continued stability and reliability of TARGET2.

5.5 Impact of Vulnerabilities on Economic Security

The insights from the Payment Systems , Policy Advisor, and Financial Economists provide a detailed understanding of the impact of vulnerabilities in TARGET2 on economic security, emphasizing the depth of risks and the need for robust resilience mechanisms.

The Payment Systems expert discusses the significant economic risks associated with settlement disruptions in TARGET2, noting the potential for banks to require central bank support during downtimes. They state, “banks may get into trouble” necessitating “central bank support” in such scenarios. This highlights systemic stability threats, with individual bank well-being heavily reliant on the infrastructure's integrity. The expert further elaborates on the challenges of settlement inoperability in treasury management and balance reporting, creating a direct link between technical deficiencies and enterprise-level operational paralysis. The impact of overnight batch processing on crucial functions such as billing, accounting, and regulatory reporting is underscored, tying system outages to a wide range of organizational outcomes. Additionally, the loss of settlement finality eroding liquidity transparency is highlighted, pointing to potential market structural degradations and magnifying risks like transaction counterparty exposures.

The Policy Advisor addresses both contained and cascading impacts of vulnerabilities, emphasizing immediate reconciliation issues for banks and broader systemic risks affecting trade flows and financial markets. They caution, “vulnerabilities typically manifest as operational disruptions though second-order effects can rapidly emerge.” The expert describes scenarios where problems occurring on a Monday might only be solved overnight, leading to significant balance issues for consumers or companies by the next morning. This emphasizes the importance of swift response protocols and acknowledges that downstream processes can still experience turbulence. The expert also observes that if “[databases] are really destroyed,” the impact would be significantly larger, underscoring the systemic implications of integrity compromise.

The Financial Economist outlines the severity of risks from potential vulnerabilities in TARGET2, focusing on system-wide impacts beyond isolated financial losses. They note the criticality of political decisions, stating, “when one country decides to leave the euro...that can lead to really stress in the system and even lead to a collapse.” This underscores the interconnected nature of the Eurozone’s financial systems and the profound implications of such political changes. The expert also highlights that persistent operational issues could accelerate migration to alternate systems like cryptocurrencies, revealing how trust erosion can lead to significant shifts in the financial landscape. They emphasize that these vulnerabilities, while appearing as isolated occurrences, carry the capacity to rapidly transform economic structures.

Combining these insights, a comprehensive picture emerges of the vulnerabilities within TARGET2 and their potential to impact economic security significantly. The Payment Systems expert's focus on operational repercussions, the Policy Advisor's emphasis on the systemic risks arising from vulnerabilities, and the Financial Economist's highlighting of political and trust-based risks collectively underscore the multifaceted nature of these threats. This analysis illuminates the critical need for a

proactive and agile approach to resilience, aiming to safeguard economic security by anticipating and managing the complex shifts that stem from systems failure within the financial ecosystem.

5.6 Operational Indicators and Economic Security Impact in TARGET2

The Policy Advisor discusses the challenges in measuring comprehensive metrics within TARGET2, particularly due to its structure that spans both localized databases under decentralized control and collective components across jurisdictions. This complexity is highlighted by the observation that while in-country systems allow for more direct control and monitoring, the visibility of collective elements remains more obscured. The expert notes the inherent constraints in evaluating TARGET2's performance from a system-wide perspective, emphasizing the need for a multi-layered approach to assessment. This includes considering both the operational intricacies of localized systems and the broader implications of cross-system reliance. The Policy Advisor's insights underscore the importance of layered social and technical assessments in understanding TARGET2's operational health, advocating for a more comprehensive approach beyond reliance on quantitative metrics alone.

The Financial Economist affirms the use of vital operational metrics that provide valuable insights into TARGET2's management and potential economic impact. Their discussion extends to the multi-faceted concept of economic security, emphasizing the importance of foundational infrastructure resilience. The expert aligns with the notion that economic security within complex systems like TARGET2 should be viewed through the lens of "resilience of vital systems against vulnerabilities and threats." This perspective underscores the critical role of resilience in maintaining the system's stability and ensuring its capacity to withstand various threats. Furthermore, the Financial Economist elaborates on the far-reaching impact of vulnerabilities in TARGET2, noting that significant political changes or systemic operational issues could lead to widespread instability and potentially trigger shifts towards alternative systems like cryptocurrencies. Such insights highlight the interconnectedness of financial systems and the cascading effects that disruptions in TARGET2 could have on the broader economic landscape.

The insights from the Policy Advisor and Financial Economists offer a nuanced understanding of TARGET2's operational indicators and their impact on economic security emerges. The Policy Advisor's emphasis on the complexities of comprehensive assessment and the need for a comprehensive evaluation approach highlights the challenges in fully capturing TARGET2's operational health. The Financial Economist's focus on resilience and the systemic implications of vulnerabilities in TARGET2 brings to light the broader economic risks and the importance of maintaining robust infrastructure to support financial stability. Together, these perspectives underscore the necessity of a multifaceted approach to monitoring and managing TARGET2, one that considers both the operational specifics and the wider socio-economic context in which the system operates. This approach is vital for ensuring the system's resilience and safeguarding the economic security of the broader financial ecosystem.

5.7 Mitigation Strategies

In the endeavour to fortify TARGET2 against its identified vulnerabilities, theoretical insights must be translated into concrete actions. The vulnerabilities at the heart of this discussion—namely, Unstable Interfaces and Networks, Miscommunication and Coordination Issues, along with Ineffective Testing and Change Management—embody significant socio-technical asymmetries. These asymmetries highlight a misalignment between the system's social and technical dimensions, which, if neglected,

could significantly compromise the effectiveness and dependability of this essential financial infrastructure.

In the course of this thesis, consultations with experts have yielded profound insights into the gravity of these vulnerabilities. Yet, there has been a conspicuous silence on actual incidents, a void effectively bridged by the illuminating Deloitte report, commissioned by the European Central Bank (ECB) following the system crashes in 2020 (Deloitte, 2021). This document, emerging from thorough analysis, provides a practical perspective on the theoretical vulnerabilities previously identified. The alignment between the socio-technical gaps we have deduced and the deficiencies documented in the report is not coincidental but rather validates the precision of the initial assessments.

Armed with the clarity provided by this comprehensive report, and informed by the risk prioritization articulated through the heat map(severity analysis), we direct our focus towards the trio of vulnerabilities identified as one of the most critical ones. This focused approach does not negate the importance of other potential risks but creates a template for future exploration.

Subsequent sections of this chapter will explore the detailed mitigation strategies designed to address these vulnerabilities. Each proposed strategy is grounded in a dual commitment: firstly, to socio-technical optimization, aiming to realign the interaction between human factors and technical systems; and secondly, to the application of a risk management framework that ensures our recommendations are not only robust and actionable but also in harmony with the operational dynamics of TARGET2.

By embarking on this targeted and strategic path, we endeavour to not only address the immediate vulnerabilities but also to contribute to the long-term resilience and security of TARGET2. Through the integration of socio-technical principles and a rigorous risk management framework, we aim to bolster the infrastructure against future challenges, ensuring its stability and reliability as a cornerstone of the European financial landscape.

Unstable Interfaces and Network Issues (C)

In the report, one of the critical incidents discussed was due to unstable interfaces, particularly the mismatch in the message-schema between TARGET2 and T2S, which caused service disruptions. This incident underscores the vulnerability within the system where interface instability can lead to significant operational challenges.

In the context of network stability, the report also identified network issues as a root cause of service disruptions, which corresponds to the "Unstable Interfaces and Networks" vulnerability we have pinpointed. The instability in this area not only affected the immediate functionality of the TARGET2 system but also had a ripple effect on the connected services, demonstrating the interconnected nature of the system's infrastructure.

The convergence of these points from the Deloitte report with our identified vulnerability of "Unstable Interfaces and Networks" underscores the critical need to address this area. It validates the importance of focusing our mitigation strategy on enhancing the robustness and reliability of the system's interfaces and networking components to prevent similar occurrences in the future.

Recommendations in the report

Standardization and Transparency in Monitoring: The report advises standardizing the monitoring process for the TARGET2 and T2S systems across all infrastructure, platform, and application layers. This would involve developing a comprehensive monitoring framework that ensures all critical components are under continuous surveillance for stability and performance.

Central Asset Inventory Database: It recommends that all inventories relevant to the TARGET Services, including Configuration Items (CIs), be captured in a centralized asset inventory database. This database should document the dependencies between services and CIs, which is essential for timely recognition of the impact on TARGET Services in the event of an incident.

Clear Assignment of Asset Ownership: Critical IT components that comprise the TARGET Services should be assigned to clearly identifiable asset owners. This ensures that there is defined responsibility and accountability, which is crucial for maintaining system integrity and addressing any issues promptly.

These recommendations are designed to mitigate the risks associated with unstable interfaces and networks by enhancing system oversight and clarifying operational responsibilities. Implementing these recommendations would lead to an improvement in the stability and reliability of the system's network infrastructure.

Mitigation Strategy (Socio Technical Lens)

1. Standardization and Transparency in Monitoring

Action Plan:

- Develop a comprehensive monitoring framework integrating both technical tools and human oversight.

- Employ advanced software for real-time monitoring and involve staff trained in interpreting and responding to the data.

Responsibility:

- Form a cross-functional team involving IT, operations, and risk management to oversee the monitoring process.

- Regular training for staff to understand and effectively use the monitoring tools.

Resource Allocation:

- Budget for both the technological aspects (software, hardware) and human elements (training, staff hours).

Monitoring and Evaluation:

- Regular feedback sessions with the monitoring team to assess tool effectiveness and operator training needs.

- Adapt the monitoring processes based on evolving system requirements and user feedback.

2. Central Asset Inventory Database

Action Plan:

- Create a centralized database that not only tracks physical and software assets but also incorporates the human elements like user access levels and responsibility areas.

- Document the dependencies between assets and how they interact within organizational processes.

Responsibility:

- Assign database management to a team that understands both the technical and operational aspects of the assets.

- Engage stakeholders from different departments for input on asset usage and dependencies.

Resource Allocation:

- Invest in robust database software and allocate resources for staff involvement in database maintenance and updates.

Monitoring and Evaluation:

- Continuous evaluation of the database's accuracy and relevance to current operational procedures.

- Regular feedback from users to refine the database's functionality and usability.

3. Clear Assignment of Asset Ownership

Action Plan:

- Assign ownership of IT components to individuals or teams, integrating this responsibility into their regular roles and workflows.

- Ensure that the owners have a clear understanding of both the technical aspects of the assets and their impact on organizational processes.

Responsibility:

- High-level management to identify and assign asset owners.

- Regular interactions between asset owners and other stakeholders to ensure alignment of technical and operational goals.

Resource Allocation:

- Resources for ongoing training and support for asset owners.

- Tools for monitoring and managing their assigned assets.

Monitoring and Evaluation:

- Evaluate the effectiveness of asset management in terms of both technical performance and organizational impact.

- Feedback loops for continuous improvement based on user and stakeholder experiences.

Incorporating a socio-technical framework into these mitigation strategies ensures a holistic approach, recognizing that the effectiveness of technical systems is deeply intertwined with the social context in which they operate. This approach highlights the importance of human factors, organizational culture, and communication in the successful implementation of technical solutions.

Miscommunication and Coordination Issues (H)

The Deloitte report identifies several vulnerabilities related to miscommunication and coordination issues within the TARGET2 system. These issues include deficiencies in communication protocols during incidents and the lack of structured processes for incorporating lessons learned. Specifically, the report highlights the ineffective dissemination of information during crisis management and the unclear roles and responsibilities, leading to coordination challenges among stakeholders.

This alignment with our identified vulnerability of "Miscommunication and Coordination Issues" points to the need for improved communication strategies and enhanced coordination mechanisms within the TARGET2 system. By addressing these issues, the goal is to foster a more cohesive operational environment, ensuring that all parties involved in the system's operation are well-informed and effectively coordinated.

Recommendations in the Report:

1. Improving Communication Protocols: The report suggests enhancing external communication by improving the usability of the ECB website, designing more bidirectional communication, and streamlining communication between ECB and NCBs.

2. Formalizing Lessons Learned Process: Implementing a formal lessons learned process is recommended to ensure that insights from incidents are systematically used to improve future operations.

3. Consistency in Documentation and Communication: Ensuring consistency and comprehensibility in the documentation of processes and policies, especially those related to communication and crisis management.

Mitigation Strategy (Socio-Technical Lens)

1. Improving Communication Protocols

Action Plan:

- Develop and implement a comprehensive communication strategy that includes bidirectional information flow and clear protocols during incidents.

- Utilize various communication channels effectively, ensuring information is accessible and understandable to all relevant stakeholders.

Responsibility:

- Assign a dedicated communication team, including representatives from different departments, to manage and oversee the communication strategy.

Resource Allocation:

- Allocate resources for developing and maintaining communication platforms and for training staff in effective communication practices.

Monitoring and Evaluation:

- Regularly assess the effectiveness of communication channels and protocols, adapting them as necessary based on feedback from stakeholders.

2. Formalizing Lessons Learned Process

Action Plan:

- Establish a formal process for capturing, analyzing, and integrating lessons learned from past incidents into current practices.

- Conduct regular review meetings post-incident to gather insights and develop action plans.

Responsibility:

- Designate a team to manage the lessons learned process, including documenting findings and ensuring their implementation.

Resource Allocation:

- Resources for the documentation and management of the lessons learned process, as well as for implementing recommended changes.

Monitoring and Evaluation:

- Track the implementation of lessons learned and evaluate their impact on system performance and coordination efficiency.

3. Consistency in Documentation and Communication

Action Plan:

- Standardize documentation related to communication and crisis management protocols.

- Ensure all communication and documentation are clear, consistent, and accessible to relevant parties.

Responsibility:

- Assign responsibility for maintaining documentation standards to a specific team or department.

Resource Allocation:

- Allocate resources for the development and maintenance of standardized documentation.

Monitoring and Evaluation:

- Regular audits of documentation for consistency and clarity, and periodic feedback sessions with stakeholders for continuous improvement.

Incorporating these strategies with a socio-technical focus ensures that both the social (organizational, human) and technical aspects of communication and coordination within the TARGET2 system are addressed, leading to a more robust, efficient, and reliable operational environment.

Ineffective Testing and Change Management (S)

In the Deloitte report, a significant focus is placed on the vulnerabilities surrounding ineffective testing and change management within the TARGET2 system. The report identifies shortcomings in the planning and implementation of changes, highlighting a lack of comprehensive risk-based assessment and planning in the change-planning process. It also notes deficiencies in the test management approach, which fails to reflect the scope, complexity, and potential impact of changes accurately.

These findings from the report align closely with the "Ineffective Testing and Change Management" vulnerability we identified. The report's emphasis on the inadequacy of current testing protocols and the risks associated with unassessed and poorly managed changes underscore the need for a more robust and systematic approach to testing and change management in the TARGET2 system.

Recommendations in the Report:

1. Comprehensive Risk-Based Assessment in Change-Planning: The report recommends including a comprehensive risk-based assessment and planning approach in the change-planning process, with defined minimum information requirements and objective criteria for decision-making.

2. Robust Test Management Approach: It suggests defining objective criteria to decide the scope and extent of required test activities, ensuring that tests reflect the actual conditions and risks associated with changes in the production environment.

3. Functional Test Environment for Network Changes: The report identifies the absence of a functional test environment for network changes, recommending the establishment of such an environment to test changes before applying them to the production environment.

Mitigation Strategy (Socio Technical Lens)

1. Comprehensive Risk-Based Assessment in Change-Planning

Action Plan:

- Implement a detailed risk assessment framework for evaluating changes, considering their potential impact on both technical and operational aspects.

- Develop guidelines and criteria for decision-making in the change-planning process, ensuring all risks are identified and addressed.

Responsibility:

- Assign a cross-functional team, including IT, risk management, and operational staff, to oversee the risk assessment and change-planning processes.

Resource Allocation:

- Allocate resources for developing and maintaining the risk assessment framework and for training staff on risk assessment procedures.

Monitoring and Evaluation:

- Regular reviews of the change-planning process and its outcomes to ensure risks are being adequately identified and mitigated.

2. Robust Test Management Approach

Action Plan:

- Define a structured test management approach that includes various types of tests (unit, system, integration, negative) to cover different scenarios.

- Ensure that the testing environment closely replicates the production environment to validate the behavior of tested systems.

Responsibility:

- Designate a specialized testing team to develop and implement the testing approach, ensuring they collaborate closely with IT and operational teams.

Resource Allocation:

- Invest in creating or enhancing testing environments and tools. Allocate resources for continuous training in advanced testing methodologies.

Monitoring and Evaluation:

- Regular assessments of testing processes and their effectiveness in identifying issues before changes are rolled out to the production environment.

3. Functional Test Environment for Network Changes

Action Plan:

- Establish a dedicated test environment for network-related changes, allowing for thorough testing before implementation in the live environment.

- Include procedures for testing changes first on a primary site before deploying on secondary sites.

Responsibility:

- Task IT infrastructure teams with developing and managing the test environment, ensuring continuous collaboration with network management teams.

Resource Allocation:

- Budget for the development and maintenance of the network test environment, including necessary hardware and software tools.

Monitoring and Evaluation:

- Conduct regular reviews of the test environment's effectiveness and its alignment with the actual network conditions and requirements.

Incorporating these strategies with a socio-technical focus ensures that both technical requirements and organizational aspects are considered in testing and change management processes. This comprehensive approach aims to enhance the resilience and efficiency of the TARGET2 system by ensuring that changes are thoroughly assessed and tested within a structured and collaborative framework.

5.8 TARGET2's Conceptual Framework Based on Expert Perspectives

The insights from the Policy Advisor, Financial Economist and Payment Systems experts collectively provide a nuanced understanding of TARGET2's conceptual framework, highlighting the importance of its networked value, and integration within the broader financial ecosystem.

The Policy Advisor challenges the notion of separately considering networked value, advocating for a more unified approach. He suggests that these aspects, particularly for banks and society, are intrinsically interlinked and should be viewed in conjunction, stating, "I see also arguments to bring them more together, especially for banks and for society being rather small and always the need to go outside." This perspective emphasizes the integrated nature of internal and external dependencies in financial systems, underscoring the need for a holistic view that reflects real-world systemic interconnections. Additionally, he advises on the significance of examining TARGET2's integration within the existing Dutch financial infrastructure, highlighting the necessity to align conceptual constructs with practical realities of systemic interplays.

Complementing this view, the Financial Economist acknowledges the conceptual framework's constructive approach in understanding TARGET2's operations and impact but recommends simplifying it by reducing dimensions or illustrating their interconnections more clearly. He advocates for a visual representation of the framework to better showcase the relationships between different elements, like system integration and resilience, stating, "The dimensions could be interlinked." This suggestion points towards a more interconnected depiction of the framework, moving beyond a

siloed perspective of discrete modules to a comprehensive understanding of TARGET2's multifaceted dynamics.

Although the Payment Systems expert did not explicitly address this theme, their insights implicitly contribute to shaping the conceptual framework. They present TARGET2 as an integrated system with multiple interdependent components, resonating with analogies of biological systems and business operations. This perspective informs the framework elements by highlighting the interactive alignment of TARGET2's components towards the common goal of facilitating transactions. The expert's balance between acknowledging vulnerabilities and emphasizing resilience offers a foundation for incorporating risk considerations into the framework, potentially through adaptability assessments. Furthermore, their focus on transactions as the core purpose, supported by technology and policies, provides direction for structuring framework dimensions that link operational capabilities with security considerations.

An enriched conceptual framework for TARGET2 emerges from these perspectives, advocating for a more integrated and comprehensive representation. The Policy Advisor's emphasis on the interconnectedness of networked value, the Financial Economist's focus on clarifying and interlinking framework dimensions, and the Payment Systems expert's insights on integrated system functioning and performance quantification collectively inform a robust, multidimensional understanding. This integrated approach underscores the importance of a nuanced framework that captures the complex dynamics of TARGET2, including its operational interdependencies, systemic resilience, and critical role in the broader economic and financial landscape.

Chapter 6 Discussion and Reflections

The comprehensive study of TARGET2, employing a qualitative approach with a systematic coding framework and thematic analysis, has revealed specific socio-technical vulnerabilities within the system. This empirical identification aligns with and substantiates the interconnected risks discussed in literature, tracing impact pathways and mapping vulnerabilities to monitoring indicators for optimized risk mitigation. Expert perspectives have reinforced TARGET2 as an apt socio-technical system illustration, filling gaps in literature and empirically enriching conceptual foundations. The experts' insights, coupled with the methodological rigor of the research design – encompassing document analysis and validation through expert interviews – provide a nuanced understanding of TARGET2's complexities. This analysis not only confirms the theoretical frameworks but also offers practical insights into the system's operation, vulnerabilities, and its critical role in economic security, particularly in the context of the Netherlands. Thus, the study effectively bridges theoretical concepts with empirical findings, highlighting the intricate socio-technical dynamics of TARGET2 and their implications for economic stability and security.

6.1 Summary of Findings

This research thoroughly examines the TARGET2 system, a key platform for processing high-value financial transactions in Europe, through detailed document analysis and insights from experts. It investigates how TARGET2 serves as a prime example of a socio-technical system, where technology and social structures are closely linked. Drawing on findings from the literature (Panourgias, 2015; Whitworth, 2011), the study highlights the integration of sophisticated technology and the network of stakeholders involved in managing and overseeing the system. This approach addresses gaps in previous research that have not fully applied a socio-technical perspective to understanding platforms like TARGET2 and their importance for economic stability.

The research identifies key technical elements that are crucial for TARGET2's operation, such as centralized processing platforms, communication systems, risk analysis tools, cost evaluation applications, and comprehensive data storage solutions. At the same time, it explores the social aspects by detailing the roles of various participants including central bank officials, commercial bankers, securities dealers, and retail customers. It also examines the governance framework, which encompasses regulatory bodies, technical oversight committees, and national authorities.

By documenting the socio-technical structure of TARGET2, the study creates a reference model for further analysis of the system's dynamics. It addresses a significant gap in the literature that has overlooked the comprehensive examination of TARGET2 by employing theoretical models that emphasize the intricate relationship between technological capabilities and social settings (Panourgias, 2015). This detailed codification expands the understanding of TARGET2, laying a foundation for broader discussions on the impact of digital infrastructures on economic health.

The review of existing literature underscores the growing dependency on technological systems for critical operations and the emergence of new risks associated with this reliance (Fåk, 2010; Tkachenko et al., 2019). It stresses the need for a thorough investigation. By methodically detailing TARGET2's components from a socio-technical viewpoint, this research responds to these concerns and prepares the ground for a comprehensive evaluation.

Following the detailed examination of TARGET2's socio-technical structure, the research delved into the intricate operational mechanisms that enable the system to process transactions efficiently. It identified several key processes as fundamental to TARGET2's operation, such as real-time settlement

of transactions, monitoring of liquidity flows, assessing risks, ensuring compliance with regulations, and managing crises. The study proposed that the smooth functioning of these processes relies on the effective interplay between the system's technological aspects and its social components—essentially, how well the technical features and human elements work together.

This investigation spotlighted crucial interactions within the system, such as the relationship between the core transaction mechanisms and the banks that use them, the oversight conducted by regulatory bodies, how information is communicated to and from end-users, and the enforcement of secure access through identification and permission protocols. The research analyzed how technical capabilities and organizational goals influence each other in these interactions, uncovering key points of integration and areas where mismatches occur.

For example, the study pointed out that the accuracy of transactions depends not only on the robustness of the settlement algorithms but also on the banks' compliance with operational guidelines, showcasing a balanced socio-technical relationship. On the other hand, it noted potential issues like delays in crisis management due to slow communication between technical staff and decision-making bodies, illustrating instances of socio-technical imbalance.

By examining these socio-technical interactions, the research emphasizes the importance of a well-coordinated effort between the technological infrastructure and human participants of TARGET2 for its operational stability. This perspective aligns with existing literature on the resilience of economic infrastructures, suggesting that to maximize the technical efficiency of systems like TARGET2, they must be integrated within an appropriate social framework. The analysis concludes that the effectiveness and reliability of TARGET2, as a critical economic infrastructure, are significantly influenced by the harmony between its technological advancements and the social context in which they are deployed.

After uncovering the intricate operations of TARGET2, the study then focused on delineating its essential and diverse roles within the European financial system. A thorough investigation into how TARGET2 interacts with the various actors in the European financial environment showcased its extensive impact.

TARGET2 is identified as critical for implementing Eurozone monetary policies, facilitating the immediate movement of liquidity from central banks. This function is key for the European Central Bank (ECB) to adjust the supply of money and interest rates effectively, enhancing macroeconomic stability across the Eurozone.

Moreover, the system serves as a crucial mediator ensuring the finality of settlements among commercial banks, which is vital for the smooth flow of capital. By guaranteeing that interbank payments are final and irreversible, TARGET2 promotes the efficiency of credit distribution, stimulating broader economic activity through enhanced lending and investment.

TARGET2 is also essential for businesses requiring fast cross-border payments, such as for managing inventory financing and seamless integration with international supply chains. This capability supports trade flexibility, strengthening both regional and global supply chains critical for economic vibrancy.

Beyond its direct stakeholders, TARGET2 plays a significant role in maintaining consumer confidence in the financial system's stability. Although consumers do not interact with TARGET2 directly, the system's efficient processing ensures a stable banking environment, fostering economic confidence among the public.

The analysis concludes that TARGET2's multifaceted functionality—spanning regulatory oversight, liquidity management, risk management, and crisis mitigation—solidifies its status as a pillar of financial strength in Europe. The study underscores TARGET2's paramount importance as the foundational support for European principles of stability, prosperity, and seamless market operations, highlighting its indispensable role in the European financial architecture.

Up to this point, the discussion about TARGET2 has largely focused on its successful integration into the European financial ecosystem and its critical functionalities. However, the study also hints at potential weaknesses within TARGET2's socio-technical structure, suggesting that these could lead to significant risks. This section highlights the vulnerabilities stemming from coordination issues between the system's operational capabilities and its governance, delays in updating technical and regulatory responses to incidents, and the challenge of ensuring compliance with current cybersecurity norms.

The analysis cautions that, although unlikely, a total failure in the core settlement algorithms due to software flaws could lead to a freeze in liquidity, affecting consumer banking services. Additionally, the risk of access credential leaks from participant databases represents a hidden danger. These 'black swan' events could allow unauthorized access and fraudulent activities, undermining trust in the system. While problems with the user interface currently result in minor delays, in stressful situations, these could escalate, leading to significant liquidity issues.

The research proposes that TARGET2's resilience should not solely focus on withstanding individual system failures but should also enhance its adaptability to rapidly identify and address issues. This approach includes the implementation of system-wide 'biosensors' for monitoring technical performance and user activity. Ensuring a highly coordinated response among technical, operational, and governance teams is crucial for preventing widespread economic impact.

The findings reinforce TARGET2's essential role in the European payment infrastructure, facilitating the flow of liquidity across various economic sectors. However, the identified risks related to the lack of synchronized coordination between its technical operations and administrative governance highlight a critical area of concern. Especially during times of economic uncertainty, these vulnerabilities could pose significant threats. Therefore, addressing these socio-technical gaps is vital for the ECB to enhance TARGET2's robustness and secure Europe's financial stability.

This comprehensive examination of TARGET2's structure, its operational mechanisms, and its broad economic impact uncovers a system that, while efficient, is susceptible to disruptions requiring a more unified approach to governance.

The study suggests that policy changes should view TARGET2 not just as a standalone transaction processor but as a vital part of a larger financial and economic network. It calls for a shift in oversight from merely technical to a broader socio-technical framework that involves a wide range of stakeholders. This approach acknowledges the complex interplay between the technical aspects of TARGET2 and the social dynamics of its user community.

To this end, the research underscores the importance of the Socio-Technical Integration Function (STIF) as a pivotal enhancement to TARGET2's operational framework. The formation of the STIF would involve assembling a management team comprising technology architects, banking compliance experts, financial regulators, and specialists in algorithmic auditing. This multidisciplinary team would collaboratively oversee the digital infrastructure, blending diverse skills and perspectives to foster mutual understanding across the finance and technology sectors. Such an approach is instrumental in enhancing the overall system oversight and ensuring a cohesive operational strategy.

In conclusion, transforming TARGET2's governance from a purely technical focus to an integrated socio-technical system is crucial for maintaining Europe's financial stability. Recognizing and addressing the potential risks arising from inadequate coordination among humans, as well as from technical flaws, is essential. This holistic approach to governance, aimed at quickly identifying and fixing minor issues before they escalate, is key to building a resilient payment infrastructure that supports Europe's economic well-being.

10

Chapter 7 Conclusion

The comprehensive study undertaken in this thesis has been pivotal in illuminating the socio-technical dynamics of the TARGET2 system and its consequential role in the economic security of the Netherlands. The initial literature review was instrumental in establishing the foundational understanding of economic security and the criticality of financial technologies within this framework. This review was essential to contextualize the importance of TARGET2 in the Dutch financial ecosystem, particularly highlighting its function as a critical technology.

The primary aim of this research was to dissect and analyze the intricate interplay between the technical components and social interfaces of TARGET2, exploring how this interaction influences its functionality, operational resilience, and overall impact on economic security. Through an in-depth qualitative analysis comprising document analysis and expert interviews, the study delved into the core operations of TARGET2, revealing its critical socio-technical elements and operational implications. This exploration was crucial in identifying the vulnerabilities within TARGET2's framework and understanding their potential impact on the economic stability of the Netherlands.

The findings from this study not only respond to the initial research questions but also offer significant theoretical and practical implications. The research contributes to the broader understanding of how critical financial technologies, like TARGET2, underpin economic security. It emphasizes the importance of recognizing and managing the socio-technical aspects of such systems, including governance structures, user engagement models, and technical infrastructure. The study challenges the notion that critical financial systems are purely technical entities. Instead, it underscores the necessity of a holistic approach that encompasses both the social and technical facets to enhance system resilience and reliability.

Previous research has often overlooked the socio-technical perspective in critical financial systems. This thesis addresses this gap by proposing a novel multidimensional framework for evaluating and managing the criticality of financial infrastructures like TARGET2. This framework not only encompasses technical robustness and operational stability but also adapts to the inherent risks and challenges in the financial landscape. It introduces a new paradigm in understanding and managing financial technologies, emphasizing the need for a balanced approach that considers both the technical and social dimensions.

The contribution of this thesis lies in offering a comprehensive analysis of TARGET2's socio-technical dynamics and its implications for economic security. By integrating theoretical perspectives with empirical findings, the study provides valuable insights for policymakers, regulators, and stakeholders in the financial industry. Implementing the findings and recommendations of this study could enhance the resilience and security of the TARGET2 system, thus reinforcing the economic stability of the Netherlands. The proposed framework not only aids in understanding the complexities of managing critical financial infrastructures but also provides for diagnostic tools for enhancing economic safeguards in an increasingly interconnected and technology-reliant financial environment. Overall, this research marks a significant advancement in the discourse on financial infrastructure management and economic security, highlighting the pivotal role of socio-technical systems in national and global economic landscapes.

7.1 Addressing the Research Question

Sub Research Question 1

What are the key technical components and social interfaces of the TARGET2 system?

The socio-technical examination of TARGET2 unveils a complex web of technical systems and social interactions that are crucial for its operations.

Technically, TARGET2 is built on foundational platforms like the Single Shared Platform (SSP), TARGET Instant Payment Settlement (TIPS), and TARGET2-Securities (T2S), which are key to ensuring settlement finality and managing liquidity. These platforms are supported by interfaces such as the TIPS Interface (TIPSI) and Ancillary Systems Interface (ASI), which link participant systems together. Secure communication is facilitated by protocols like SWIFTNet, while various monitoring and reconciliation tools strengthen the system's oversight capabilities.

On the social side, the study highlights the governance structure that links the system's operation to its ownership by Eurosystem central banks and oversight by regulatory bodies like the European Central Bank (ECB) Governing Council, which is responsible for monetary policy decisions within the TARGET2 ecosystem. It also outlines the relationships among direct settlement participants, including commercial banks and their interactions with regional and industry-specific financial institutions. Moreover, the analysis sheds light on the service delivery connections between centralized payment operation teams and participants, alongside system testing processes that ensure the platform's reliability and security.

By detailing these technical and social components, the analysis provides a clearer picture of TARGET2 as more than a mere payment system. It emerges as a vital institutional hub that supports the seamless functioning of Europe's financial landscape, highlighting its critical role in the interconnected European economy. This socio-technical mapping enhances our understanding of TARGET2's significance, emphasizing its position as a central node in the architecture of European finance.

Sub-Research Question 2

How does the socio-technical interplay within the TARGET2 system contribute to its functionality and operation?

The socio-technical framework of TARGET2 integrates to facilitate its critical function of processing a high volume of transactions, which is essential for maintaining economic stability. The system's technical backbone allows for the secure and real-time routing of payments, while its social components ensure that user feedback is continuously incorporated, enhancing the system's effectiveness in meeting monetary policy and liquidity management goals.

For example, the Single Shared Platform (SSP) enables real-time gross settlement, streamlining batch transfers among commercial banks. These banks play a key role in verifying transactions, authorizing them, and providing liquidity, demonstrating the coordination between TARGET2's technical capabilities and banking operations. Additionally, the TARGET Instant Payment Settlement (TIPS) feature modernizes the process of consumer remittances, supported by a framework that aligns platform algorithms with the collateral management policies of Eurosystem Central Banks. Crisis management within TARGET2 involves a collaboration between technical response teams and financial stability oversight entities such as the European Commission and the ECB Governing Board, ensuring a coordinated response to potential disruptions.

TARGET2, therefore, acts as more than just a mechanism for payment transactions; it integrates various stakeholders from commercial banks to businesses to consumers within a trusted transaction network, underpinned by socio-technical cohesion. To maintain seamless platform operations, it is crucial to continuously refine the interaction between human elements and the system, adapting to changing user demands, governance frameworks, and risk landscapes. Ultimately, the system's contribution to economic security is derived not solely from its technical infrastructure but from the effective integration of social elements, highlighting the importance of active social engagement alongside technological advancement.

Sub-Research Question 3

What operational indicators can be used to define and measure 'economic security' in the context of the TARGET2 system?

The analysis of the TARGET2 system uncovers key performance metrics that act as indicators of economic security, highlighting the system's contribution to the stability and efficiency of the European financial landscape:

System Uptime Rate: A high rate of system availability underscores TARGET2's technical resilience, ensuring uninterrupted operations crucial for the finality of settlements and the effectiveness of monetary policy signals. This reliability supports the continuous flow of transactions, a backbone of financial stability.

Transaction Error Rates: Low error rates in transaction processing reflect operational excellence, fostering market confidence and reducing systemic risk. Precision in settlement processes is vital for maintaining trust among market participants and ensuring the integrity of financial transactions.

Transaction Speed/Delay: The ability to process payments swiftly and with minimal delays is essential for the efficient distribution of liquidity and the timely execution of monetary policy interventions. Quick transaction speeds enhance the system's responsiveness to market needs and policy adjustments.

Compliance Rates with Governance Decisions: High compliance rates indicate effective alignment with legal and regulatory frameworks, aligning operations with the financial stability goals of the Eurosystem. This metric underscores the importance of adherence to governance decisions and regulatory policies.

These performance indicators collectively reflect the economic security facilitated by TARGET2's integrated socio-technical system. They encompass settlement efficiency, operational precision, responsiveness, compliance with governance, and crisis management capabilities.

At its core, TARGET2 stands as the central hub of settlement in European finance, where its efficiency underpins the continuous movement of money that drives consumption, trade, and employment. The system's performance metrics are direct reflections of its systemic health and its role as a catalyst for the markets of goods, labor, and prosperity across Europe. By ensuring the smooth operation and robust performance of TARGET2, the system contributes significantly to the economic vitality of the continent.

Sub-Research Question 4

What potential vulnerabilities and threats within the TARGET2 system could impact its operation and overall economic stability?

The primary vulnerabilities identified as arising from socio technical asymmetries or disconnects are as followed;

Technical disruptions: Outages or failures within core platforms like SSP and TIPS could severely impact transaction processing and settlement finality. This disrupts liquidity distribution essential for smooth financial system functioning.

Transaction processing bottlenecks: System congestion during peak transaction loads can delay transfer settlement between banks. This affects liquidity positions and the efficiency of monetary policy transmission across the Eurozone.

Unreliable system interfaces and networks: Integration flaws between settlement modules or network instabilities can halt interbank payments. This breeds uncertainty around transaction finality, negatively influencing market confidence.

Inaccurate static data: Errors in transaction verification data or misconfigured algorithms can cause incorrect fund allocation. This results in settlement disputes that increase systemic risk.

Communication and coordination deficiencies: Ineffective crisis response due to fragmented communication between technical teams and management delays recovery initiatives. This worsens the impact of disruptions on payment operations.

The primary threats arising from vulnerabilities identified in TARGET2's socio-technical framework include:

System component failures: Failures in critical system components could occur due to outdated or inadequate replacements, causing disruptions in payment processing and settlement delays.

Procedural or operational failures: Lapses in standard procedures or process execution due to human errors or inadequate controls can undermine operational reliability.

External events: Vulnerabilities in disaster recovery capacities can get exploited by natural disasters or power outages, severely disrupting operations.

Security-related incidents: Data security gaps and inadequate access controls may lead to compromises in data/communication confidentiality and system integrity.

Unauthorized access: Weak identity and access management controls risk enabling unauthorized individuals to gain access to privileged systems and data.

Supplier-related incidents: Over-reliance on third-party suppliers poses risks of disruptions propagating from shortcomings in their systems' security or delivery robustness.

Participant-related events: Inadequate oversight around participant management may fail to contain disruptions originating from participant systems or actions.

The research identifies and elaborates on socio-technical vulnerabilities within the TARGET2 system, shedding light on potential threats to its stability and the broader economic framework. It documents how platform disruptions, processing bottlenecks, network instability, and miscommunication risks could critically affect transaction processing, liquidity, and financial information flows. By highlighting these fractures, the analysis underscores the imperative for robust technical solutions and coherent policy frameworks to mitigate risks, ensuring the resilience of financial operations against operational and systemic challenges. This examination not only

contributes to understanding TARGET2's vulnerabilities but also informs strategies for safeguarding economic security.

Sub-Research Question 5

How does the TARGET2 system's interdependency with other financial systems factor into its criticality for economic security?

TARGET2's integration with a wide array of financial entities, including central banks, commercial banks, payment platforms, and financial market infrastructures (FMIs) within the Eurozone, underscores its vital role in ensuring economic security. This interconnectedness enhances TARGET2's importance in several critical aspects of financial operations:

Execution of High-Value Transactions: TARGET2 is central to the processing of large-scale financial transfers, managing liquidity, and enacting monetary policy across national borders. These functions are foundational for the stability and smooth operation of financial markets.

Ripple Effects of Dysfunctions: Given its central role, any operational issues within TARGET2 can have far-reaching impacts, potentially jeopardizing the financial stability of the entire Eurozone. The system's smooth functioning is thus paramount to avoid triggering a cascade of financial disruptions.

Impact on Settlement Finality and Liquidity Flows: Problems in these areas can erode confidence in financial markets, with significant delays having the potential to disrupt financial activities across interconnected systems. Such issues underscore the need for TARGET2's reliability and efficiency.

Risk Propagation Through Interconnections: The tight linkage between TARGET2 and other financial systems facilitates the spread of risks, necessitating robust coordination among both multinational and national authorities to manage and respond to crises effectively.

TARGET2's extensive interconnections position it as a linchpin in the European financial architecture, acting as a critical backbone supporting the continent's economic and financial infrastructure. Protecting and ensuring the operational integrity of TARGET2 is crucial for maintaining the broader stability and resilience of the Eurozone's financial ecosystem, highlighting its indispensable role in safeguarding Europe's economic prosperity.

Main Research Question

How does the TARGET2 system contribute to the economic security of the Netherlands from a socio-technical perspective?

The TARGET2 system contributes to the economic security of the Netherlands through a complex interplay of its socio-technical components. Technically, it provides the essential infrastructure for real-time gross settlement of transactions, which is crucial for the execution of high-value interbank payments, liquidity management, and the implementation of monetary policies. This technical foundation ensures the stability and efficiency of financial transactions across the Dutch financial ecosystem.

From a social perspective, the system is underpinned by a robust governance framework that encompasses multiple levels of operational roles, from the ECB Governing Council to settlement managers. The interaction between users and technical systems is facilitated through clear communication channels and well-defined operational procedures, ensuring that financial operations align with established policies and standards.

However, the resilience of TARGET2 has been tested by occasional system crashes, which led to temporary disruptions. These incidents highlight the system's vulnerabilities and the critical need for continuous improvements in both technology and operational protocols. Despite these challenges, the robust governance framework of TARGET2, involving entities like the ECB Governing Council and various operational roles, plays a pivotal role in swiftly addressing and rectifying such disruptions. This responsiveness is essential for maintaining system integrity and aligning financial operations with established policies and standards.

From a socio-technical perspective, these elements collectively ensure the Dutch financial system's resilience:

Reliability Amidst Challenges: TARGET2 provides a reliable platform for financial institutions, crucial for the country's financial stability. Even when faced with disruptions, the system's design and governance allow for quick recovery and mitigation of impacts, underlining the importance of resilience in financial infrastructure.

Effective Policy Transmission: The system ensures that monetary policies set by the ECB are effectively transmitted to the Dutch banking sector. This process influences key economic factors like interest rates and money supply, crucial in economic policymaking, especially during recovery periods following disruptions.

Facilitation of Financial Transactions: TARGET2 supports the settlement of both domestic and international transactions, vital for the smooth operation of the Netherlands' trade and investment activities. The system's ability to maintain these functions, even in the face of technical challenges, is a testament to its resilience and importance to the nation's economy.

Security and Compliance: TARGET2 maintains a secure environment for financial transactions, thus preserving user trust and the Netherlands' reputation as a financially secure and compliant nation within the Eurozone. This security is crucial, especially in maintaining confidence in the system post-crash and during the recovery process.

Through socio-technical analysis, TARGET2 emerges as a critical component in safeguarding the Netherlands' economic security. The system’s technical robustness and social integrity, harmonized with a responsive and adaptive approach to challenges, create a resilient financial ecosystem. Despite occasional setbacks like system crashes, TARGET2's overall design and operational strategies ensure its effectiveness and reliability in supporting the nation’s economic stability.

7.2 Conceptual Framework

In this research, we have embarked on a comprehensive exploration of the TARGET2 system, delving deep into its socio-technical aspects and evaluating their impact on the economic security of the Netherlands. This journey involved dissecting the intricate layers of TARGET2, from unraveling its essential components and interfaces to comprehending its integral role in the wider financial ecosystem. Through this multifaceted analysis, we have reached a pivotal point: the construction of a conceptual framework that encapsulates our extensive findings and provides a nuanced understanding of TARGET2's operational and strategic importance.

This framework, a product of our detailed investigation, interweaves the complex socio-technical interactions within TARGET2 with their operational consequences and potential vulnerabilities. It integrates insights from a thorough examination of the operational indicators that define economic security in the context of TARGET2 and scrutinizes the system's interrelations within the global

financial network. To systematically capture the essence of TARGET2 and its significance in bolstering the Netherlands' economic stability, the framework is structured around five key dimensions: Integration, Reliability, Adaptability, Networked Value. Each dimension represents a specific facet of TARGET2 (Fig-7.1):

Integration: Examining the synergy between technical elements and social interfaces within TARGET2, highlighting how this integration influences system functionality.

Reliability: Focusing on the system's operational efficiency and effectiveness, emphasizing its consistency and dependability.

Adaptability: Assessing TARGET2's resilience to vulnerabilities and its capability to adjust to evolving challenges and risks.

Networked Value: Evaluating TARGET2's contribution to economic security, particularly through its role in financial stability and policy execution. Also captures TARGET2's interconnectedness with other financial systems and its impact on the broader financial landscape.

The development of these dimensions marks a critical advancement in our understanding of TARGET2, providing a comprehensive framework that not only reflects our academic insights but also serves as a practical guide for future research, policy formulation, and system enhancement.

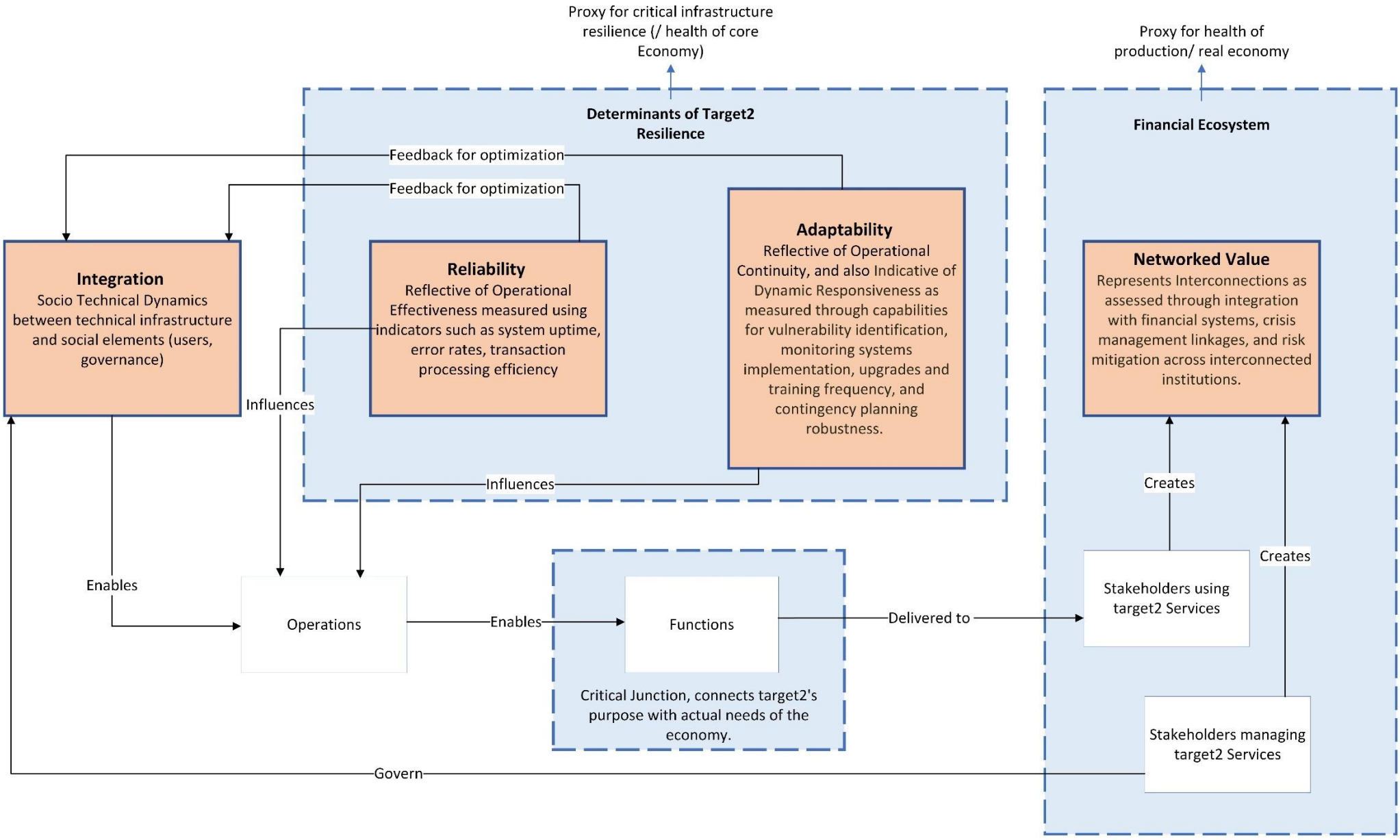

Figure 7-1 Conceptual Framework

We delve deeper into each dimension now.

Integration (I)- Socio-Technical System Dynamics

The "Integration" dimension in the conceptual framework focuses on the intricate socio-technical dynamics within the TARGET2 system, emphasizing how its technical components and social elements coalesce to influence its overall design and functionality. This aspect is pivotal for comprehending the symbiotic relationship between TARGET2's technical infrastructure, comprising elements like the Single Shared Platform (SSP), TARGET Instant Payment Settlement (TIPS), and TARGET2-Securities (T2S), and its social counterparts, including a diverse range of users such as commercial banks, indirect participants, and ancillary systems, along with the encompassing governance structure led by the European Central Bank (ECB) and other central banks.

Our research illuminated how this integration is essential for TARGET2's operational effectiveness. We observed that the system's robust technical foundation requires harmonization with the demands of its users and the regulatory framework set by its governance bodies. This alignment is not static but dynamic, evolving through continuous feedback and technical refinements. Such a loop of interaction and adaptation is integral to TARGET2's ongoing evolution and responsiveness to changing conditions.

The impact of this socio-technical integration on TARGET2's functionality is profound. It directly influences the system's ability to efficiently manage real-time gross settlements, liquidity, and the execution of ECB's monetary policies. The alignment of governance decisions with user compliance also shapes TARGET2's operational framework, ensuring it remains in line with strategic objectives and regulatory standards.

In essence, the Integration dimension underscores the criticality of a well-synchronized socio-technical system within TARGET2. It highlights the need for the system's technical capabilities to be responsive and adaptable to the social context, encompassing user needs, governance directives, and operational roles. This understanding is crucial for grasping TARGET2's role in safeguarding the economic security of the Netherlands, ensuring the system is not only efficient and reliable but also attuned to the needs of its diverse stakeholders.

Reliability (R)- Operational Effectiveness Indicators

The "Reliability" dimension of the conceptual framework zeroes in on the operational effectiveness of the TARGET2 system, **underlining the importance of consistent performance and dependability in its operations.** This dimension is centered around key indicators that signify how reliably the system functions in handling crucial financial transactions.

The research identified the crucial role of TARGET2 in managing high-value transactions with precision and speed. The system's ability to process these transactions in real-time and with a high degree of accuracy is paramount for the stability of the financial system.

The reliability of TARGET2 is also reflected in its system uptime and error rates. High uptime indicates the system's robustness and its ability to remain operational without significant disruptions. Low error rates are equally critical, as they signify the system's accuracy in transaction processing, a vital aspect considering the volume and value of transactions it handles.

The reliability of TARGET2 directly impacts the economic security of the Netherlands by ensuring the smooth functioning of financial operations. Consistent and dependable transaction processing supports the stability of the banking sector and maintains trust among its users.

The system's operational reliability also plays a crucial role in implementing monetary policies effectively, a vital aspect of economic stability and security.

In summary, the "Reliability" dimension of our framework encapsulates TARGET2's operational effectiveness as a critical component of its contribution to economic security. By focusing on indicators like system uptime, error rates, and transaction processing efficiency, we emphasize the significance of a reliable and efficient system in maintaining the stability and trustworthiness of the financial infrastructure. This dimension provides a quantitative measure of TARGET2's performance, offering insights into its ability to sustain the financial operations that underpin the economic stability of the Netherlands.

Adaptability (A)- Vulnerabilities and Evolution

The "Adaptability" dimension of our conceptual framework examines TARGET2's capacity to identify and respond to potential vulnerabilities, assessing the system's ability to adapt to changing circumstances and emerging risks. This dimension is crucial in understanding how TARGET2 maintains its resilience and operational integrity in the face of challenges that could impact its performance and, by extension, the economic security of the Netherlands.

Our analysis highlighted several potential vulnerabilities within the TARGET2 system, including usability issues, technical disruptions, and transaction processing bottlenecks. These vulnerabilities, if unaddressed, could lead to inefficiencies, errors, or even significant operational disruptions.

We delved into how these vulnerabilities might manifest and their potential impact on TARGET2's operations. For instance, usability issues could hinder user interactions with the system, while technical disruptions could lead to delayed transactions and undermine trust in the system's reliability.

An essential part of TARGET2's adaptability is its ability to recognize these vulnerabilities and implement measures to mitigate their impact. This includes continuous monitoring, regular system upgrades, and user training programs to enhance operational readiness. The system's adaptability is also evident in its **crisis management protocols and contingency planning**, ensuring that it can maintain operations and manage liquidity even in adverse conditions.

The adaptability of TARGET2 is directly linked to the economic security of the Netherlands. The system's ability to adjust to vulnerabilities and emerging risks safeguards the continuity of financial operations, a critical factor for maintaining market stability. Moreover, TARGET2's adaptability contributes to its role in the execution of monetary policy and regulatory compliance, further emphasizing its importance in sustaining the economic stability of the country.

In summary, the "Adaptability" dimension of our framework encapsulates TARGET2's responsiveness to vulnerabilities and its ability to manage risks effectively. This dimension underscores the importance of a system that is not only robust but also flexible and responsive to changing conditions and emerging challenges. It illustrates how TARGET2's capacity to adapt and evolve plays a vital role in safeguarding the economic security of the Netherlands, ensuring that the financial system remains stable, trustworthy, and resilient.

Networked Value (N) – Economic Security

The "Networked Value" dimension of our conceptual framework emphasizes TARGET2's role in the broader economic landscape, particularly its contribution to the economic security of the Netherlands. This dimension showcases how TARGET2, as a key component of the financial infrastructure, is not just a standalone entity but part of a larger networked system, where its value is amplified through its interactions and integrations with other financial systems and stakeholders.

Our research has demonstrated that TARGET2 is a linchpin in the Dutch financial ecosystem. Its operations, encompassing settlement of high-value transactions and real-time gross settlement, are essential for maintaining the liquidity and stability of the banking sector. By facilitating efficient and secure transactions, TARGET2 supports the smooth functioning of financial markets, which is crucial for the economic well-being of the Netherlands. Its role extends to supporting the ECB's monetary policy, influencing factors like inflation and interest rates, which are vital for economic stability.

TARGET2's value is also derived from its interconnectedness with global financial markets. Its ability to process cross-border transactions efficiently makes it an integral part of the international financial system, facilitating trade and investment activities. This interconnectedness also means that TARGET2's performance and reliability have far-reaching implications, impacting not just the Dutch economy but also the broader Eurozone and international financial markets.

The networked value of TARGET2 is also evident in its impact on various stakeholders, including commercial banks, regulatory bodies, and consumers. For instance, its efficient operation is critical for banks in managing their liquidity and for regulatory bodies in ensuring financial stability. For consumers and businesses, TARGET2's reliability and efficiency in processing transactions underpin the trust in the banking system and financial services, which is essential for economic activities and consumer confidence.

This dimension of our conceptual framework also delves into the systemic interconnectivity of TARGET2, focusing on its crucial linkages with both domestic and international financial systems and infrastructures. This dimension is pivotal in understanding TARGET2 not as a standalone entity but as an integral component within a larger financial ecosystem that encompasses both the Dutch financial sector and the global financial landscape.

The research underscores TARGET2's central role in the European financial network, where it interacts with a variety of financial systems, including securities settlement systems like TARGET2-Securities (T2S) and cross-border payment platforms.

These interactions underpin the seamless execution of complex financial operations, such as securities trading and international settlements, crucial for capital market functionality and cross-border trade efficiency.

TARGET2's connectivity extends well beyond the Eurozone, playing a key role in handling cross-border euro transactions. This positions it as an essential player in the international financial arena, influencing economic activities globally.

This extensive connectivity means that events in other financial systems can impact TARGET2, affecting its operations and the Dutch financial ecosystem.In financial crises, TARGET2's interconnected role becomes increasingly critical. It is central to crisis management, providing liquidity and stability to the banking sector and helping mitigate systemic risks.

Coordination between TARGET2 and other financial infrastructures during crises is vital for sustaining confidence in the financial system and averting cascading failures across interconnected networks.

In summary, The "Networked Value" dimension underscores TARGET2's critical role in supporting the economic security of the Netherlands, emphasizing its function not just as technical infrastructure but as a cornerstone within a broad, interconnected financial ecosystem. This dimension highlights how TARGET2 facilitates crucial financial transactions, contributing to the stability and prosperity of the Dutch economy and the Eurozone. It also points to TARGET2's extensive systemic interconnectivity, illustrating its embeddedness in both domestic and international financial

networks. This interconnectedness enhances financial operation efficiency but also exposes the system to external risks, showcasing the need for robust risk management. Understanding TARGET2's dual role in facilitating economic stability and managing global financial integration is essential for appreciating its comprehensive impact on the Netherlands' economic security.

7.3 Contribution to the field

In this thesis, the exploration of the TARGET2 system and its implications for economic security has been approached through a comprehensive socio-technical lens. This perspective has been instrumental in addressing previously unexplored aspects of critical financial infrastructures, particularly in understanding the interplay between technology and economic policy. The thorough examination and analysis of socio-technical components, interactions, and vulnerabilities within TARGET2 have yielded a valuable, evidence-based risk assessment framework. This framework stands as a significant resource for policymakers and financial authorities, facilitating informed decision-making in securing vital financial market infrastructures.

Furthermore, the research advocates for a harmonized approach that spans social, technical, and regulatory dimensions, thereby establishing a new paradigm for policy formulation in managing financial systems. The introduction of a conceptual framework, integrating system integration, networked value, resilience, and adaptability, provides a robust analytical framework applicable across various sectors. This framework enhances our understanding of critical systems and their operational intricacies.

Significantly, the findings emphasize the interconnected nature of financial systems and the magnified risks this interconnectivity poses for economic stability. The insights gained contribute to the broader discourse on systemic risk prevention and management. The methodology employed, which combines detailed document analysis with expert interviews, further advances qualitative research approaches in studying complex systems and infrastructures.

In conclusion, the contributions of this thesis are manifold, extending across critical infrastructure security analysis, the application of socio-technical theory, economic risk evaluation, and the development of comprehensive policy-oriented frameworks. These contributions are invaluable for financial authorities and scholars alike, paving the way for further research and informed policy-making in the realm of financial stability and economic security.

7.4 Practical Implications of the Study

In this thesis, the investigation of the TARGET2 system through a socio-technical lens offers significant practical implications for stakeholders in financial stability and economic security. The study's findings highlight the need for holistic governance by policymakers and financial regulators, addressing vulnerabilities from socio-technical asymmetries. It advocates for proactive oversight to prevent systemic issues, underscoring the importance of continuous monitoring and adaptive response mechanisms.

The research also provides a foundational blueprint for financial authorities to conduct in-depth risk audits. These audits are designed to identify and assess subtle interdependencies, informed by a structured approach to likelihood analysis and expert insights. This approach ensures a comprehensive understanding of potential threats, enhancing the effectiveness of risk management strategies.

For organizations relying on TARGET2, the research encourages greater alignment between employee protocols and technical systems. Emphasizing a vigilant approach to socio-technical risks, it suggests cultivating a culture that is keenly aware of potential communication gaps and process deviations.

From an infrastructure management perspective, the study underscores the importance of regular contingency planning and the establishment of robust redundancy mechanisms. These strategies are crucial for managing unexpected systemic shocks. It also points out the value of operational indicators such as system uptime, transaction processing efficiency, and network reliability in monitoring socio-technical asymmetries. Tracking these metrics facilitates an early warning system, enabling preemptive actions to strengthen vulnerabilities.

Additionally, the study proposes a conceptual framework that integrates socio-technical considerations, offering a versatile tool for balanced policy decisions in managing financial platforms and embracing new innovations like blockchain technology.

In conclusion, this thesis presents practical strategies for risk-aware and proactive infrastructure oversight, crucial for safeguarding interconnected financial systems in an evolving digital landscape.

7.5 Research Limitations and Recommendation for Future Research

In this study, the focused examination of the TARGET2 system and its implications within the Netherlands has yielded in-depth insights, albeit with inherent limitations, which are counterbalanced by proposed strategies for future research enhancement.

The concentration on TARGET2, while providing a detailed socio-technical analysis, is somewhat limited in its wider application across diverse financial systems. To address this, future research could embrace comparative studies involving multiple international financial transaction systems, broadening the scope and enriching the generalizability of the findings.

Additionally, the study's primary focus on the Dutch context restricts its extrapolation to the broader Eurozone or global financial networks interconnected with TARGET2. An effective strategy to overcome this limitation would be to extend the research to a multi-country examination within the Eurozone or the EU, thereby capturing a more diverse range of economic security perspectives related to TARGET2.

A notable limitation lies in the heavy reliance on official documentation for analyzing TARGET2, which might overlook the informal institutional dynamics that significantly influence governance and system operations. To mitigate this, incorporating ethnographic methodologies, such as embedding within operational teams managing TARGET2, would provide invaluable insights into the informal aspects of process adaptations, team interactions, and the exchange of tacit knowledge.

The expert validation process, primarily involving Eurozone professionals, poses the risk of inherent biases. To counter this, the inclusion of diverse perspectives from fields such as cybersecurity, history, and sociology could provide necessary adversarial viewpoints, enriching the analysis and challenging financial assumptions.

Finally, the study's analytical depth may inadvertently exclude perspectives from less financially literate populations, a crucial aspect in understanding the broader impact of financial systems. Participatory research methods, involving non-expert groups like everyday citizens and small business owners, could play a pivotal role in democratizing financial literacy and uncovering unique insights into system transparency and accountability.

In summary, the thesis, while comprehensive in its current scope, opens avenues for future research that include diversifying cases, expanding geographical focus, embedding within operational contexts, introducing a variety of perspectives, and embracing inclusive participation. Such a multi-faceted

approach promises to further enhance the study's rigor and relevance in the field of financial systems analysis.

7.6 Recommendation for the ECB Executive Board:

Based on comprehensive insights from a detailed thesis analysis, which underscores the indispensable role of socio-technical integration in enhancing the resilience of TARGET2, a nuanced recommendation is proposed for the European Central Bank (ECB) Executive Board. This analysis reveals the necessity for initiating a Socio-Technical Integration Function (STIF) within TARGET2 operations. The function aims to harmonize the system's technological infrastructure with a broad spectrum of socio-economic elements, encompassing governance frameworks, stakeholder interactions, regulatory compliance, and cultural dynamics.

The rationale for addressing this recommendation to the ECB Executive Board stems from its pivotal role in steering the Eurosystem's financial infrastructure and its direct oversight capabilities over TARGET2. The ECB Executive Board's unique position enables it to enact systemic changes, ensuring that socio-technical integration becomes a cornerstone of TARGET2's operational ethos. This strategic alignment is crucial for maintaining the system's robustness, adaptability, and alignment with the Eurozone's financial stability objectives.

The establishment of the STIF is aimed at facilitating a deeper understanding and integration of various social factors, including organizational behavior, policy evolution, and user-centric practices, alongside ongoing technological advancements. This approach acknowledges that the successful operation of TARGET2 relies on a synchronized blend of technological innovation and social considerations, far beyond mere stakeholder engagement.

By recommending the STIF to the ECB Executive Board, the objective is to ensure that TARGET2 can effectively meet the current and future challenges of its diverse user base, thereby safeguarding the Eurozone’s financial infrastructure against potential disruptions. This initiative underscores the Eurosystem's dedication to a stable, efficient, and inclusive financial ecosystem, aligning with the ECB's strategic priorities and the broader goals of economic and financial stability within the Eurozone.

References

Abad, J., Löffler, A., Schnabl, G., & Zemanek, H. (2013). Fiscal divergence, current account divergence and TARGET2 imbalances in the EMU. Intereconomics, 48(1), 51-58.

Ahmady, A. (2023). The Development of National Payment Systems: Lessons Learned from Developing Country Payment Systems. M-RCBG Associate Working Paper Series.

Akande, A. J., Foo, E., Hou, Z., & Li, Q. (2023). Cybersecurity for Satellite Smart Critical Infrastructure. In Emerging Smart Technologies for Critical Infrastructure (pp. 1-22). Cham: Springer Nature Switzerland.

Albert, W., & Tullis, T. (2013). Measuring the user experience: collecting, analyzing, and presenting usability metrics. Newnes.

Alcaraz, C., & Zeadally, S. (2015). Critical infrastructure protection: Requirements and challenges for the 21st century. International journal of critical infrastructure protection, 8, 53-66.

Alesina, A., Ozler, S., Roubini, N., & Swagel, P. (1996). Political instability and economic growth. Journal of Economic growth.

Allen, R. C. (2009). Engels' pause: Technical change, capital accumulation, and inequality in the British industrial revolution. Explorations in Economic History, 46(4), 418–435. https://doi.org/10.1016/j.eeh.2009.04.004

Andruseac, G. (2015). Economic security–new approaches in the context of globalization. CES Working Papers, 7(2), 232-240.

Appelbaum, S.H. (1997). Socio-technical systems theory: an intervention strategy for organizational development. Management Decision, 35(6), 452-463.

Archibugi, D., & Pietrobelli, C. (2003). The Globalisation of Technology and its Implications for Developing Countries: Windows of Opportunity or Further Burden? Technological Forecasting and Social Change.

Armstrong, A. (2016). EU membership, financial services and stability. National Institute Economic Review, 236, 31-38.

Arthur, K. N. A. (2017). Financial innovation and its governance: cases of two major innovations in the financial sector. Financial innovation, 3, 1-12.

Athanassiou, P. (2020). Payment Systems. In The EU Law of Economic and Monetary Union.

Attfield, S., Kazai, G., Lalmas, M., & Piwowarski, B. (2011, February). Towards a science of user engagement. In WSDM workshop on user modelling for Web applications (pp. 9-12).

Aubert, B. A., Patry, M., & Rivard, S. (2005). A framework for information technology outsourcing risk management. ACM SIGMIS Database: the DATABASE for Advances in Information Systems, 36(4), 9-28.

Bailey, J. E., & Pearson, S. W. (1983). Development of a tool for measuring and analyzing computer user satisfaction. Management science, 29(5), 530-545.

Bank, E. C. (2021). What is TARGET2? https://www.ecb.europa.eu/ecb/educational/explainers/tell-me/html/target2.en.html

Barredo-Zuriarrain, J., Molero-Simarro, R., & Quesada-Solana, A. (2017). Euro-dependence—a peripheral look beyond the Monetary union: a proposal of reform of the TARGET2. Review of radical political economics, 49(3), 375-393.

Baxter, G., & Sommerville, I. (2011). Socio-technical systems: From design methods to systems engineering. Interacting with computers, 23(1), 4-17.

Bech, M. L., & Hobijn, B. (2006). Technology diffusion within central banking: the case of real-time gross settlement. FRB of New York Staff Report, (260).

Bech, M. L., Shimizu, Y., & Wong, P. (2017). The quest for speed in payments. BIS quarterly review March.

Beck, T. (2006). Creating An Efficient Financial System: Challenges In A Global Economy. https://doi.org/10.1596/1813-9450-3856

Berg, A., & Ostry, J. D. (2011). Inequality and Unsustainable Growth: Two Sides of the Same Coin? IMF.

Berndsen, R., & Heijmans, R. (2017). Risk Indicators for Financial Market Infrastructure: From High Frequency Transaction Data to a Traffic Light Signal. De Nederlandsche Bank Research Paper Series.

Berndsen, R., & Heijmans, R. (2020). Near-Real-Time Monitoring in Real-Time Gross Settlement Systems: A Traffic Light Approach. Capital Markets: Market Microstructure eJournal.

Biais, B., Foucault, T., & Moinas, S. (2016). Equilibrium fast trading. Journal of Financial Economics, 116(2), 292-313.

Bigley, G. A., & Roberts, K. H. (2001). The incident command system: High-reliability organizing for complex and volatile task environments. Academy of Management Journal, 44(6), 1281-1299.

Bimber, B. A., & Popper, S. (1994). What is a Critical Technology? https://www.rand.org/pubs/drafts/DRU605.html

Bindseil, U., & König, P. (2011). The economics of TARGET2 balances. Humboldt-Universität zu Berlin, Wirtschaftswissenschaftliche Fakultät.

Blake, D. (2018). Target2: The Silent Bailout System that Keeps the Euro Afloat. International Finance eJournal.

Blake, D. (2018). Target2: The Silent Bailout System that Keeps the Euro Afloat. International Finance eJournal.

Blanchard, O., Dell'Ariccia, G., & Mauro, P. (2010). Rethinking Macroeconomic Policy. Journal of Money, Credit and Banking

Bossone, B., Srinivas, G., & Banka, H. (2020). Granting access to real-time gross settlement systems in the FinTech era. Journal of Payments Strategy & Systems, 14(4), 363-379.

Bradić-Martinović, A. (2011). Systemic risks control as a determinant of payment systems development in WB countries.

Brown, G. G., Carlyle, W. M., Salmeron, J., & Wood, K. (2005). Analyzing the vulnerability of critical infrastructure to attack and planning defenses. In Emerging Theory, Methods, and Applications (pp. 102-123). Informs.

Brynjolfsson, E., & McAfee, A. (2014). The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies. W. W. Norton & Company.

Bullmann, D., & Pinna, A. (2017). The future of European financial market infrastructure: A business case for distributed ledger technology?. Journal of Securities Operations & Custody, 9(1), 38-46.

Burton-Jones, A., & Grange, C. (2013). From use to effective use: a representation theory perspective. Information systems research, 24(3), 632-658.

Cable, V. (1995). What is international economic security?. International Affairs, 71(2), 305-324.

Cai, J., Eidam, F., Saunders, A., & Steffen, S. (2018). Syndication, interconnectedness, and systemic risk. Journal of Financial Stability, 34, 105-120.

Cales, M., Chabert, D., Hichri, W., & Marchand, N. (2011). The Reform of European Securities Settlement Systems: Towards an Integrated Financial Market. European Economics: Macroeconomics & Monetary Economics eJournal.

Carstens, A. (2020). Shaping the future of payments. BIS Quarterly Review, March.

Cecchetti, S. G., McCauley, R. N., & McGuire, P. (2012). Interpreting TARGET2 balances.

Chang, M., & Jones, E. (2013). Belgium and the Netherlands: Impatient capital. Market-Based Banking and the International Financial Crisis, 79-102.

Chapelle, A., Crama, Y., Hübner, G., & Peters, J. P. (2008). Practical methods for managing operational risk in the financial sector. Journal of Banking & Finance, 32(6), 1049-1061.

Checkland, P. (1999). Systems thinking. Rethinking management information systems, 45-56.

Chemmanur, T. J., Imerman, M. B., Rajaiya, H., & Yu, Q. (2020). Recent developments in the fintech industry. Journal of Financial Management, Markets and Institutions, 8(01), 2040002.

Cherns, A. (1976). The principles of sociotechnical design. Human Relations, 29(8), 783–792. https://doi.org/10.1177/001872677602900806

Chick, V., & Dow, S. C. (1997). Competition and the future of the European banking and financial system. In Money, financial institutions and macroeconomics (pp. 253-270). Dordrecht: Springer Netherlands.

Chiu, I. H. (2017). A new era in fintech payment innovations? A perspective from the institutions and regulation of payment systems. Law, Innovation and Technology, 9(2), 190-234.

Chmielewski, T., & Sławiński, A. (2019). Lessons from TARGET2 imbalances: The case for the ECB being a lender of last resort. Economics and Business Review.

Clemente, D. (2013). Cyber security and global interdependence: what is critical? (p. 7). London: Chatham House, Royal Institute of International Affairs.

Clingendael & KPMG. (2019). Gaming the new security nexus (tech. rep.). Dutch Transformation Forum. https://www.clingendael.org/publication/gaming-new-security-nexus

Clingendael & KPMG. (2019). Gaming the new security nexus. Dutch Transformation Forum. https://www.clingendael.org/publication/gaming-new-security-nexus

Coburn, A., Leverett, E., & Woo, G. (2018). Solving cyber risk: protecting your company and society. John Wiley & Sons.

Coiera, E. (2007). Putting the technical back into socio-technical systems research. International journal of medical informatics, 76, S98-S103.

Crowston, K., & Kammerer, E. E. (1998). Coordination and collective mind in software requirements development. IBM Systems Journal, 37(2), 227-245.

D'Andrea, A., & Limodio, N. (2023). High-Speed Internet, Financial Technology, and Banking. Management Science.

Danielsson, J., Hartmann, P., & De Vries, C. G. (2001). The cost of conservatism: Extreme returns, value-at-risk and the Basle 'multiplication factor'. Risk, 14(1), 101-103.

Dapp, T., Slomka, L., AG, D. B., & Hoffmann, R. (2014). Fintech–The digital (r) evolution in the financial sector. Deutsche Bank Research, 11, 1-39.

Davis, M. C., Challenger, R., Jayewardene, D. N., & Clegg, C. W. (2014). Advancing socio-technical systems thinking: A call for bravery. Applied Ergonomics, 45(2), 171-180.

Deloitte GmbH Wirtschaftsprüfungsgesellschaft. (2021). Report on the external review of TARGET Services in the context of the incidents in March, May, August, October, and November 2020. European Central Bank.

DNB (2023) What are the Target Services? https://www.dnb.nl/en/sector-information/cash-and-payment-systems/target-services-t2-t2s-tips/what-are-the-target-services/

Dorfleitner, G., Hornuf, L., Schmitt, M., Weber, M., Dorfleitner, G., Hornuf, L., & Weber, M. (2017). Definition of FinTech and description of the FinTech industry. FinTech in Germany, 5-10.

Drew, R. (2016). Technological determinism. A companion to popular culture, 165-183.

Emery, F. E., & Trist, E. L. (1960). Socio-technical systems. In C. W. Churchman & M. Verhulst (Eds.), Management sciences, models and techniques (pp. 83-97). Pergamon.

en Veiligheid, N. C. T. (2019). Nationale Veiligheid Strategie (tech. rep.). Ministrie Van Justitie en Veiligheid.

Etienne, J. (2011). Compliance theory: A goal framing approach. Law & Policy, 33(3), 305-333.

Evenett, S. J., & Hoekman, B. M. (2004). Economic Development and Multilateral Trade Cooperation. World Bank and Palgrave Macmillan.

Fahrholz, C. H., & Freytag, A. (2011). Whither the TARGET2 System? Taking a Glance at the Real Economic Facets of the Euro-Area Debt Crisis. Applied Economics Quarterly.

Fahrholz, C. H., & Freytag, A. (2012). Will TARGET2-Balances be Reduced again after an End of the Crisis? Research Papers in Economics

Fåk, V. (2010). IT–Risks and Security. In Risks in Technological Systems (pp. 143-160). London: Springer London.

Faraj, S., & Xiao, Y. (2006). Coordination in fast-response organizations. Management Science, 52(8), 1155-1169.

Fjäder, C. O. (2016). National security in a hyper-connected world: Global interdependence and national security. Exploring the security landscape: Non-traditional security challenges, 31-58.

Flechais, I., Riegelsberger, J., & Sasse, M. A. (2005, September). Divide and conquer: the role of trust and assurance in the design of secure socio-technical systems. In Proceedings of the 2005 workshop on New security paradigms (pp. 33-41).

Friedman, M., & Schwartz, A. J. (1964). A Monetary History of the United States, 1867-1960. Economica, 31(123), 314. https://doi.org/10.2307/2550627

Furfine, C. H., & Stehm, J. (1998). Analyzing alternative intraday credit policies in real-time gross settlement systems. Journal of Money, Credit and Banking, 832-848.

Gai, P., Haldane, A., & Kapadia, S. (2013). Complexity, concentration and contagion. Journal of Monetary Economics, 58(5), 453-470.

Galbiati, M., & Stanciu-Vizeteu, L. (2015). Communities and driver nodes in the TARGET2 payments system. Journal of Financial Market Infrastructures, 3(4).

Garcia-de-Andoain, C., Heider, F., Hoerova, M., & Manganelli, S. (2015). Lending-of-Last-Resort is as Lending-of-Last-Resort Does: Central Bank Liquidity Provision and Interbank Market Functioning in the Euro Area. European Finance eJournal.

Garcia-de-Andoain, C., Heider, F., Hoerova, M., & Manganelli, S. (2015). Lending-of-Last-Resort Is as Lending-of-Last-Resort Does: Central Bank Liquidity Provision and Interbank Market Functioning in the Euro Area. Banking & Insurance eJournal.

Geels, F. W. (2004). From sectoral systems of innovation to socio-technical systems: Insights about dynamics and change from sociology and institutional theory. Research policy, 33(6-7), 897-920.

Geels, F. W. (2005). Processes and patterns in transitions and system innovations: Refining the co-evolutionary multi-level perspective. Technological Forecasting and Social Change, 72(6), 681–696. https://doi.org/10.1016/j.techfore.2004.08.014

Glowka, M., Müller, A., Friz, L. P., Testi, S., Valentini, M., & Vespucci, S. (2022). TARGET2 analytical tools for regulatory compliance. ECB Occasional Paper, (2022/300).

Gonzalez-Granadillo, G., Dubus, S., Motzek, A., Garcia-Alfaro, J., Alvarez, E., Merialdo, M., ... & Debar, H. (2018). Dynamic risk management response system to handle cyber threats. Future Generation Computer Systems, 83, 535-552.

Goodman, S. E. (2010). Cybersecurity: A National Security Issue. In Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy

Gortsos, C. (2020). The Basic Tasks of the European Central Bank Within the Eurosystem and Issuance of Banknotes and Coins.

Greer, B. I. (1986). European Economic Security. Harvard University. https://doi.org/10.4324/9781003099796-13

Greer, B. I. (1986). European Economic Security. Harvard University. https://doi.org/10.4324/9781003099796-13

Griffith, T. L., & Dougherty, D. (2001). Beyond socio-technical systems: introduction to the special issue. Journal of Engineering and Technology Management, 18(3-4), 207–218. https://doi.org/10.1016/s0923-4748(01)00034-0

Grimsley, M., Meehan, A., & Gupta, K. (2006). Evaluative design of e-government projects: A public value perspective. In Proceedings of the Annual Hawaii International Conference on System Sciences (HICSS) (pp. 152c-152c).

Habib, I. (1999). The Agrarian System of Mughal India 1556-1707. http://ci.nii.ac.jp/ncid/BA2145028X

Hale, A., & Borys, D. (2013). Working to rule, or working safely? Part 1: A state of the art review. Safety science, 55, 207-221.

Hallegatte, S., Rentschler, J., & Rozenberg, J. (2017). Lifelines: The Resilient Infrastructure Opportunity. World Bank

Handig, M., Holzfeind, R., & Jobst, C. (2012). Understanding TARGET 2: The Eurosystem's Euro Payment System from an Economic and Balance Sheet Perspective. Monetary Policy & the Economy.

Hanseth, O., Aanestad, M., & Berg, M. (2004). Guest editors' introduction: Actor-network theory and information systems. What's so special?. Information technology & people, 17(2), 116-123.

Hanushek, E. A., & Woessmann, L. (2008). The Role of Cognitive Skills in Economic Development. Journal of Economic Literature.

Hardie, D. (2020). ECB says Target2 outage was caused by third-party network device. https://www.centralbanking.com/central-banks/financial-market-infrastructure/7703461/ecb-says-target2-outage-was-caused-by-third-party-network-device

Hausken, K. (2017). Defense and attack for interdependent systems. European Journal of Operational Research, 256(2), 582-591.

Heidegger, M. (1954). The question concerning technology. Garland Publishing.

Heijmans, R., & Heuver, R. (2011). Is this Bank Ill? The Diagnosis of Doctor TARGET2. European Finance eJournal.

Heijmans, R., & Wendt, F. (2020). Measuring the Impact of a Failing Participant in Payment Systems. Financial Crises eJournal.

Heijmans, R., & Wendt, F. (2023). Measuring the impact of a failing participant in payment systems. Latin American Journal of Central Banking, 4(4), 100106.

Heijmans, R., Heuver, R., & Levallois, C. (2016). Dynamic visualization of large financial networks.

Heijmans, R., Heuver, R., & Walraven, D. (2010). Monitoring the Unsecured Interbank Money Market Using Target2 Data. Mutual Funds.

Heilbroner, R. L., & Milberg, W. (2008). The making of economic society. Prentice Hall.

Hobbes, T. (1651). Leviathan.

Hoorens, S., Retter, L., Lynch, A., Frinking, E. J., Nederveen, F., & Phillips, W. D. (2020). Relationships between the economy and national security: Analysis and considerations for economic security policy in the Netherlands.

Hristov, N., Hülsewig, O., & Wollmershäuser, T. (2018). Capital Flows in the Euro Area and TARGET2 Balances. Monetary Economics: International Financial Flows.

Huber, G. P. (1990). A theory of the effects of advanced information technologies on organizational design, intelligence, and decision making. Academy of management review, 15(1), 47-71.

Hull, J. C. (2015). Risk management and financial institutions (Vol. 733). John Wiley & Sons.

Impenna, C., & Masi, P. (1997). Risks in Interlinked Settlement Systems: How to Measure the Impact of Settlement Delay in the Italian RTGS System (BIREL).

Ioan-Franc, V., & Diamescu, M. A. (2010). Some opinions on the relation between security economy and economic security. Revista Romana de Economie, 31(2).

Jobst, C., Handig, M., & Holzfeind, R. (2012). Understanding tarGet2: the eurosystem's euro Payment System from an economic and Balance Sheet Perspective. Monetary Policy & the economy Q, 1, 81-91.

Jobst, C., Handig, M., & Holzfeind, R. (2012). Understanding tarGet2: the eurosystem's euro Payment System from an economic and Balance Sheet Perspective. Monetary Policy & the economy Q, 1, 81-91.

Justitie van en Veiligheid, M. (2021). Overzicht vitale processen. https://www.nctv.nl/onderwerpen/vitale-infrastructuur/overzicht-vitale-processen

Justitie van en Veiligheid, M. (2022). Vitale infrastructuur. https://www.nctv.nl/onderwerpen/vitale-infrastructuur

Kaminska, I. (2019). How RTGS inadvertently killed system liquidity. https://www.ft.com/content/36e15d64-8052-3808-83bc-6a1d30089b3c

Katman, F. (2015). ON SECURITY: Security in the Age of Ambiguity. In Global challenges to the Transatlantic World (pp. 39-47). Editorial Universidad de Alcalá.

Kaufman, H. (2021). Red Tape: Its Origins, Uses, and Abuses. Brookings Institution Press.

Kaufmann, D., Kraay, A., & Mastruzzi, M. (1999). Governance Matters. World Bank.

Kelly, L. R. (2016). Inside the pipeline that transfers 2.7 billion euros a minute. https://www.bloomberg.com/news/articles/2016-09-21/inside-the-pipeline-that-transfers-2-7-billion-euros-a-minute?leadSource=uverify%20wall#xj4y7vzkg

Keynes, J. M. (1936). The General Theory of Employment, interest and Money. Political Science Quarterly, 51(4), 600–602. https://doi.org/10.2307/2143949

Khiaonarong, M. T., & Humphrey, D. (2022). Instant Payments: Regulatory Innovation and Payment Substitution Across Countries. International Monetary Fund.

Kivimaa, P., Brisbois, M. C., Jayaram, D., Hakala, E., & Siddi, M. (2022). A socio-technical lens on security in sustainability transitions: Future expectations for positive and negative security. Futures, 141, 102971.

Koponen, R. (2012). TARGET2-Securities moving ahead on schedule.

Korol, I., & Poltorak, A. (2018). Financial risk management as a strategic direction for improving the level of economic security of the state. Baltic Journal of Economic Studies, 4(1), 235-241.

Krarup, T. (2019). Between competition and centralization: the new infrastructures of European finance. Economy and Society, 48(1), 107-126.

Krarup, T. (2019). Between competition and centralization: the new infrastructures of European finance. Economy and Society, 48(1), 107-126.

Kregel, J. (2019). Globalization, Nationalism, and Clearing Systems. The Review of Keynesian Studies, 1, 1-21.

Krüger, P. S., & Brauchle, J. P. (2021). The European Union, cybersecurity, and the financial sector: A primer. .

Kuhnle, S. (2004). The survival of the European Welfare State. Routledge.

Laplante, P., & Amaba, B. (2021). Artificial intelligence in critical infrastructure systems. Computer, 54(10), 14-24.

Laugé, A., Hernantes, J., & Sarriegi, J. M. (2015). Critical infrastructure dependencies: A holistic, dynamic and quantitative approach. International Journal of Critical Infrastructure Protection, 8, 16-23.

Law, J., & Singleton, V. (2000). Performing technology's stories: On social constructivism, performance, and performativity. Technology and culture, 41(4), 765-775.

Lee, G., DeLone, W., & Espinosa, J. A. (2007). Ambidextrous coping strategies in globally distributed software development projects. Communications of the ACM, 50(10), 35-40.

Lee, J. (1991). Financial Sector and Economic Development: A Survey. https://www.adb.org/publications/financial-sector-and-economic-development-survey

Leffler, M. P. (1990). National security. The Journal of American History, 77(1), 143-152.

Leonardi, P. M. (2012). Materiality, sociomateriality, and socio-technical systems: What do these terms mean? How are they related? Do we need them?. Materiality and organizing: Social interaction in a technological world, 25, 48-75.

Leonardi, P.M. & Barley, S.R. (2008). Materiality and change: Challenges to building better theory about technology and organizing. Information and Organization, 18(3), 159-176.

Liu, F., Maitlis, S., & Selzer, J. (2010). Bridging the rhetorical gap: How senior managers craft communication. Harvard Business School Organizational Behavior Unit Working Paper, 11-031.

Lubik, T., & Rhodes, K. (2012). TARGET2: symptom, not cause, of eurozone woes. Richmond Fed Economic Brief.

Lucarelli, B. (2017). Intra-eurozone payments imbalances: Implications for the TARGET2 payments system. Review of Radical Political Economics, 49(3), 343-357.

Luiijf, E., Burger, H., & Klaver, M. (2003). Critical (information) infrastructure protection in the Netherlands, 9–19.

Lynch, M. (2016). Social constructivism in science and technology studies. Human Studies, 39, 101-112.

Lyytinen, K., Mathiassen, L., & Ropponen, J. (1998). Attention shaping and software risk—a categorical analysis of four classical risk management approaches. Information systems research, 9(3), 233-255.

Maglaras, L. A., Kim, K. H., Janicke, H., Ferrag, M. A., Rallis, S., Fragkou, P., & Cruz, T. J. (2018). Cyber security of critical infrastructures. Ict Express, 4(1), 42-45.

Majchrzak, A., Rice, R. E., Malhotra, A., King, N., & Ba, S. (2000). Technology adaptation: The case of a computer-supported inter-organizational virtual team. MIS quarterly, 24(4), 569-600.

Martin, D., Christoph, H., & Katharina, T. (2019). The consolidation of TARGET2 and TARGET2-Securities: How is the Eurosystem exploring synergies across its infrastructures, and how will this impact day-to-day operations?. Journal of Securities Operations & Custody, 11(3), 198-212.

Martins, B. O., & Ahmad, N. (2020). The security politics of innovation: Dual-use technology in the EU's security research programme. Emerging security technologies and EU governance: Actors, practices and processes. Oxon, New York: Routledge, 58-73.

Massarenti, M., Petriconi, S., & Lindner, J. (2012). Intraday Patterns and Timing of TARGET2 Interbank Payments.

Masselink, M., & van den Noord, P. (2009). The global financial crisis and its effects on the Netherlands. ECFIN Country Focus, 6(10), 1-7.

Mazzucato, M. (2018). The Value of Everything: Making and Taking in the Global Economy. Penguin

McPartland, J. (2005). Liquidity algorithms: a tale of two countries. Chicago Fed Letter, (Sep).

McPhail, K. (2003). Managing operational risk in payment, clearing, and settlement systems (No. 2003-2). Bank of Canada.

McSweeney, B. (1996). Identity and security: Buzan and the Copenhagen school. Review of international studies, 22(1), 81-93.

Medar, L.-I., & Chirtoc, I. (2017). The Development Of The European Banking Industry Through The Target Payments System. Annals - Economy Series.

Mennen, M. G., & Van Tuyll, M. C. (2015). Dealing with future risks in the Netherlands: the National Security Strategy and the National Risk Assessment. Journal of Risk Research, 18(7), 860-876.

Merabti, M., Kennedy, M., & Hurst, W. (2011, March). Critical infrastructure protection: A 21 st century challenge. In 2011 International Conference on Communications and Information Technology (ICCIT) (pp. 1-6). IEEE.

Mersch, Y. (2016). Making Europe's financial market infrastructure a bulwark of financial stability. Financial Stability Review.

Mierau, J., & Mink, M. (2018). A Descriptive Model of Banking and Aggregate Demand. De Economist, 166, 207-237.

Mintzberg, H. (1979). The structuring of organizations. Englewood Cliffs, NJ: Prentice hall.

Mokyr, J. (1990). The Lever of Riches: Technological Creativity and Economic Progress. Oxford University Press

Moro, B. (2016). The European Crisis and the Accumulation of TARGET2 Imbalances.

Moteff, J. D. (2007). Risk management and critical infrastructure protection: Assessing, integrating, and managing threats, vulnerabilities and consequences. Congressional Research Service, The Library of Congress.

Moteff, J. D., Copeland, C., Fischer, J. W., & Resources, Science, and Industry Division. (2003, January). Critical infrastructures: What makes an infrastructure critical?. Washington, DC: Congressional Research Service, Library of Congress.

Nanaeva, Z., Aysan, A. F., & Shirazi, N. S. (2021). Open banking in Europe: the effect of the revised payment services directive on Solarisbank and Insha. Journal of Payments Strategy & Systems, 15(4), 432-444.

Newman, E. (2005). Human security: mainstreamed despite the conceptual ambiguity?. St Antony's International Review, 1(2), 24-36.

O'Brien, H. L., & Toms, E. G. (2008). What is user engagement? A conceptual framework for defining user engagement with technology. Journal of the American society for Information Science and Technology, 59(6), 938-955.

Oiecevici, O., Calefariu, G., & Burcă, C. (2020). Monitoring the IT Systems for High Availability and Optimal Performances. Informatica Economica, 24(2), 5-16.

Ottens, M., Franssen, M., Kroes, P., & Van De Poel, I. (2006). Modelling infrastructures as socio-technical systems. International journal of critical infrastructures, 2(2-3), 133-145.

Panourgias, N. S. (2015). Capital markets integration: A sociotechnical study of the development of a cross-border securities settlement system. Technological forecasting and social change, 99, 317-338.

Parać Vukomanović, I. (2019). NEW SERVICES OFFERED WITHIN THE REMIT OF TARGET2 – HOW DO THEY CORRESPOND WITH TFEU AND CENTRAL BANK TASKS? EU AND MEMBER STATES – LEGAL AND ECONOMIC ISSUES.

Parker, C. & Nielsen, V. L. (2011). Explaining Compliance: Business Responses to Regulation. Edward Elgar Publishing.

Pasmore, W.A. et al. (2019). Socio-technical systems in an age of complexity: A systems inquiry into how organizations can foster innovation, resilience, and human fulfillment. Human Relations, 72(10), 1543-1573.

Perrow, C. (2011). Normal accidents: Living with high risk technologies. Princeton university press.

Peterson, R.R. (2004). Crafting information technology governance. Information Systems Management, 21(4), 7-22.

Pezzuto, I. (2019). Turning globalization 4.0 into a real and sustainable success for all stakeholders.

Poncelet, P. (2008). The Contribution of TARGET2 to European Integration. European Banking Federation, Paris.

Popelo, O., Dubyna, M., & Kholiavko, N. (2021). World experience in the introduction of modern innovation and information technologies in the functioning of financial institutions. Baltic Journal of Economic Studies, 7(2), 188-199.

Prewett, K. W., Prescott, G. L., & Phillips, K. (2020). Blockchain adoption is inevitable—Barriers and risks remain. Journal of Corporate accounting & finance, 31(2), 21-28.

Rajendran, P., Kamalendran, S., & Subramaniam, S. R. (2019). Incident management in cloud computing. Journal of Network and Systems Management, 27(2), 234-269.

Rehak, D., Markuci, J., Hromada, M., & Barcova, K. (2016). Quantitative evaluation of the synergistic effects of failures in a critical infrastructure system. International Journal of Critical Infrastructure Protection, 14, 3-17.

Renn, O. (1998). The role of risk perception for risk management. Reliability engineering & system Safety, 59(1), 49-62.

Repousis, S. (2016). Money laundering and Greek banking payment and settlement systems. Journal of Money Laundering Control.

Retter, L., J. Frinking, E., Hoorens, S., Lynch, A., Nederveen, F., & D. Phillips, W. (2020). Relationships between the economy and national security. RAND Corporation. https://www.rand.org/pubs/research_reports/RR4287.html

Romer, C. D. (1993). The nation in depression. Journal of Economic Perspectives, 7(2), 19–39. https://doi.org/10.1257/jep.7.2.19

Ronis, S. R. (2011). Economic Security Neglected Dimension of National Security?. Smashbooks.

Rooj, D., & Sengupta, R. (2020). THE REAL-TIME IMPACT ON REAL ECONOMY—A MULTIVARIATE BVAR ANALYSIS OF DIGITAL PAYMENT SYSTEMS AND ECONOMIC GROWTH IN INDIA. Asian Development Bank Institute. https://www.adb.org/sites/default/files/publication/602111/adbi-wp1128.pdf

Ropohl, G. (1999). Philosophy of socio-technical systems. Society for Philosophy and Technology Quarterly Electronic Journal, 4(3), 186-194.

Rothschild, E. (1995). What is Security. Daedalus, 124(3). http://connections-qj.org/article/what-security

Sauro, J., & Lewis, J. R. (2016). Quantifying the user experience: Practical statistics for user research. Morgan Kaufmann.

Scott, S.V. & Zachariadis, M. (2012). Origins and development of SWIFT, 1973–2009. Business History, 54(3), 462-482.

Sherman, A. T., DeLatte, D., Neary, M., Pham, L., & Oliva, L. (2009). Security for service oriented architectures. SANS Institute.

Simpson, S.S. (2002). Corporate crime, law, and social control. Cambridge University Press.

Siponen, M., & Oinas-Kukkonen, H. (2007). A review of information security issues and respective research contributions. ACM Sigmis Database, 38(1), 60-80.

Sony, M., & Naik, S. (2020). Industry 4.0 integration with socio-technical systems theory: A systematic review and proposed theoretical model. Technology in society, 61, 101248.

Vukomanović, I. P. (2019). NEW SERVICES OFFERED WITHIN THE REMIT OF TARGET2 – HOW DO THEY CORRESPOND WITH TFEU AND CENTRAL BANK TASKS? EU AND MEMBER STATES – LEGAL AND ECONOMIC ISSUES.

Whelan, K. (2014). TARGET2 and Central Bank Balance Sheets. European Economics: Macroeconomics & Monetary Economics eJournal.

Whittaker, J. (2016). Eurosystem Debts Do Matter. European Finance eJournal.

Appendix

A.1 Description of Technical and Social Components from Table 4.1

Technical Components

Core platforms

1. SSP (Single Shared Platform): The SSP functions as the technological backbone of the TARGET2 system, facilitating real-time gross settlement of high-value Euro transactions across European banks. It's a robust and sophisticated infrastructure, ensuring the seamless execution of interbank payments. The platform operates on a dual-site configuration, providing geographical redundancy to guarantee uninterrupted service and resilience against system failures. This setup is crucial for maintaining the integrity and reliability of the European financial system.

2. 2. TIPS (TARGET Instant Payment Settlement): TIPS is an advanced, real-time settlement system designed by the Eurosystem to process instant payments, specifically SEPA Instant Credit Transfers. It operates continuously, providing 24/7/365 availability to handle immediate transaction demands. The system's architecture is notable for its self-healing capabilities, distributed across multiple sites for enhanced performance and fault tolerance. This platform represents a significant leap in payment technology, offering unprecedented speed and reliability in processing instant payments.

3. T2S (TARGET2-Securities): T2S stands as a pivotal component in the European financial landscape, centralizing the settlement of securities transactions in central bank money. It's engineered to facilitate both Delivery-versus-Payment (DvP) and Free-of-Payment (FoP) settlement types for Central Securities Depositories (CSDs). The platform is instrumental in managing the cash leg of securities trading, ensuring efficient and secure transfer of funds corresponding to securities transactions. Operated on a unified platform by the 4CB (four central banks), T2S aims to harmonize and streamline post-trade processes across Europe, enhancing the efficiency and stability of securities markets.

These platforms collectively underpin the European financial infrastructure, each playing a specialized role in ensuring the fluidity, security, and efficiency of financial transactions, whether in the realm of high-value payments, instant transactions, or securities settlement.

Interfaces

1. T2SI (T2S Interface): T2SI acts as the crucial link for technical connectivity and message exchange between the SSP and the T2S platform. It plays a key role in ensuring seamless coordination and integrated liquidity management between the Payment Module (PM) accounts in TARGET2 and the Dedicated Cash Accounts (DCAs) in T2S. Utilizing the ISO 20022 XML messaging standard, T2SI facilitates efficient, secure, and standardized communication, crucial for the smooth operation of cross-platform transactions and liquidity management in the European financial system.

2. TIPSI (TIPS Interface): TIPSI establishes the necessary application-to-application connections between the SSP and the TIPS platform, essential for executing liquidity transfers. This interface enables the interoperability between the Real-Time Gross Settlement (RTGS) system of TARGET2 and the instant payment settlement mechanism of TIPS. Through TIPSI, transfers are efficiently settled by direct debits and credits on the transit accounts, ensuring a fluid and reliable process for managing liquidity across these two platforms.

3. ASI (Ancillary System Interface): ASI provides a specialized settlement channel that allows various ancillary systems to integrate with the SSP. It supports a diverse array of settlement procedures, each specifically designed to meet the unique requirements of different ancillary system (AS) transaction flows. Leveraging XML messaging for communication, ASI ensures that these systems can securely and effectively settle transactions via the SSP, catering to a wide range of financial services and needs within the European market infrastructure.

These interfaces, T2SI, TIPSI, and ASI, are integral to the cohesion and functionality of the European financial infrastructure. They enable the robust platforms of SSP, TIPS, and T2S to interact seamlessly, ensuring that the entire system operates smoothly and efficiently, from high-value interbank payments to instant payments and securities settlements.

Networks

1. SWIFTNet: SWIFTNet serves as the primary messaging network for participants engaging with the SSP, facilitating the exchange of payment instructions and system-related messages. It offers various communication services, such as FIN, Interact, and FileAct, each tailored to different types of messaging requirements. This network is pivotal in providing widespread, reliable access, ensuring that participants can seamlessly and securely transmit their financial messages across the globe. Its robustness and ubiquity make it a cornerstone in the international financial communication infrastructure.

2. ESMIG (Eurosystem Single Market Infrastructure Gateway): ESMIG functions as a secure, unified gateway for various market actors to access the TIPS platform and other Eurosystem market infrastructures. It's responsible for crucial tasks like authentication, authorization, as well as the validation and routing of messages. By streamlining these processes, ESMIG plays a vital role in enhancing the efficiency and security of the communication network, supporting the seamless operation of the Eurosystem's market infrastructures. Its implementation marks a significant step towards a more integrated and efficient European financial market.

Applications

1. ICM (Information and Control Module): The ICM is a key application within the SSP, offering direct participants and ancillary systems a comprehensive platform to monitor their activities, account balances, and transactions. It also enables the initiation of payments, particularly under contingency scenarios. The ICM is versatile, supporting both User-to-Application (U2A) and Application-to-Application (A2A) modes, thereby catering to a range of user preferences

and technical requirements. This module is essential for ensuring that participants maintain continuous oversight and control over their operations within the TARGET2 system.

2. CRISP (Cost Recovery Information System for Pricing): CRISP plays a crucial role in the financial management of the Eurosystem's market infrastructures. It's tasked with generating detailed billing data, creating invoices, and providing operational statistics to central banks. These functions are vital for operational controlling and cost monitoring, enabling a transparent and efficient approach to cost recovery. By providing clear insights into usage and associated costs, CRISP helps maintain financial accountability and transparency across the system.

3. GUI (Graphical User Interface): For both the TIPS and T2S platforms, dedicated Graphical User Interfaces are provided to enhance user experience and efficiency. These interfaces allow users to manage transactions and liquidity with ease, monitor settlement processes, and access important reporting data. The GUIs are designed to be user-friendly, ensuring that complex financial transactions and data monitoring are accessible and manageable, thereby facilitating smoother operations for all users involved in these platforms.

Static Data and Databases

1. Reference Data: This category includes essential information such as participant details and configuration data, which encompasses account master data, directory entries, and system settings crucial for the smooth functioning of the platforms. In the SSP, this data is housed within the Static Data module. For the TIPS platform, similar reference data is managed through the Central Routing Directory Management (CRDM) system. This data forms the backbone of the system's operational integrity, ensuring that all transactions and interactions are based on current and accurate information.

2. Directories: These are specialized databases that store Bank Identifier Code (BIC) routing information, which is key to directing payment flows among participants in the respective schemes. The TARGET2 directory is used for routing PM (Payment Module) payments, while the TIPS directory is dedicated to routing instant payments. These directories are updated regularly to reflect any changes, ensuring efficient and accurate routing of payments across the network.

3. Account Balances: This critical data set includes information on liquidity positions, turnover, and transactions for various accounts such as PM accounts, TIPS Dedicated Cash Accounts (DCA), T2S DCAs, and others. This information is vital for monitoring liquidity, facilitating settlement processes, and conducting reconciliation activities. Accurate and up-to-date account balance data is essential for the effective management of liquidity and financial resources within these platforms.

4. Transaction Logs: These logs provide comprehensive and detailed records of all transactions that are settled or processed, whether at the platform, account, or overall system level. These logs serve as an audit trail, supporting crucial functions like oversight, reconciliation, and operational monitoring. They are fundamental to maintaining transparency, ensuring

accountability, and facilitating the analysis and resolution of any discrepancies or issues that may arise in the transaction process.

Settlement Algorithms

In systemic payment clearing and settlement systems such as TARGET2, settlement algorithms play a critical role. They encapsulate a set of predefined rules and procedures that dictate how payments are managed within the system. These algorithms determine the order in which payments are accepted, queued, processed, and potentially rejected. The design and implementation of these algorithms are crucial for ensuring the efficiency and reliability of the settlement process. They must adeptly handle a variety of payment scenarios, balancing priorities such as liquidity availability, transaction urgency, and counterparty risk. By effectively managing these factors, settlement algorithms help maintain the smooth operation and stability of financial clearing and settlement systems.

Social Elements

Users

1. Direct Participants: These entities are key players in the European financial infrastructure, holding accounts across various platforms for different types of transactions. They maintain Payment Module (PM) accounts for Euro transactions within TARGET2, TIPS Dedicated Cash Accounts (DCAs) for instant payments, and T2S DCAs for managing the cash leg of securities transactions. Direct participants have the capability to connect directly to these platforms using various secure communication channels, such as SWIFT, the TIPS Network Service Provider (NSP), or Value-Added Network Service Providers (VAN-SP). This direct connection underscores their integral role in the financial ecosystem, facilitating efficient and secure transaction processing.

2. Indirect Participants: These participants engage with the TARGET2 system through a direct PM participant. They do not hold their own PM accounts; instead, they execute their send and receive payment transactions through the PM account of a direct participant. This arrangement allows indirect participants to be part of the Euro transaction system, leveraging the infrastructure and access provided by direct participants. It's a model that enables broader participation in the financial system, especially for entities that may not require or have the capacity for direct platform access.

3. Ancillary Systems: This term refers to a diverse group of entities, including retail payment systems and securities settlement systems, among others. These systems are crucial for the settlement of the cash leg of various types of financial transactions. They connect to the SSP (Single Shared Platform) using a dedicated interface, designed to handle their specific settlement needs and transaction flows. The integration of ancillary systems into the broader financial infrastructure via the SSP is vital for the comprehensive and efficient processing of a

wide range of transaction types, enhancing the overall robustness and capability of the European financial system.

Governance Bodies

1. Level 1 - The ECB Governing Council: This body is at the pinnacle of the governance structure, offering strategic guidance and making final decisions on high-level policies and rules for TARGET2. The ECB Governing Council's role is crucial as it sets the direction and framework within which the TARGET2 system operates, ensuring that it aligns with broader monetary and financial policies.

2. Level 2 - The Market Infrastructure Board: Operating under the delegation from Level 1, the Market Infrastructure Board plays a significant role in the management of TARGET2. It is responsible for subsidiary decision-making on various aspects, providing a more focused and detailed oversight than the broader strategic guidance of Level 1. This board ensures that TARGET2's operations are in line with the strategic direction set by the ECB Governing Council.

3. Level 3 - The SSP/TIPS/T2S providing central banks: These banks are tasked with the technical and operational management of the respective platforms - SSP, TIPS, and T2S. Their management is within the scope and mandates provided by the higher governance levels. This level is where the day-to-day running of the platforms takes place, dealing with technicalities, operational challenges, and ensuring the smooth functioning of these critical financial infrastructures.

Operational Roles

1. Settlement managers: These individuals are responsible for the management, monitoring, and oversight of the daily functioning of settlement processes. Their roles encompass a broad range of activities including the provision of liquidity, overseeing payment flows, and handling transactions from ancillary systems (AS). Settlement managers play a critical role in ensuring that the settlement processes run smoothly and efficiently, maintaining the stability and reliability of the financial system.

2. Service desks: The service desks act as the primary point of contact for operational assistance and technical support for users of the system. They handle a variety of tasks such as assisting with system access, incident reporting, and managing static data. Their role is crucial in providing timely and effective support to ensure uninterrupted system operations and to help users navigate and resolve any issues or queries related to the system.

Organizational Processes

1. Governance: This involves high-level direction setting and decision-making processes. It includes articulating policies and rules to ensure the system functions align with user needs and adhere to the principles of safety, efficiency, and stability. Governance is key to maintaining the integrity and effectiveness of the system.

2. Operations: This refers to the day-to-day management and oversight of settlement flows, infrastructure monitoring, and user coordination to ensure smooth system functioning. Settlement managers are integral to this process, playing a vital role in maintaining operational fluency.

3. Testing: This encompasses a range of activities such as certification testing, integration testing, and user acceptance testing. These tests are performed by both users and operators to validate various system components before they are officially launched in a production environment. Testing is crucial for ensuring that new components integrate seamlessly and function as intended.

4. Change management: This is a managed, consultative process focused on determining the content of new releases, planning, and coordinating changes with all stakeholders. The goal is to continually meet user needs while protecting the operational stability of the system. Effective change management is essential for adapting to evolving requirements and maintaining the resilience of the system.

Communication Flows

1. Status updates and notifications: These are essential communication tools used to keep users informed about the ongoing progress of settlements, as well as any incidents or problems that require awareness or action. They play a crucial role in ensuring that all participants are up-to-date and can respond appropriately to any changes or issues.

2. Queries and requests: This form of communication allows users to seek support, information, or assistance regarding the operations of the system. It's a vital channel for users to address concerns, clarify doubts, and ensure their operational needs are met effectively.

3. Broadcasts and circulars: These are used to inform stakeholders about important decisions, events, and to disseminate critical operational instructions from system operators. Broadcasts and circulars are key to ensuring that all relevant parties are aware of and understand significant updates or changes in the system.

4. Messaging: This enables the exchange of instruction messages and information both within and between the technical components of the system and its users. Messaging is fundamental to the operation of the system, facilitating the necessary communication that drives transaction processing, coordination, and management.

Operational Procedures

1. Normal settlement procedures: These are the standard, daily workflows and processes involved in the management of settlements, provision of liquidity, clearing of payments, and processing of transactions from ancillary systems (AS), among other tasks. They represent the routine, business-as-usual activities that ensure the smooth and efficient functioning of the system under normal conditions.

2. Incident response procedures: These procedures are activated when there are unusual technical or operational events. Designated actors or teams are responsible for implementing these measures with the aim to quickly resolve the issue and restore normal system functioning. These procedures are critical for maintaining system integrity and reliability in the face of disruptions.

3. Contingency/backup procedures: These are the plans and mechanisms put in place to ensure the continuation of critical processing during exceptional circumstances or system failures. They involve using alternative methods or systems, such as ECONS I or a contingency network, to maintain essential operations when standard procedures cannot be followed. Contingency and backup procedures are essential for ensuring operational resilience and continuity in the face of unforeseen challenges.

Governance Rules and Policies

1. Participation criteria: This set of rules determines the eligibility requirements for entities wishing to access the system, either directly or indirectly. It's designed to ensure that only qualified and capable actors are granted the privileges of using the system. By setting clear standards for participation, the system maintains a high level of integrity and efficiency.

2. Access policies: These are the regulations that specify the permissions, acceptable use, message flows, and other aspects related to system access for authorized user groups. Access policies play a crucial role in managing how different actors interact with the system, ensuring that each user's engagement is in line with the overall operational and security standards.

3. Security controls: These encompass the mandatory baseline requirements for cyber, physical, and operational security that all users must adhere to. Compliance with these controls is essential for ensuring the integrity and resilience of the system against various threats. By enforcing strict security standards, the system safeguards its operations and the interests of all participants.

Settlement finality rules: These rules legally define the moment when a settlement in central bank money becomes irrevocable, immutable, and enforceable. Settlement finality provides certainty to

participants, ensuring that once a transaction is completed, it is recognized as final and binding. This legal clarity is fundamental to the trust and reliability of the settlement process.

A.2 Data Tables

Table A.1 Identification and Categorization of Operations

S.No.	Category of Operations	Key Operations Performed
1	**Transaction Processing and Management:**	Payment processing
		Execution of real-time gross settlement algorithms
		Real-time gross settlement operations
		Daily activity monitoring on TARGET2 platforms
		Static data management for settlement
		Transaction management and incident communication
2	**Liquidity Management:**	Liquidity management
		Liquidity transfer risk management
3	**Risk and Compliance**	Incident communication and security compliance
		Operational risk management integration
		Compliance with participation principles
		Technical compliance and operational reliability
4	**System Governance and Strategic Oversight:**	Policy setting and strategic direction
		Oversight of system management
		Execution of operational roles
		Compliance with governance rules and policies
		Feedback engagement for system improvements

5	**Operational Integrity and Business Continuity:**	Interface and network management for transactions
		Monitoring and incident reporting for stability
		Technical performance monitoring and reporting
		Training and preparedness for users
6	**Communication and User Interface:**	Secure financial messaging
		Operational status updates

Table A.2 Key interactions based on operations facilitated

S.No.	Interaction	Supported/Facilitated Operations
1	Core Platforms and Users	Payment processing Liquidity management User interface for transactions
2	Governance Bodies and Operational Roles	Policy setting and strategic direction Oversight of system management Execution of operational roles
3	Communication Flows between Users and Technical Systems	Secure financial messaging Operational status updates User support and information dissemination
4	Interface and Network Reliability Impact on User Operations	Monitoring and incident reporting for stability Interface and network management for transactions
5	Static Data and Settlement Algorithms Alignment with Governance and Operational Procedures	Static data management for settlement Execution of real-time gross settlement algorithms
6	Applications and Operational Procedures	Daily activity monitoring on TARGET2 platforms Transaction management and incident communication

7	Settlement Algorithms and Risk Management	Real-time gross settlement operations Operational risk management integration Liquidity transfer risk management
8	User Interaction with Governance Rules and Policies	Compliance with participation principles Feedback engagement for system improvements Incident communication and security compliance
9	Organizational Processes and Technical Reliability	Technical compliance and operational reliability Technical performance monitoring and reporting

Table A.3 Key Socio-Technical Interactions within TARGET2

S.no.	Socio Technical Interaction	Technical Aspect	Social Aspect
1	**Core Platforms and Users**	**Infrastructure and Connectivity** - The technical infrastructure of TARGET2 is centred around the Single Shared Platform (SSP), which includes various modules essential for payment processing such as the PM, SF, RM, etc. (Page 22). - Connectivity is facilitated by interfaces like the T2S Interface (T2SI) and the TIPS Interface (TIPSI), which enable the exchange of liquidity and information between different platforms and the SSP (Page 23). - The use of XML messages compliant with the ISO 20022 standard ensures uniformity in system-to-system communication between TARGET2 and T2S (Page 42).	**User Participation** The system includes a wide range of users such as credit institutions, ancillary systems, and central banks, each with different roles and requirements for participation (Page 14). Users' operations rely on the interfaces and networks for executing transactions and managing liquidity, which necessitates a user-friendly and accessible system (Page 23).

		Access and Security - Users access the SSP via SWIFT or the internet, and the TIPS platform via a TIPS Network Service Provider, with security protocols in place to ensure safe transactions (Page 23). - Internet-based PM account holders must register with an Accredited Certification Authority, following specific security procedures (Page 52).	**Governance and Policy Compliance** The governance structure of TARGET2 involves multiple levels, including the Governing Council of the ECB and the Market Infrastructure Board (MIB), which set policies and oversee the system's functioning (Pages 21-22). Users must adhere to the governance rules and policies set by these bodies, ensuring compliance and operational integrity (Pages 21-22).
		Data Management Users are required to provide static data for participation, which involves filling out forms and submitting them to their respective Central Bank (Page 55).	**Feedback and Evolution** Users are involved in the annual TARGET2 release process, where consultations with the user community are conducted to collect proposals for functional changes (Page 148).

2	**Governance Bodies and Operational Roles**	**Governance Structure:** - TARGET2 management is based on a three-level governance scheme with tasks assigned to the Governing Council of the ECB (Level 1), the Eurosystem central banks (Level 2), and the SSP/TIPS platform providing central banks (Level 3) (Pages 20-22). - The Governing Council is responsible for the general management of TARGET2, while the Market Infrastructure Board (MIB) assists the Governing Council and performs tasks at Level 2 (Page 21). - Level 3 involves the daily running of the SSP/TIPS platform based on a predefined service level agreement (Page 22).	**Roles and Responsibilities:** - Central banks have multiple roles, including as a bank of banks, TARGET2 system owner, collateral manager, and settlement agent (Page 20). - The MIB has an advisory role and performs tasks related to the general management and operational aspects of TARGET2 (Page 21).

		Technical Infrastructure Management: - The SSP includes the payment and accounting processing services systems (PAPSS) and the customer-related services systems (CRSS) (Page 22). - Operational roles such as service desks manage the technical infrastructure for financial institutions and ensure compliance with security requirements (Pages 68, 159).	**Policy Implementation and Compliance:** - Governance bodies set policies and oversee the system's functioning, while operational roles implement these policies and manage daily operations (Pages 20-22). - Participants are responsible for managing the risk stemming from their participation and must self-certify their compliance with the security requirements (Page 159).
		Security and Operational Reliability: - The Eurosystem sets a framework for security and operational reliability, producing guidelines and specifying common requirements for all users (Page 66). - Requirements regarding information security management and business continuity management are specified for all participants (Pages 164-165).	**Training and Testing:** - Procedures and training are in place to ensure operational reliability, and the ability to cope with disruptions is tested at least once a year (Page 165).

3	**Communication Flows between Users and Technical Systems**	**Communication Infrastructure:** - TARGET2 uses different SWIFT channels for FIN messages and InterAct and FileAct files, allowing for continued processing in the event of specific failures (Pages 107-108). - The TARGET2 Information System (T2IS) provides information about the operational status of TARGET2 via the ECB Market Information Dissemination (MID) system, accessible to users and the public (Pages 27-28). - System-to-system communication between TARGET2 and T2S uses XML messages compliant with the ISO 20022 standard (Page 42).	**User Engagement and Support:** - National service desks act as the primary contact point for TARGET2 users, providing support and information (Pages 23-24). - The Settlement Managers Forum and crisis managers are part of the organizational structure to manage operations and incidents (Page 23).

		Contingency and Incident Management: - There is no contingency solution for TIPS related liquidity transfers in the event of a TIPS Interface failure, highlighting the importance of reliable communication channels (Page 107). - In abnormal situations, information flow is crucial, and TARGET2 users communicate with their central bank via national communication means (Page 107).	**Policy and Procedure Adherence:** - Users are informed about local communication channels by their National Central Bank (NCB), ensuring they are aware of how to communicate within the system (Page 27). - Participants are responsible for managing risks from their participation and must self-certify compliance with security requirements (Page 159).
		Security and Compliance: - Participants must regularly review their internal systems for compliance with information security policies and standards (Page 164). - Business continuity management requirements are specified for critical participants, ensuring communication reliability even during disruptions (Page 164).	**Training and Operational Readiness:** - Training and testing procedures are in place to ensure users are prepared for abnormal situations and can maintain communication (Page 165).

4	**Interface and Network Reliability Impact on User Operations**	**Monitoring and Incident Reporting:** - Continuous monitoring of TARGET2 components and incident reporting contribute to the system's stability and robustness (Page 76). - In case of operational disruptions, users are monitored by the relevant central bank, and incident reports are required to describe the problem, impact, resolution, and preventive actions (Page 76).	**Operational Management and Communication:** - Users communicate with their central bank via national communication means during incidents, ensuring the flow of information (Page 107). - Self-certification by participants is required to confirm compliance with security and business continuity requirements (Page 165).
		System Infrastructure and Contingency: - TARGET2 uses SWIFT channels for different types of messages, ensuring continued processing in case of specific failures (Pages 107-108). - No specific business continuity procedures for TIPS are foreseen, indicating the reliance on the reliability of the interfaces and networks (Page 124).	**Risk Management and Compliance:** - Participants manage risks from their participation and must self-certify compliance with security requirements (Page 159). - In the event of outsourcing, participants must ensure third-party compliance with the security requirements (Page 165).

		Security and Operational Reliability Measures: - The Eurosystem sets a framework for security and operational reliability, specifying common requirements for all users (Pages 66, 67). - Critical participants must have procedures to ensure critical business transactions can continue during disruptions (Pages 164-165).	**Training and Preparedness:** - Training and testing procedures are in place to ensure operational readiness and the ability to cope with disruptions (Page 165).

5	**Static Data and Settlement Algorithms Alignment with Governance and Operational Procedures**	**Settlement Infrastructure and Algorithms:** - TARGET2 is technically based on a Single Shared Platform (SSP) which includes the Payment and Accounting Processing Services Systems (PAPSS) and the Customer Related Services Systems (CRSS). The SSP ensures robustness and operational reliability for both domestic and cross-border payments (Pages 14, 22-23). - The system uses settlement algorithms that handle payments individually in real-time gross settlement (RTGS) mode, ensuring immediate finality of transactions (Page 14). - Static data related to settlement procedures, such as the setup and maintenance of auto-collateralization features in T2S, is crucial for the proper functioning of the settlement algorithms (Pages 90-91).	**Operational Management and Compliance:** - Each central bank has a settlement manager responsible for managing, monitoring, and communicating within the Eurosystem, ensuring that operational procedures align with technical requirements (Page 193). - Participants are required to self-certify compliance with security requirements, which includes the proper management of static data and the use of settlement algorithms (Pages 164-165).

		Governance and Operational Rules: - Harmonized conditions for the opening and operation of accounts in TARGET2 are laid down in various annexes, ensuring that static data and settlement algorithms align with these governance rules (Pages 11-12). - The Eurosystem provides specifications like the TARGET2 General Functional Specifications (GFS) and User Detailed Functional Specifications (UDFS) to guide the application of static data and settlement algorithms (Page 11).	**Risk Management and Training:** - Critical participants must have procedures to ensure that the most critical business transactions can continue during disruptions, which involves understanding and managing the static data and settlement algorithms (Pages 164-165). - Training and testing procedures ensure that staff are prepared to manage the static data and settlement algorithms effectively, especially in abnormal situations (Page 165).

6	**Applications and Operational Procedures**	**Applications for Monitoring and Transaction Management:** - TARGET2 users are responsible for monitoring their daily activities carried out in the SSP, TIPS platform, and T2S platform, which might be performed via the ICM for services at SSP level, the TIPS GUI for the TIPS platform, or the T2S GUI for services offered via the T2S Platform (Pages 89-90).	**Operational Procedures and User Responsibilities:** - Procedures during a normal business day are described according to the phases of the business day, with users responsible for the general monitoring of business and for meeting community needs (Page 89). - In abnormal situations, incident communication is critical. Users keep in touch with their usual contacts for operational management at their respective central bank via national communication means (Pages 106-107).
		Technical Compliance and Business Continuity: - Technical compliance reviews are conducted to ensure that internal systems used for sending/receiving TARGET2 payments are in line with information security policies and standards. Business continuity management is crucial, especially for critical participants who must have a business continuity strategy in place (Page 164).	**Training and Preparedness:** - The ability to cope with operational disruptions must be tested at least once a year, and critical staff must be aptly trained. Self-certifying institutions, which include TARGET2 participants, must assess which security requirements are applicable to their specific technical infrastructure and organizational setup (Pages 164-165).

7	**Settlement Algorithms and Risk Management**	**Settlement Infrastructure and Algorithms:** - TARGET2 is based on a Single Shared Platform (SSP), which includes the Payment and Accounting Processing Services Systems (PAPSS) and the Customer Related Services Systems (CRSS). This infrastructure supports the real-time gross settlement (RTGS) system, where payments are handled individually, providing immediate and final settlement of all payments, provided that there are sufficient funds or overdraft facilities available on the payer's account with its central bank (Pages 14, 22-23).	**Governance and Compliance:** - The Eurosystem's objectives include promoting the smooth operation of payment systems and contributing to the integration and stability of the euro money market, which involves risk management considerations (Page 14). - Participants are required to immediately inform the relevant Central Bank if they become subject to crisis prevention measures or crisis management measures, ensuring that risk management is integrated into the operational procedures (Page 87).
		Risk Management in Technical Operations: - The system is designed to minimize risk, including the risk of transaction failures or delays. This is achieved through the unconditional and immediate	**Operational Management and Communication:** - Each central bank has a settlement manager who is responsible for managing, monitoring,

		processing of payment orders on a continuous basis, ensuring the finality of transactions (Page 14). - T2S provides harmonized and commoditized securities settlement, applying a single set of rules and standards for the settlement of securities transactions across all markets it operates in, which includes the cash leg settled in central bank money (Page 17).	and communicating with other settlement managers within the Eurosystem, which includes risk management activities (Pages 192-193). - The TARGET2 Guideline, while not automatically triggering legally binding rights or obligations related to a participant entering into resolution, requires participants to be aware of procedures and information needs the central bank may have defined for resolution events (Page 87).
8	**User Interaction with Governance Rules and Policies**	**Governance Structure:** - TARGET2 operates under a three-level governance scheme, with the Governing Council of the ECB at	**Compliance and Participation:** - Users must comply with the general legal structure and principles of participation in

		Level 1, the Eurosystem central banks at Level 2, and the SSP/TIPS platform providing central banks at Level 3. Decisions on the daily running of the single shared platform are taken based on a predefined service level agreement (Pages 21-22).	TARGET2, which includes meeting security requirements and controls. The Eurosystem has developed access criteria that allow users to decide on their form of participation in the system (Pages 45-46).

		Security and Operational Reliability: - The Eurosystem sets a framework specifying guidelines and common requirements that should be met by the users to ensure security and operational reliability. This includes tasks such as framework setting by the Eurosystem and compliance checks (Pages 66-67).	**User Involvement and Communication:** - Users are involved in consultations regarding the content of the annual TARGET2 release. The national central banks contact their respective national user groups to collect proposals for functional changes that would benefit a large number of users (Pages 148).
9	**Organizational Processes and Technical Reliability**	**Technical Infrastructure and Compliance:** - TARGET2's technical structure includes the Single Shared Platform (SSP) with various modules for payment processing and customer-related services. Technical compliance reviews ensure that internal systems used for sending/receiving TARGET2	**Governance and Responsibilities:** - The Eurosystem sets the framework for security and operational reliability, specifying guidelines and requirements for users. TARGET2 operates under a three-level governance structure, with responsibilities

		payments are in line with security policies and standards (Pages 22-23, 164).	distributed across the ECB Governing Council, Eurosystem central banks, and the SSP/TIPS platform (Pages 21-22, 66-67).

		Business Continuity Management: - Critical participants in TARGET2 must have a business continuity strategy in place, with procedures ensuring that critical business transactions can continue during disruptions. The ability to cope with operational disruptions must be tested at least once a year (Page 164).	**Monitoring and Incident Reporting:** - Users are closely monitored by the relevant central bank. In the event of an operational disruption, users must inform the central bank immediately. Incident reporting helps in understanding the root cause and preventing future occurrences (Pages 76).

Table A.4 Operational Implications of Socio Technical Interactions

S.no.	Socio Technical Interaction	Interpretation of Interaction	Why is it a key interaction? (Operational Implications)
1	**Core Platforms and Users**	The interaction between the technical and social aspects happens through a continuous loop of feedback, policy implementation, and technical adjustments. From a technical perspective, the infrastructure must be designed to be robust, secure, and efficient to handle the volume and complexity of transactions conducted by the users. From a social perspective, the users must be well-informed and compliant with the system's rules and procedures. Their feedback is crucial for the system's evolution, ensuring that the technical solutions meet their operational needs. The governance bodies play a pivotal role in this interaction by setting the policies that guide the technical development and by ensuring that the operational roles within the system are effectively executed. This governance ensures that the technical capabilities of TARGET2 align with the social requirements of its users, thereby contributing to the system's overall objectives.|	This is fundamental because the core processing platforms are the heart of TARGET2, facilitating all payment and settlement processes. Users' ability to conduct financial operations smoothly depends on the reliability and efficiency of these platforms. Any disruption here would directly impact the financial operations of the users, which include banks and other financial institutions critical to the functioning of the economy.

2	**Governance Bodies and Operational Roles**	The interaction between the technical and social aspects in this context is characterized by a structured approach to governance and operational management. - From a technical perspective, the governance structure is supported by a detailed technical infrastructure that includes the SSP, PAPSS, and CRSS. This infrastructure must align with the policies and decisions made by the governance bodies. - From a social perspective, the governance bodies, including the Governing Council and the MIB, set the framework and policies within which the	Governance bodies set the strategic direction and policies for TARGET2, while operational roles are responsible for the day-to-day management. This interaction ensures that the system operates within the defined regulatory framework and that the technical infrastructure is managed effectively. It's key because it aligns the system's operations with its strategic goals and regulatory requirements.

		operational roles must function. Operational roles, such as settlement managers and service desks, are responsible for the execution of these policies and the management of daily operations. The governance decisions must align with the technical capabilities and limitations of the system, ensuring that operational roles can effectively execute these decisions. This ensures compliance, efficiency, and the robustness and reliability of TARGET2, which is crucial for maintaining financial stability and confidence in the euro money market.	

3	**Communication Flows between Users and Technical Systems**	The interaction between the technical and social aspects in this context ensures that clear, timely, and secure communication is maintained between users and the technical systems. - From a technical perspective, the infrastructure includes various channels and standards for communication, such as SWIFT and XML messages compliant with ISO 20022. This infrastructure must be reliable and secure to support the necessary communication flows. - From a social perspective, users must be informed and trained to use these communication channels effectively. The national service desks and organizational structures like the Settlement Managers Forum facilitate this interaction by providing support and information. The key interaction here is ensuring that the communication infrastructure is robust and that users are well-informed and capable of using it effectively. This is vital for operational integrity and trust,	Clear and secure communication channels are essential for the integrity and efficiency of financial transactions. This interaction is key because it ensures that critical information is disseminated accurately and promptly, which is vital for maintaining trust and operational continuity in the financial system.

		and it supports TARGET2's operational reliability and responsiveness, which is key to minimizing systemic risk and supporting smooth cross-border transactions.	
4	**Interface and Network Reliability Impact on User Operations**	The interaction between the technical and social aspects in this context ensures that the reliability and security of interfaces and networks directly impact user operations. - From a technical perspective, the infrastructure includes robust monitoring systems, incident reporting mechanisms, and contingency measures to maintain network reliability. - From a social perspective, operational management involves clear communication protocols during incidents, compliance with security requirements, and ensuring that all participants are trained for operational disruptions. The key interaction here is the reliance on the technical reliability of the	Interfaces and networks are the conduits for transaction execution and liquidity management. Their reliability directly affects the users' ability to perform financial operations. This interaction is key as it underpins the operational effectiveness of the entire payment system.

		interfaces and networks, which must be supported by vigilant operational management, risk management, and compliance from the users. This ensures that user operations are effective and efficient, contributing to TARGET2's ability to process payments securely and efficiently, supporting the Eurosystem's monetary policy, and ensuring financial stability.	
5	**Static Data and Settlement Algorithms Alignment with Governance and Operational Procedures**	The interaction between the technical and social aspects in this context ensures that the accuracy and integrity of static data and the effectiveness of settlement algorithms are aligned with governance rules and operational procedures. From a technical perspective, the SSP and settlement algorithms provide the infrastructure and rules for transaction processing, which must be accurately reflected in the static data. From a social perspective, settlement managers and participants must manage this data and apply the algorithms in compliance with the operational procedures and governance rules. This includes risk management and ensuring that staff are trained to handle these	Accurate static data and effective settlement algorithms are crucial for correct transaction processing. This interaction ensures that the settlement process is fair and efficient, aligning with governance and operational procedures. It is key because inaccuracies or inefficiencies here can lead to financial losses and disputes.

		elements correctly. The key interaction here is the alignment of the technical infrastructure and rules with the operational management and governance structures. This ensures fair and efficient transaction processing, contributing to TARGET2's operational efficiency and reliability, supporting its role in minimizing systemic risk, and ensuring the smooth functioning of the euro money market.	
6	**Applications and Operational Procedures**	The interaction between the technical and social aspects in this context ensures that the design and functionality of applications align with operational procedures to effectively support daily operations, incident management, and contingency planning. - From a technical perspective, applications like the ICM, TIPS GUI, and T2S GUI are tools that facilitate transaction management, monitoring, and reporting, which must be technically compliant and part of a broader business continuity framework.	Applications provide the interface through which users interact with TARGET2, and operational procedures dictate how these applications should be used. This interaction is key because it ensures that the system is user-friendly and that the procedures are followed, which is essential for the smooth operation of financial transactions.

		- From a social perspective, operational procedures dictate how these applications are used in various scenarios, with users responsible for monitoring and managing their activities. Training and preparedness are key to ensuring that staff can effectively use these applications during both normal and abnormal situations. The key interaction here is the alignment of application functionality with the operational procedures that guide their use. This ensures TARGET2's resilience and adaptability, which is critical for maintaining continuous operation and trust in the euro money market.	

7	**Settlement Algorithms and Risk Management**	The interaction between the technical and social aspects in this context ensures that settlement algorithms are designed considering risk management principles to minimize the likelihood and impact of transaction failures or delays. From a technical perspective, the SSP and RTGS system provide the infrastructure and rules for immediate and final transaction processing, which is critical for risk management in settlement processes. From a social perspective, governance rules and policies set the framework for risk management, with participants	Settlement algorithms determine how transactions are processed, while risk management ensures that operational and financial risks are mitigated. This interaction is key because it directly affects the system's stability and the financial system's resilience to shocks.

		required to comply with these rules and communicate effectively with central banks, especially in crisis situations. The key interaction here is the design of settlement algorithms with an inherent consideration of risk management principles, supported by governance rules and operational procedures that ensure effective risk management practices are in place. This contributes to TARGET2's role in minimizing systemic risk and ensuring the stability of the financial system.	
8	**User Interaction with Governance Rules and Policies**	The interaction between the technical and social aspects in this context ensures that users understand and adhere to governance rules and policies, ensuring compliance and operational integrity. - From a technical perspective, the governance structure and security frameworks provide the rules and	Users must understand and comply with the governance rules and policies to ensure the integrity of the financial system. This interaction is key because non-compliance can lead to systemic risks and legal issues, potentially compromising the entire system.

		policies that users must follow. This includes the legal framework and the technical requirements for participation and security measures. - From a social perspective, users are expected to engage with the system, providing feedback and complying with the rules. This includes informing the relevant central bank in case of crisis prevention measures or crisis management measures and participating in consultations for system improvements. The key interaction here is the adherence to governance rules and policies by users, which is essential for the overall security, efficiency, and reliability of TARGET2. This compliance directly impacts TARGET2's ability to fulfill its broader economic and monetary objectives.	
9			

	Organizational Processes and Technical Reliability	The interaction between the technical and social aspects ensures that organizational processes are designed and executed in a way that supports and enhances the technical reliability of the system. - From a technical perspective, the infrastructure and compliance mechanisms are in place to ensure that	Organizational processes guide the strategic and operational direction, while technical reliability ensures the system's performance and availability. This interaction is key because it ensures that the system remains operational and reliable, which is essential for maintaining confidence in the financial system.

		the system's performance and availability are maintained. - From a social perspective, the governance structure involves various stakeholders in ensuring the system's operational excellence. Users have clear responsibilities for monitoring, reporting, and testing to maintain technical reliability. The key interaction here is the alignment of organizational processes with the technical reliability of TARGET2. This includes compliance with security requirements, business continuity planning, and incident management, all of which are crucial for maintaining TARGET2's operational excellence and reliability, underpinning its role in the smooth functioning of the euro money market and the broader financial stability.	

Table A.5 Vulnerability in Socio Technical Interactions

S.no.	Socio Technical Interaction	Potential Vulnerabilities	Grounding in the document
1	**Core Platforms and Users**	**Usability Issues:** This vulnerability emerges from the need for the system	**User Satisfaction and Feedback on Platform Functionality:**

		to be user-friendly. If users find the platform difficult to navigate or use, it can lead to inefficiencies and errors in transaction processing. **Technical Disruptions:** Given that TARGET2 is a critical financial infrastructure, any technical disruptions can have significant consequences, including delayed transactions and financial losses. **Transaction Processing Bottlenecks:** In a high-volume transaction environment like TARGET2, bottlenecks can slow down the entire payment system, affecting the broader financial market.	The TARGET2 Information Guide details the process of user involvement in the system's development, particularly through consultations organized for discussing the content of the annual TARGET2 release. This process includes collecting proposals for functional changes from all users and gathering feedback on these changes (page 148). A cost/benefit analysis is carried out for each change, considering feedback from the user community, which reflects the importance of user satisfaction in the system's evolution (page 149). **Reliability Metrics of the Core Platforms (Uptime, Error Rates):** The document discusses measures to ensure the security and operational reliability of TARGET2 users, including tasks and responsibilities for maintaining system reliability (page 66). The technical structure of TARGET2 is described, including the single shared platform (SSP) and various modules, which implies a focus on the reliability of these core platforms (page 22). **Efficiency of Transaction Processing (Speed, Accuracy):** While the document does not explicitly mention transaction processing efficiency in the context of user interaction, the emphasis on system reliability and user feedback indirectly supports the importance of efficient transaction processing. The system's design and continuous improvement through user feedback suggest a focus on maintaining high transaction processing efficiency.
2	**Governance Bodies and Operational Roles**	**Misalignment Between Governance and Technical Capabilities:** If the	The TARGET2 structure is based on a three-level governance scheme involving the Governing Council of the ECB, the Eurosystem central

		governance policies are not in sync with the technical capabilities of TARGET2, it can lead to ineffective system management and operational challenges. **Ineffective Operational Roles:** Operational roles need to effectively implement policies and manage the system. Inefficiencies here can lead to compliance issues and security risks. **Low Compliance Rates:** Non-compliance with governance decisions can undermine the system's integrity and increase the risk of financial losses or fraud.	banks, and the SSP/TIPS platform providing central banks. This structure is crucial for setting and overseeing policies (page 21-22). The roles of central banks in TARGET2, including their governance responsibilities, are outlined, highlighting the importance of alignment between governance and technical capabilities (page 20). The document also discusses the security and operational reliability of TARGET2 users, emphasizing the importance of compliance and effective operational roles (pages 66-67, 81-82).
3		**Miscommunication and Coordination Issues:** In a complex system like	**Clarity and Timeliness of Communication:** The TARGET2 Information System (T2IS) provides information about the operational status of

	Communication Flows between Users and Technical Systems	TARGET2, clear and timely communication is essential. Any miscommunication can lead to misunderstandings, delayed responses, and lack of coordination among users, potentially affecting the entire payment process. **Security Breaches in Communication Channels:** Given the sensitive nature of financial transactions, the security of communication channels is paramount. Any breach can lead to significant data leaks, undermining the confidentiality and integrity of financial transactions. **Underutilization of Communication Systems:** If users are not fully engaged with the communication systems, they might miss out on important updates or fail to leverage the system's full capabilities, leading to reduced operational efficiency.	TARGET2, including normal operations and abnormal situations, ensuring users are well-informed (page 27). **Security of Communication Channels:** The document discusses the technical structure of TARGET2, including security aspects of internet-based access, which is relevant to the security of communication channels (page 22). **User Engagement with Communication Systems:** Information about the connectivity technical requirements and the use of standards like ISO 20022 in communication indicates the system's efforts to facilitate user engagement and effective communication (page 42).
4		**Unstable Interfaces and Networks:** Unstable interfaces and networks can	The guide discusses the importance of monitoring the availability of TARGET2 components and incident reporting, which contributes to the

	Interface and Network Reliability Impact on User Operations	cause transaction failures, leading to financial losses and reputational damage. **High Incident Rates:** High incident rates related to network issues can erode user confidence and lead to decreased system usage. **Negative User Experience:** Negative user experience can deter current and potential system participants, reducing the system's reach and impact.	system's stability and robustness (page 76). Measures to ensure the security and operational reliability of TARGET2 users are outlined, emphasizing tasks and responsibilities related to maintaining network and interface stability (pages 66, 67). The guide details procedures in abnormal situations, including how incidents are documented and resolved, which is relevant to understanding how interface and network issues are managed (pages 106, 107). It also mentions the importance of reporting security problems concerning confidentiality and integrity, highlighting the significance of secure and reliable communication channels (page 77).
5	**Static Data and Settlement Algorithms**	**Inaccurate Static Data:** The accuracy of static data is crucial for correct	**Accuracy and Integrity of Static Data:** The document outlines the procedures for static data collection, emphasizing the importance of

	Alignment with Governance and Operational Procedures	transaction processing. Inaccuracies can lead to disputes, incorrect transaction processing, and potential financial losses. **Inefficient Settlement Algorithms:** The performance of settlement algorithms directly impacts the efficiency and fairness of the settlement process. Poor performance can cause delays and undermine trust in the system. **Misalignment with Governance and Operational Procedures:** It's essential that the algorithms and static data align with governance and operational procedures. Inconsistencies can result in non-compliance and legal challenges.	accurate data entry and validation by central banks (page 55). **Performance Metrics of Settlement Algorithms:** The guide discusses various settlement procedures, such as Procedure 6, which highlights the importance of efficient and reliable settlement algorithms (pages 44-45). **Consistency with Governance and Operational Procedures:** The document details the settlement procedures and mechanisms, such as the guarantee fund mechanism and scheduled time, which align with governance and operational procedures (page 45).
6		**Application Usability and Functionality Issues:** If the applications used in	**User Feedback on Applications:** The document provides information about the technical specifications for the processing of payments and

	Applications and Operational Procedures	TARGET2 are not user-friendly or lack essential functionalities, it can lead to inefficiencies in daily operations, such as transaction handling and monitoring. **Non-Adherence to Operational Procedures:** In a system as critical as TARGET2, strict adherence to operational procedures is essential. Any deviation can increase the risk of operational failures, especially during incidents or high-stress periods. **Ineffective Applications for Contingency Scenarios:** Applications need to be robust enough to handle contingencies. If they are not, it can compromise the system's ability to respond to unexpected events, affecting its overall resilience.	operational documentation, which are relevant to application functionality and usability (page 11). **Adherence to Operational Procedures:** The guide includes details on contingency requirements and operational disruptions, emphasizing the importance of adhering to operational procedures (page 164-165). **Effectiveness of Applications:** Information about the TARGET2 Information System (T2IS) and its role in providing operational status updates indicates the effectiveness of applications in supporting operational procedures (page 27-28).
7	**Settlement Algorithms and Risk Management**	**Inadequate Settlement Algorithm Performance:** If the settlement	**Settlement Algorithms and Risk Management Integration:** The document on page 159 discusses risk management in the context of

		algorithms are not robust or efficient, it can lead to transaction delays, inefficiencies, and potential financial instability. **Ineffective Risk Management:** A lack of effective risk management strategies can result in unmitigated risks materializing, leading to system disruptions and loss of confidence. **Poor Integration of Risk Management in Algorithms:** If risk management principles are not adequately integrated into the settlement algorithms, the system may be vulnerable to emerging threats and challenges.	TARGET2 participants, highlighting the importance of managing risks associated with indirect participation and security requirements. This reflects the integration of risk management in the system's operational framework. **Technical Structure and Risk Management:** On pages 22-23, the technical structure of TARGET2 is outlined, including aspects related to the security of internet-based access. This information is relevant to understanding how risk management is embedded in the technical infrastructure of TARGET2. **Settlement Times and Risk Management:** Information about the settlement times of ancillary systems, as mentioned on pages 11-12, is crucial for understanding how settlement algorithms are designed to manage operational risks effectively.
8		**Lack of Awareness and Unintentional Non-Compliance:** If users are not fully	The TARGET2 Information Guide discusses the legal framework for TARGET2, including the Guideline on TARGET2 (ECB/2012/27), which

	User Interaction with Governance Rules and Policies	aware of the governance rules and policies, they might inadvertently violate them, affecting the system's legal and regulatory standing. **Systemic Risks Due to Low Compliance Levels:** Low compliance with governance rules can introduce systemic risks and vulnerabilities, potentially compromising the entire system. **Ineffective Governance Communication:** Poor communication of governance rules can hinder the system's ability to enforce policies and maintain order, leading to operational inefficiencies.	is the legal basis for the system and with which the Infoguide must be fully compliant (page 10). The document outlines the TARGET2 governance structure, including the roles and responsibilities of the Governing Council of the ECB, the Eurosystem central banks, and the SSP/TIPS platform providing central banks, highlighting the multi-level governance scheme (pages 21-22). It also details the security and operational reliability measures for TARGET2 users, including tasks and responsibilities to ensure compliance with guidelines and common requirements set by the Eurosystem (pages 66-67, 80-81). The guide mentions the requirement for TARGET2 participants to submit self-certification statements to their respective central banks, ensuring compliance with security requirements (page 165).
9		**Misalignment of Organizational Processes with Technical Reliability**	**Alignment of Organizational Processes with Technical Reliability Requirements:** The document discusses the certification testing and

	Organizational Processes and Technical Reliability	**Requirements:** This vulnerability arises when organizational processes are not in sync with the technical needs of the system, potentially leading to increased system downtime and inefficiency. **Inadequate System Performance Metrics:** Without proper metrics to monitor system performance and availability, it's challenging to assess and ensure the system's reliability. **Ineffective Testing and Change Management:** Poor testing and change management practices can leave the system vulnerable to unaddressed issues and outdated practices, affecting its ability to handle transactions reliably.	measures to ensure the security and operational reliability of TARGET2 users, which aligns with the need for organizational processes to support technical reliability (page 65-66, 74). **Metrics on System Performance and Availability:** The guide outlines procedures for different phases of a normal business day and describes procedures to be followed in abnormal events, which are relevant to system performance metrics (page 10). **Effectiveness of Testing and Change Management:** The document details the requirements for testing contingency arrangements and business continuity, as well as change management for yearly releases and emergency changes, which are crucial for assessing the effectiveness of testing and change management (page 10, 79, 80).

Table A.6 Functions (Roles/Services) Delivered by Target2 to Stakeholders

Stakeholders	Roles/Services Facilitated by Target2
European Central Bank (ECB)	**Operational Management:** TARGET2 is crucial for the ECB's real-time gross settlement of transactions, essential for the Eurozone's financial stability and efficiency. **Policy Implementation:** TARGET2 facilitates key aspects of the ECB's monetary policy, such as controlling money supply and managing liquidity across the Eurozone. **Regulatory Oversight:** ECB sets participation criteria for TARGET2, ensuring operational and financial standards for entities interacting with the system.
De Nederlandsche Bank (DNB)	**Facilitating Settlement of Interbank Payments**: TARGET2 plays a vital role in managing the liquidity of the Dutch banking system. **Implementing Monetary Policies:** DNB uses TARGET2 to execute policies set forth by the ECB, impacting economic factors like interest rates and money supply. **Regulatory and Oversight Role:** DNB ensures domestic institutions comply with TARGET2 operational standards, crucial for maintaining the integrity of financial transactions.
Commercial Banks and Financial Institutions	**Settlement of High-Value Transactions:** TARGET2 is indispensable for interbank settlements, handling large volumes of transactions accurately and in real time. **Implementation of Monetary Policies:** TARGET2 allows these banks to adjust their lending and deposit rates in line with the ECB's directives. **Compliance with ECB Criteria:** Ensuring adherence to high standards of technical, operational, and liquidity management.

Payments and Settlement Systems	**Final Settlement Layer:** TARGET2 provides the final settlement for high-value transactions, ensuring finality and irrevocability of payments. **Securities Settlements:** Crucial for delivery versus payment settlements in securities, minimizing transaction risks.
Businesses and Corporations	**Facilitating Financial Operations:** TARGET2 underpins high-value Euro transactions, enabling efficient processing of payments and liquidity management. **Ensuring Transaction Finality and Reducing Settlement Risk:** This boosts confidence in trade and investment activities.
Consumers	**Underpinning Banking Services:** TARGET2 ensures swift and secure settlement of interbank transactions, fundamental to the reliability of banking services. **Influencing Consumer Confidence and Economic Behavior:** Efficient processing of financial transactions bolsters consumer trust in the banking system.

Regulatory and Supervisory Bodies (e.g., ECB, AFM)	**Oversight and Regulation:** Ensuring the safe, efficient, and reliable operation of TARGET2, minimizing systemic risk. **Maintaining Stability and Confidence:** Their oversight is crucial in crisis situations for financial resilience.
International Financial Market Participants	**Settling Euro Transactions:** Access to TARGET2 for settling euro transactions is vital for activities like portfolio investments and foreign exchange transactions. **Efficient Cross-Border Settlement Process:** Promotes the seamless movement of capital and integration of international financial markets.

Financial Market Infrastructures (FMIs)	**Facilitating Settlement of Financial Transactions:** TARGET2 is interconnected with other payment and settlement systems for efficient processing. **Delivery Versus Payment in Securities Settlements:** Ensuring simultaneous exchange of securities and cash.

Table A.7 Drivers of Economic Security with respect to TARGET2 and Economic Security of the Netherlands

Stakeholder	**Derived Drivers of Economic Security**	**Explanation**
European Central Bank (ECB)	1. Ensures Eurozone's financial stability and efficiency 2. Effective execution of monetary policy 3. Maintenance of financial market integrity	1. TARGET2's real-time gross settlement is vital for managing Eurozone-wide financial flows. 2. Facilitating aspects of ECB's monetary policy impacts conditions like inflation and interest rates. 3. Setting participation criteria in TARGET2 helps the ECB ensure adherence to operational and financial standards.

De Nederlandsche Bank (DNB)	1. Stability in the Dutch banking system 2. Alignment of national banking operations with Eurozone policies 3. Compliance and operational integrity in the Dutch financial sector	1. TARGET2's management of liquidity is crucial for the Dutch banking system. 2. DNB uses TARGET2 to align with Eurozone economic strategies. 3. Ensuring compliance with TARGET2 standards is vital for financial stability in the Netherlands.
Commercial Banks and Financial Institutions	1. Secure and efficient interbank settlements 2. Direct impact on lending and economic activity 3. Adherence to operational standards	1. Reliable handling of large transaction volumes stabilizes the banking sector. 2. Adjustments in lending and deposit rates influence credit availability. 3. Compliance ensures financial stability and trust in the banking system.
Payments and Settlement Systems	1. Irrevocability and finality in payments 2. Minimization of transaction risk in securities trading	1. Ensuring finality in transactions reduces systemic risk and enhances security. 2. Secure settlement of securities transactions is crucial for capital market stability.

Businesses and Corporations	1. Efficiency in high-value transactions 2. Confidence in trade and investment	1. Efficient payment processing supports business operations and growth. 2. Reduced settlement risk bolsters business confidence and stimulates economic activity.
Consumers	1. Reliability in consumer banking 2. Consumer confidence in the financial system	1. Secure settlement of interbank transactions ensures reliable banking services. 2. Efficient transaction processing reinforces consumer trust and influences economic behavior.
Regulatory and Supervisory Bodies (e.g., ECB, AFM)	1. Systemic risk minimization 2. Financial resilience in crises	1. Safe and efficient operation of TARGET2 reduces systemic financial risks. 2. Oversight during crisis situations is key for maintaining market stability and public confidence.

International Financial Market Participants	1. Facilitation of international economic activities 2. Seamless capital movement and market integration	1. Efficient settlement of euro transactions is vital for international trade and investment. 2. Smooth cross-border transactions enhance economic interactions at an international level.
Financial Market Infrastructures (FMIs)	1. Efficiency and integration of financial markets 2. Risk reduction in securities transactions	1. Interconnectivity with other systems ensures efficient market processing. 2. Simultaneous exchange mechanisms in securities settlements minimize risks and enhance market confidence.

A.3 Stakeholder Analysis

ECB

The European Central Bank (ECB) occupies a central position in the financial ecosystem of the Netherlands, primarily due to its pivotal role in overseeing and managing the TARGET2 system. As the central bank for the entire Eurozone, the ECB is not just an administrative entity but a key operational player, directly involved in the functioning of TARGET2. This involvement is critical, given that TARGET2 serves as the primary system for large-value and urgent Euro transactions across the Eurozone (Handig, Holzfeind, & Jobst, 2012).

TARGET2, under the ECB's purview, is instrumental in executing real-time gross settlement of transactions. This functionality is not just a technical feature but a cornerstone of the Eurozone's financial stability and efficiency, as analyzed by Bindseil & König (2011). The system's capability to process transactions in real-time ensures immediate and final settlement, a vital aspect in reducing the risk of payment defaults that could ripple through the financial system.

For the ECB, TARGET2 is more than a transaction processor; it is an extension of its monetary policy arm. Through TARGET2, the ECB implements key aspects of its monetary policy, such as controlling money supply and managing liquidity in the banking system. These operations are not confined to a single nation but span the entire Eurozone, influencing financial conditions across member states, including the Netherlands (Gortsos, 2020).

The economic implications of this relationship are profound. TARGET2's efficiency and reliability directly affect the implementation of monetary policies, which in turn influences inflation, interest rates, and overall economic stability in the Netherlands (Moro, 2016). Moreover, the ECB's ability to provide emergency liquidity assistance through TARGET2 during times of financial distress underscores the system's critical role in safeguarding against systemic financial crises.

Furthermore, the ECB's regulatory role over TARGET2 extends to setting participation criteria, ensuring that entities interacting with the system adhere to stringent operational and financial standards. This regulatory oversight is essential not just for the smooth functioning of TARGET2 but also for maintaining the integrity and trustworthiness of the broader financial system (Vukomanović, 2019).

In summary, the ECB's relationship with TARGET2 is symbiotic and multifaceted. It encompasses operational management, policy implementation, and regulatory oversight, all of which have significant economic implications for the Netherlands. The smooth functioning of TARGET2, overseen by the ECB, is pivotal in ensuring the stability and efficiency of the Eurozone's financial infrastructure, directly impacting the financial health and economic stability of the Netherlands (Whittaker, 2016).

DNB

De Nederlandsche Bank (DNB), as the central bank of the Netherlands, holds a crucial position in the Dutch financial landscape, particularly in its relationship with TARGET2. As a member of the Eurosystem, DNB's interaction with TARGET2 is integral to its core functions, including the implementation of monetary policy and the oversight of the domestic financial system (Heijmans, Heuver, & Walraven, 2010).

TARGET2 plays a vital role in DNB's operations, especially in facilitating the settlement of interbank payments in euro. This role is not merely transactional but is deeply connected to the broader monetary and economic stability in the Netherlands (Moro, 2016). Through TARGET2, DNB manages the liquidity of the Dutch banking system, ensuring that banks have sufficient access to funds for their operations (Heijmans, Heuver, & Walraven, 2010). This liquidity management is a key aspect of DNB's responsibility to maintain financial stability in the Netherlands.

Moreover, DNB's use of TARGET2 extends to the implementation of monetary policies set forth by the ECB. The ability to execute these policies effectively, which often involves large-scale transactions across borders, is underpinned by the efficient and reliable functioning of TARGET2 (Mierau & Mink, 2018). As such, TARGET2 serves as a conduit through which DNB exercises its monetary policy decisions, impacting key economic factors like interest rates and money supply within the Dutch economy.

The economic implications of DNB's relationship with TARGET2 are significant. On a practical level, the smooth operation of TARGET2 ensures the seamless flow of high-value transactions, which is essential for the functioning of the banking sector and, by extension, the entire Dutch economy (Handig, Holzfeind, & Jobst, 2012). Any disruption in TARGET2 can potentially lead to liquidity issues and financial instability, highlighting the system's criticality.

Furthermore, DNB's role in overseeing domestic financial institutions that use TARGET2 places it at a pivotal juncture of national and supranational financial governance. This position requires DNB to align its regulatory and oversight practices with broader Eurozone policies while catering to the unique aspects of the Dutch financial system. DNB ensures that domestic institutions comply with the operational standards of TARGET2, which is crucial for maintaining the integrity and efficiency of financial transactions within the Netherlands (Athanassiou, 2020).

In summary, DNB's relationship with TARGET2 is characterized by a dynamic interplay of operational management, policy implementation, and regulatory oversight. This relationship is foundational to the financial stability and economic well-being of the Netherlands. TARGET2's role as a key infrastructure for interbank settlements not only facilitates DNB's core operations but also significantly impacts the broader economic landscape of the country.

Commercial Banks and financial Institutions

Commercial banks and financial institutions in the Netherlands play a pivotal role in the financial ecosystem, significantly influenced by their interaction with TARGET2. These entities, ranging from large banks like ING, Rabobank, and ABN AMRO to smaller financial institutions, are integral in facilitating everyday financial transactions for businesses and consumers.The relationship between these banks and TARGET2 is primarily defined by their reliance on the system for efficient and secure settlement of high-value and urgent Euro transactions. TARGET2, operating as a real-time gross settlement system, ensures that transactions between these institutions are processed swiftly and irrevocably. This functionality is not just a matter of operational convenience; it's a critical component of the financial stability and liquidity management within the banking sector (Heijmans, Heuver, & Walraven, 2010); (Heijmans & Heuver, 2011).

For commercial banks, TARGET2 is indispensable for interbank settlements. The system's ability to handle large volumes of transactions accurately and in real-time is crucial for maintaining liquidity flow between banks. This, in turn, impacts these institutions' capacity to provide continuous financial services to their customers, including loan disbursement, deposit handling, and facilitating international trade transactions (Handig, Holzfeind, & Jobst, 2012).

The economic implications of this relationship are profound. The efficiency and reliability of TARGET2 directly affect the operational stability of these banks. Delays or disruptions within TARGET2 can lead to a cascade of issues, from liquidity crunches to delays in customer transactions. Such scenarios can quickly escalate, potentially affecting the broader banking sector and, consequently, the entire Dutch economy (Heijmans & Wendt, 2020).

Moreover, these financial institutions must comply with the criteria set by the ECB to participate in TARGET2. This compliance ensures that they adhere to high standards of technical, operational, and liquidity management, contributing to the overall integrity and stability of the financial system (Hristov, Hülsewig, & Wollmershäuser, 2018).

TARGET2 also plays a vital role in the implementation of monetary policies transmitted through these banks. As conduits of monetary policy, the smooth functioning of TARGET2 allows these banks to effectively adjust their lending and deposit rates in line with the ECB's directives, influencing economic activity and stability in the Netherlands (Moro, 2016).

In summary, the relationship between commercial banks and financial institutions with TARGET2 is fundamental to their daily operations and overall functionality. This relationship underscores the critical role of TARGET2 in underpinning the stability and efficiency of the financial system in the Netherlands, highlighting its impact not only on these institutions but also on the broader economic landscape.

Payments and Settlement Systems

Payment and Settlement Systems in the Netherlands, encompassing platforms like SEPA for managing Euro transactions and other domestic systems like Equens for retail payments, have a crucial relationship with TARGET2. These systems are integral to the financial infrastructure, facilitating a wide range of transactions, from everyday retail payments to complex securities settlements.

The interplay between these systems and TARGET2 is primarily centered around the settlement process. While payment and settlement systems handle the processing and clearing of transactions, TARGET2 provides the final settlement layer, particularly for high-value transactions. This relationship is critical because it ensures the finality and irrevocability of payments, a cornerstone in reducing systemic risk and ensuring transaction integrity (Repousis, 2016); (Medar & Chirtoc, 2017).

TARGET2's role as a settlement layer has significant implications for the efficiency and reliability of these systems. For instance, securities settlement platforms rely on TARGET2 for delivery versus payment (DvP) settlements, which ensure the simultaneous exchange of securities and cash, minimizing the risk in such transactions (Athanassiou, 2020).

From an economic perspective, the smooth functioning of TARGET2 is vital for the overall efficiency of the financial market infrastructure. It supports the seamless flow of payments across different systems, which in turn affects the liquidity in the financial markets and the ability of businesses and individuals to carry out financial transactions without delays (Parać Vukomanović, 2019); (Heijmans, Heuver, & Walraven, 2010).

Moreover, the ECB's oversight of TARGET2, aimed at ensuring interoperability and smooth transaction flows, is key to maintaining a coherent and integrated European payments landscape. This oversight ensures that different payment and settlement systems can effectively communicate and settle transactions with one another, which is essential for the stability and efficiency of the financial system (Lubik & Rhodes, 2012).

Businesses and Corporations

Businesses and corporations in the Netherlands, encompassing a wide spectrum from large multinationals to small and medium-sized enterprises (SMEs), interact with the TARGET2 system indirectly but crucially through their banking relationships. While these entities do not directly engage with TARGET2, the system's functionality significantly impacts their financial operations.

The primary interaction point for businesses with TARGET2 is through commercial banks, which they utilize for managing finances and conducting a broad range of transactions. TARGET2, serving as the backbone for high-value Euro transactions, underpins these financial activities. It enables banks to process transactions efficiently, ensuring that businesses can reliably move funds, receive payments, and manage their liquidity (Heijmans, Heuver, & Walraven, 2010).

The criticality of TARGET2 for businesses lies in its ability to facilitate seamless and prompt settlement of transactions. This efficiency is particularly vital for companies engaged in international trade, where

timely settlements are crucial. The assurance that payments and receipts are processed without delay or failure is essential for maintaining cash flow and operational stability (Blake, 2018).

Moreover, the role of TARGET2 in ensuring transaction finality and reducing settlement risk has broader economic implications. The reliability of the system in handling transactions directly influences the confidence businesses have in engaging in trade and investment activities. Any disruption in TARGET2 can lead to delays in payments, affecting supply chains, business contracts, and overall market confidence. This could ripple through the economy, affecting economic growth, employment, and investment decisions (Heijmans, Heuver, & Levallois, 2016).

Additionally, the smooth functioning of TARGET2 supports businesses in their international transactions within the Eurozone, thereby promoting economic integration and market expansion. It provides a stable and reliable platform for businesses to expand their operations across borders, contributing to the overall economic vitality of the Netherlands (Fahrholz & Freytag, 2011).

In summary, while businesses and corporations in the Netherlands do not interact with TARGET2 directly, they are significantly impacted by its operational efficiency and reliability. TARGET2's role in facilitating smooth financial transactions is fundamental to the financial health of businesses, influencing their operational capabilities, confidence in the financial system, and contributing to the broader economic landscape of the country.

Consumers

Consumers, encompassing individuals and households in the Netherlands that utilize financial services, have an indirect yet pivotal relationship with TARGET2. While they may not directly engage with or be aware of TARGET2, this system plays a crucial role in facilitating the financial transactions that are part of their daily lives (Dijstelbloem et al., 2017).

For consumers, the primary point of interaction with the financial system is through retail and commercial banks, where they manage personal finances and execute transactions (van der Cruijsen et al., 2022). These range from simple activities like transferring money and paying bills to more complex financial dealings. TARGET2, as a high-value payment system, underpins these banking services by ensuring the swift and secure settlement of transactions between banks (ECB, 2021). This backend role of TARGET2, though invisible to consumers, is fundamental to the reliability and efficiency of the banking services they depend on (Jonker & Kosse, 2013).

The significance of TARGET2 for consumers lies in its ability to process interbank transactions in real-time (Pollock, 2022). This capability ensures that when consumers make a payment or receive funds, the process is seamless, with minimal delay. This efficiency is particularly crucial for transactions that require immediate settlement, such as urgent bill payments or time-sensitive transfers (DNB, 2021).

Economically, the smooth functioning of TARGET2 has broader implications for consumer confidence and economic behavior. The assurance that financial transactions are processed efficiently bolsters consumer trust in the banking system. This trust, in turn, influences their spending patterns, savings decisions, and overall engagement with financial services. In a broader sense, consumer spending and financial activities are significant drivers of economic growth and stability (Masciandaro & Bruno, 2021). Thus, the reliability of TARGET2 in facilitating these activities indirectly supports the economic well-being of the country.

Moreover, in an increasingly digitalized banking environment, where consumers are engaging more with online banking and financial technologies, the role of TARGET2 becomes even more critical (ECB, 2020). It supports the infrastructure that enables modern banking methods, ensuring that even as financial services evolve, the underlying settlement processes remain robust and reliable.

In summary, consumers in the Netherlands, while not directly interacting with TARGET2, are significantly impacted by its operational efficiency (Jonker & Kosse, 2013). TARGET2's role in ensuring

the smooth and reliable settlement of financial transactions underpins the banking services that consumers rely on, directly affecting their financial experience and confidence in the financial system. Through this indirect relationship, TARGET2 plays a key role in the financial health and stability of consumer activities, contributing to the broader economic landscape.

Regulatory and Supervisory Bodies

Regulatory and supervisory bodies, particularly at the EU level such as the European Central Bank (ECB), and national authorities like the Dutch Financial Markets Authority (AFM), hold a fundamental role in the oversight and regulation of the financial system, including critical payment systems like TARGET2. These entities are the sentinels and stewards of financial stability, providing the necessary governance and regulatory frameworks that underpin the operation of systems like TARGET2 (Cales, Chabert, Hichri, & Marchand, 2011).

The ECB, as elucidated in its 2009 report, has a statutory mandate to promote the smooth functioning of payment systems within the Eurosystem, which encompasses TARGET2. This mandate translates into the ECB's active role in setting oversight policies and standards for TARGET2, ensuring that the system operates within a robust legal and governance framework. As the operator of TARGET2, the ECB's responsibilities extend beyond mere oversight; it ensures that all operational, technical, and legal aspects of TARGET2 are aligned with the broader objectives of financial stability and efficiency (Garcia-de-Andoain, Heider, Hoerova, & Manganelli, 2015).

National regulators, like the AFM in the Netherlands, complement this oversight at the domestic level. They monitor and regulate the activities of Dutch banks and financial institutions that access TARGET2, ensuring these entities adhere to the standards and practices set for the system. This dual layer of regulation — both at the European and national levels — is crucial for maintaining a harmonious and integrated financial environment, especially in a system as fundamental as TARGET2 (Whelan, 2014).

The economic implications of this regulatory framework are profound. By ensuring the safe, efficient, and reliable operation of TARGET2, these regulatory bodies help minimize systemic risk, a critical factor in safeguarding the financial system against potential disruptions. Their oversight is not just about operational integrity; it's about maintaining stability and confidence for all stakeholders dependent on TARGET2 — from banks to businesses, consumers, and the broader economy. This stability is particularly crucial in crisis situations, where the robustness of systems like TARGET2 becomes a linchpin for financial resilience (Chmielewski & Sławiński, 2019).

In essence, the relationship between regulatory bodies like the ECB and AFM and TARGET2 is integral to the financial ecosystem. Their role goes beyond governance; they are key actors in ensuring that TARGET2 remains a reliable and stable backbone of the European financial infrastructure, directly impacting the economic stability and security of the Netherlands and the entire Eurozone (Garcia-de-Andoain, Heider, Hoerova, & Manganelli, 2015).

International Financial Market Participants

International financial market participants, including institutions such as investment banks, hedge funds, pension funds, and insurance companies, are key actors in the global financial landscape, particularly in their engagement with cross-border transactions and markets (Masciandaro & Bruno, 2021). While these entities are based outside the Netherlands, their interaction with TARGET2 is crucial in the context of euro-denominated transactions (ECB, 2013).

These international participants, though not directly connected to TARGET2, access the system for settling euro transactions through banks that are direct participants (ECB, 2020). This access is vital for a range of activities essential to their operations, such as making portfolio investments across EU financial markets or engaging in foreign exchange transactions with European banks. As highlighted in an ECB Working Paper (No. 1619, 2013), TARGET2 is instrumental in providing settlement in central

bank money for all credit operations involving international counterparties (ECB, 2013). This capability of TARGET2 to facilitate transactions across borders is not just a feature of the system but a fundamental aspect of its design, enhancing the fluidity and integration of European financial markets (ECB, 2020).

The smooth cross-border settlement process enabled by TARGET2 is key to the efficient flow of capital across Europe (Valiante, 2016). It allows these international financial institutions to execute transactions swiftly and securely, which is essential for maintaining the liquidity and continuity of their operations. This efficiency has broader implications for the integration of international financial markets, as it promotes the seamless movement of capital, contributing to the global interconnectedness of financial activities.

The ECB's oversight in this context is aimed at ensuring that TARGET2 can reliably support the needs of these global financial institutions (ECB, 2021). This oversight is critical in maintaining the integrity and reliability of TARGET2, ensuring it meets the standards required for handling complex, high-value international transactions.

In summary, the relationship between international financial market participants and TARGET2 is a cornerstone of the Eurozone's financial infrastructure (Valiante, 2016). While these participants are not direct users of the system, their reliance on TARGET2 for euro-denominated transactions underscores the system's importance in global finance. The linkages between TARGET2 and international finance are pivotal in ensuring the Eurozone maintains open, efficient, and robust payment systems and capital markets, facilitating the free flow of capital across borders and contributing to the stability and integration of the global financial system (ECB, 2020).

Financial Market Infrastructures

Financial Market Infrastructures (FMIs) are the foundational systems that support and facilitate the functioning of financial markets and institutions. These infrastructures, as outlined by the Bank for International Settlements, encompass a variety of systems including payment systems like TARGET2, securities settlement systems, central counterparties, and trade repositories. Each of these components plays a specific and crucial role in the broader financial ecosystem (Berndsen & Heijmans, 2017).

TARGET2, as a vital part of these FMIs, holds a central position in ensuring the smooth operation of financial transactions across the Eurozone, including the Netherlands. It is a critical infrastructure that facilitates the settlement of interbank payments and is interconnected with other payment and settlement systems. This interconnection allows for the efficient processing of a range of financial transactions, from high-value interbank transfers to securities settlements (Mersch, 2016).

Securities settlement systems and other related platforms often rely on TARGET2 for the critical process of delivery versus payment (DvP). DvP settlements, facilitated by TARGET2, ensure the simultaneous exchange of securities and cash, which is essential for reducing the risk in securities transactions. The reliability of TARGET2 in these settlements is vital for the overall integrity and efficiency of these processes (Berndsen & Heijmans, 2020).

The smooth functioning of TARGET2 is not merely a technical requirement but is integral to the efficient operation of the wider financial market infrastructure (Valiante, 2016) (Krarup, 2019). Financial institutions, both within and outside the Netherlands, depend on TARGET2 for the reliable settlement of transactions. Any inefficiency or disruption in TARGET2 could have immediate and widespread implications, potentially affecting various facets of financial operations.

Oversight and governance by entities such as the ECB are crucial in this context. The ECB closely monitors TARGET2 and other interconnected FMIs to ensure their stability and coordinated

functioning. This oversight is essential for maintaining systemic resilience, as issues with TARGET2 could rapidly translate into broader systemic risks (Heijmans & Wendt, 2020).

TARGET2's robustness and reliability are therefore central to the broader financial stability. Its role goes beyond just being a component of the financial infrastructure; it is a key element of the financial "plumbing" that enables markets and institutions to securely and efficiently transact and transfer funds. The health and stability of TARGET2 are thus pivotal not only for the smooth functioning of individual financial transactions but also for upholding the stability and integrity of the entire financial market infrastructure.

Academia

Academia, which includes universities, research institutions, and individual scholars, plays a crucial role as a stakeholder in the TARGET2 ecosystem. As a center for independent analysis and innovative thinking, academic entities contribute significantly to the development and refinement of TARGET2. For instance, Whelan (2014) discusses the impact of TARGET2 on central banks' balance sheets, arguing that the system is largely innocent of facilitating bailouts or peripheral current account deficits, thus providing a critical perspective on its functioning and efficacy (Whelan, 2014). Furthermore, Fahrholz and Freytag (2012) highlight the significant role of TARGET2 in economic integration and monetary policy within the Eurozone, emphasizing its contribution to real resource misallocation and the challenges in rebalancing claims and liabilities (Fahrholz & Freytag, 2012). Additionally, Moro (2016) points out the importance of TARGET2 in the context of the European crisis, reflecting funding stress in banking systems and the necessity for political integration of EMU countries for effective crisis resolution (Moro, 2016).

Moreover, academic research and publications offer a deeper understanding of TARGET2's role within the Eurozone's monetary framework. The educational role of academia, as described by Handig, Holzfeind, and Jobst (2012), ensures a continuous influx of informed, skilled individuals into the financial sector. This is crucial for shaping the next generation's understanding and approach to systems like TARGET2, thereby influencing its policy context and operational evolution (Handig, Holzfeind, & Jobst, 2012). Through these functions, academia not only shapes the perception and intellectual discourse surrounding TARGET2 but also plays an indirect yet impactful role in its policy and operational development.

A.4 Interview Protocol

Experts are reached out through email, seeking their willingness to participate in the research. The emails are customized to request their subject matter expertise for the validation process. Experts who are willing to participate will then receive the following invite and consent form.

Participant Consent Form

Dear Participant,

You are being invited to participate in a research study titled Exploring the Criticality of TARGET2: A Socio-Technical Analysis of Its Role in the Economic Security of the Netherlands. This study is being done by Anurag Arora from the TU Delft. The purpose of this research study is to understand the criticality of Target2 Payments Settlement System for the Economic Security of the Netherlands, and will take you approximately 60 minutes to complete. The data will be used to validate the results obtained from a prior document analysis. I will be asking you questions about operations and vulnerabilities within Target2 system, and their potential economic implications. As with any online activity, the risk of a breach is always possible. To the best of our ability, your answers in this study will remain confidential. We will minimize any risks by: Participants in the study will have access to their personal information and the right to correct or delete it without providing any reason. Only the master student researcher and supervisor conducting the interviews will have access to personal information during the study, which will be stored on stored on TU Delft's One Drive and the data will

be deleted at the latest 2 years after the end of the project (but may be deleted sooner). The data may be used to as supporting material for future scientific publication and presentations. The data will be stored in a TUD OneDrive and will not be shared with 3rd parties. Non-personal information (anonymised transcripts) may be shared anonymously for scientific publications and presentations. Participants may withdraw from the study at any time without providing a reason. You will receive anonymised transcripts before publication, and you are free to contact us if there are any concerns. Your participation in this study is entirely voluntary and you can withdraw at any time. You are free to omit any questions.

10 Corresponding Researcher: Anurag Arora: a.arora-student.tudelft.nl

PLEASE TICK THE APPROPRIATE BOXES	Yes	No
A: GENERAL AGREEMENT – RESEARCH GOALS, PARTICPANT TASKS AND VOLUNTARY PARTICIPATION		
1. I have read and understood the study information, or it has been read to me. I have been able to ask questions about the study and my questions have been answered to my satisfaction.	☐	☐
2. I consent voluntarily to be a participant in this study and understand that I can refuse to answer questions and I can withdraw from the study at any time, without having to give a reason.	☐	☐
3. I understand that taking part in the study involves: video recorded online interview on Microsoft Teams, as well as the storage of your name and email ID for contact purposes (calendar invites). The recordings will be transcribed as text and the recordings will be destroyed.	☐	☐
4. I understand that the interview will end within 60 mins	☐	☐
B: POTENTIAL RISKS OF PARTICIPATING (INCLUDING DATA PROTECTION)		
5. I understand that taking part in the study also involves collecting specific personally identifiable information (PII) [name and email] and associated personally identifiable research data (PIRD) [job position] with the potential risk of my identity being revealed	☐	☐
6. I understand that the following steps will be taken to minimise the threat of a data breach, and protect my identity in the event of such a breach: Anonymous data collection, (pseudo-) anonymization, secure data storage/limited access, transcription	☐	☐
7. I understand that personal information collected about me that can identify me, such as [name, email, or job positions], will not be shared beyond the study team.	☐	☐
8. I understand that the (identifiable) personal data I provide will be destroyed	☐	☐
C: RESEARCH PUBLICATION, DISSEMINATION AND APPLICATION		
11. I understand that after the research study the de-identified information I provide will be used for: quotes from interviews [anonymized], anonymized transcripts, and indigenous knowledge that contributes to the research on Target2 Payment System.	☐	☐
12. I agree that my responses, views or other input can be quoted anonymously in research outputs	☐	☐
D: (LONGTERM) DATA STORAGE, ACCESS AND REUSE		
14. I give permission for the de-identified [anonymized transcripts] that I provide to be archived in the publicly available TU Delft repository so it can be used for future research and learning.	☐	☐
15. I understand that I will receive anonymized transcripts before publication for review	☐	☐

Target Participants

Prior to the interview, an executive summary of the research results will be shared with the experts. This will help them familiarize themselves with the questions that will follow during the interview. Nevertheless, a brief introduction will still be provided at the beginning of the interview. Since the interview aims to validate the obtained results, the expert will be briefed about these results prior to each question to offer context and background.

Senior Policy Advisor

As a Policy Advisor, this expert plays a direct role in formulating policy priorities and responses related to payment systems oversight and issues affecting economic security. Therefore, their strategic guidance and perspective can validate crucial aspects of our TARGET2 research outcomes that may impact or inform future policy decisions regarding governance, risk management, vulnerability interventions and overall approaches to bolstering the economic security manifested through infrastructure like TARGET2.

Question 1

How well does my conceptual framework capture the critical policy priorities and concerns regarding TARGET2 from DNB's perspective?

Rationale

This question directly tests whether our proposed conceptual framework dimensions align well with important policy issues that DNB actually faces around TARGET2 and managing its role in economic security. If confirmed, it would indicate that the frameworks developed in our research reflect real-world policy priorities and applications from DNB's standpoint, rather than purely theoretical concepts without relevance. It substantiates whether the frameworks can serve as an applicable diagnostic lens guiding future policy formulation because they encompass concerns that already resonate from a frontline policy context.

Validation Objective

Framework-Policy Alignment - Validating alignment of conceptual framework to policy priorities

Question 2

What are the implications of the vulnerabilities I have identified on future policy formulation for bolstering economic security?

Rationale

Here, we are seeking expert perspective on whether the vulnerabilities identified through analysis of TARGET2 do indeed warrant mitigation steps through new or adapted policies aimed at safeguarding economic security. If the assessment suggests those vulnerabilities imply a policy response is necessary in areas like new governance protocols, enhanced risk frameworks, etc., it substantiates that our research accurately identified risky dynamics requiring intervention from a policy standpoint. It verifies that priorities to bolster economic security would need addressing those research-informed vulnerabilities.

Validation Objective

Vulnerability Implications - Assessing implications of identified vulnerabilities requiring policy interventions

Question 3

Which dimensions of my framework have the most relevance for guiding policy decisions related to risk management and governance of payment systems?

Rationale

This question asks the policy expert to directly identify which elements of our conceptual framework offer the most real-world value in shaping future policy directions for governance and risk management of payment systems including TARGET2. Concrete validation that specific dimensions provide applicable handle to determine policy changes affirms the practical relevance of those frameworks in anchoring policy formulations. It crystallizes the actual utility based on an insider policy perspective.

Validation Objective

Operationalizability - Determining framework's ability to inform governance and risk management policy decisions

Question 4

What potential policy recommendations do you foresee stemming from my assessment of TARGET2's role in the Dutch financial ecosystem?

Rationale

Finally, soliciting the policy expert's perspectives on prospective policy responses that could develop based on our extensive analysis of TARGET2 provides direct validation that the research yields tangible courses-of-action to strengthen economic security. If new policies or interventions are envisioned as events stemming from the insights surfaced through our assessment, it offers confirmation of applying research to formulate recommendations. This cements the ability of our analysis approach, frameworks and findings to meaningfully inform policy measures, not just serve as an academic exercise.

Validation Objective

Research Utility - Evaluating potential for research to guide policy recommendations related to economic security

Payment Systems Expert

The payment systems expert has an authoritative view into the actual operations, oversight priorities, and system interdependencies associated with financial market infrastructures like TARGET2. Leveraging their insider perspective, we can substantiate the accuracy and completeness of our TARGET2 system characterization including the functionality mapping, stakeholder analysis and emphasis on particular operational criticalities.

Question 1

How accurately does my stakeholder analysis represent the current ecosystem of entities reliant on TARGET2's operations?

Rationale

This question probes the precision of our stakeholder mapping analysis against the known landscape of stakeholders with dependencies and engagement with the TARGET2 infrastructure. Seeking confirmation that we have accurately depicted the constellation of actors across regulatory, financial, operations and user segments provides validity that our foundational ecosystem characterization is grounded in reality. It cross-verifies if our worldview of TARGET2's positioning within a complex stakeholder web matches with the expert's operational oversight vantage point. Accurately mapping the TARGET2 stakeholder ecosystem is crucial for contextualizing the infrastructural system, appropriately scoping its breadth of influence, and anchoring subsequent analyses of functionality, vulnerabilities and economic impacts stemming from its performance.

Validation Objective

Contextual Accuracy - Validating precision of system characterization and stakeholder ecosystem mapping compared to on-ground oversight perspective

Question 2

To what extent does my summary of TARGET2's functionality and services align with your understanding based on DNB oversight activities?

Rationale

This question asks the payments expert to cross-verify how well our documentation and synthesis of TARGET2's functionalities mirrors DNB's view of the system's capabilities, services and role based on hands-on oversight. Confirmation that our analysis accurately and comprehensively captures the operational essence of the system per DNB's vantage point serves to validate that our characterized system parameters are grounded in operational realities versus theoretical depictions. It also substantiates that our functional profiling serves as a credible baseline for further evaluating systemic vulnerabilities or economic impacts rooted in TARGET2's performance profile since our documentation aligned with actual functionality according to the domain expert oversight perspective.

Validation Objective

Functional Representation - Confirming accuracy and completeness of depicted TARGET2 functionality based on operational reality

Question 3

Are there any mismatches between my depicted critical functions and how they are emphasized or deprioritized from an oversight standpoint?

Rationale

While the previous question probes the accuracy of depicted functionality, this question focuses on revealing potential gaps or misplaced emphasis relative to how DNB priorities particular functionalities or dependencies in managing risks or stability from an oversight standpoint. The Payment Systems expert has insight into where DNB's oversight activities are targeted based on infrastructure performance profiles. Surfacing any mismatches serves to validate that our importance placed on highlighting or analyzing particular functions mirrors frontline oversight priorities. Significant mismatches would indicate a need to re-calibrate our risk or criticality designations for certain functionalities. Alignment confirms our emphasis characterization informs what operational dynamics indeed warrant heavy oversight due to economic security impacts.

Validation Objective

Risk Emphasis - Certifying identified critical functions match areas of heavy oversight emphasis

Question 4

What additional systemic interdependencies beyond my mapping warrant consideration regarding TARGET2 operational criticality?

Rationale

Finally, we probe the payments expert's expertise to reveal any overlooked interdependencies or connections that reinforce TARGET2's systemic importance from an economic security standpoint. Their unique operational oversight view can shed light on under-emphasized risk transmission channels or cascading impacts that may be underemphasized in our analysis. Surfacing these blind spots serves to make our downstream vulnerability and risk assessments more holistic and representative by minimizing the probability of missed or hidden transmission channels through which vulnerabilities propagate. It improves the completeness of capturing chain reactions thereby making our system criticality analysis more balanced regarding where vulnerabilities manifest in economic costs.

Validation Objective

Interdependency Mapping - Completing systemic interconnections that influence economic security impacts

Question 5

Based on your familiarity in overseeing real-time gross settlement (RTGS) systems across financial market infrastructures, how well would my conceptual framework and vulnerability analysis transfer or be adaptable when assessing economic security impacts of RTGS platforms beyond just TARGET2?

Rationale

This question aims to gauge the external validity and wider applicability of our TARGET2-based conceptual framework and analytical approach to evaluating vulnerabilities and economic security impacts. As an oversight expert across multiple types of financial settlements infrastructure, the Payment Systems Expert has a well-informed view into commonalities and differences in risks profiles and critical economic impacts. Their input on the transferability or adaptability of our assessment frameworks to other systems helps validate the generalizability versus the Netherlands/TARGET2 specificity. Feedback highlighting extension potential or constraints would reveal assumptions and contextual dependencies that shape the lens of our analysis frameworks, and allow us to qualify the boundaries regarding expansive application to other RTGS infrastructures. Ultimately, this allows us to clarify the scope conditions related to universally applying or customizing the conceptual framework to inform economic security analysis of payment systems beyond TARGET2.

Validation Objective

External Validity - Evaluating wider applicability of conceptual framework and vulnerability analysis to other payment systems

Financial Economist

The Financial Economist represents an expert peer who can scrutinize the methodological soundness and analytical rigor underpinning the linkages made between the socio-technical attributes of the TARGET2 system to representations of economic security for the Netherlands. Their economic lens helps determine the credibility of assumptions and logical flow in the conceptual frameworks connects system dynamics to stability impacts.

Question 1

How sound is my approach of linking socio-technical dynamics to economic security concepts based on established economic theory?

Rationale

This key question explores whether our approach, which connects technical dynamics and characteristics to aspects of economic security, is consistent with known cause-and-effect theories in economics. Feedback from experts, confirming that our analysis is solid according to well-established theories, will show that our approach is methodologically sound and not based on weak assumptions. It aims to rigorously test our approach against current academic understanding and verify if our assumptions linking system performance to economic results are accurate.

Validation Objective

Theoretical Grounding - Evaluating methodology vis-a-vis established economic theory for linking system dynamics to economic security

Question 2

Have I logically derived measurable proxies (operational indicators) that can effectively capture thresholds related to economic security?

Rationale

This question aims to carefully examine how we have come up with measurable proxies (operational indicators) that represent thresholds related to the ideas of economic stability and security. We seek expert confirmation that the steps we took to derive these indicators are logical and that the chosen metrics are good indicators of these limits. This will give us confidence that the indicators we've set up are meaningful. Essentially, it's a close look at how we decided on these particular indicators.

Validation Objective

Indicator Derivation - Scrutinizing rigor in logical buildup of economic vulnerability indicators

Question 3

How robust are the causal mechanisms I have postulated connecting vulnerabilities to indicators and downstream economic impacts?

Rationale

While the previous questions focus on how well our ideas align with theory and how we derive our indicators, this question aims to test how strong and logical our suggested cause-and-effect relationships are. These relationships connect vulnerabilities, metrics, and outcomes. Expert reviews are important here because they can point out parts of our cause-and-effect chains that might not be statistically strong or might be based on weak assumptions about how risks lead to indicators and then to costs. Their feedback can help us make our predictions more reliable by addressing any weak points or gaps in logic.

Validation Objective

Causal Modeling - Critiquing robustness of mechanisms linking vulnerabilities to indicators to outcomes

Question 4

Are there any gaps in my analytical flow connecting TARGET2's performance to financial stability and systemic risk?

Rationale

Lastly, we want to understand if there are any missing parts or mistakes in how we've linked different aspects of system performance to their effects on stability. If experts point out places where our reasoning is weak, it will prompt us to re-examine and strengthen those parts of our analysis. We might have unclear connections between poor performance and increased risks. By fixing these weak spots, we can make our arguments about how performance is linked to risk more convincing and clearly show how economic costs arise from these issues.

Validation Objective

Analytical Integrity - Identifying gaps weakening inference between system performance to economic stability

Question 5

To what extent does our conceptual framework put forth a theoretically and analytically sound approach for linking TARGET2's dynamics to economic security manifestations?

Rationale

While earlier questions focused on evaluating specific mechanisms within our analysis, this question targets comprehensive scrutiny of our conceptual approach itself. As an expert grounded in economic theory, their feedback can validate whether our overarching framework provides a mathematically and analytically sound foundation for tying system properties to economic outcomes. It probes the reasonability of our frameworks to serve as an instrument for informing system-to-security translations.

Validation Objective

Framework Integrity - Assessing inherent soundness of conceptual framework for linking system dynamics with economic security

Interview Summary

Summary of Interviews

Policy Advisor

Socio-Technical Integration

Expert's insights substantiate the research's depiction of TARGET2 as a socio-technical system incorporating both technical and social components. He outlines the various elements of TARGET2, delineating between “the platform and the direct participants which are the banks” and nods to human roles, validating the categorization of core platforms as technical elements and users as social elements.

Furthermore, his perspective enhances the understanding of TARGET2’s technical configuration. He provides additional architectural specifics around interfaces like TIPS and T2S, communication networks like SWIFTNet and ESMIG that facilitate system connectivity, and applications like CRISP that enable operations. Alongside elaborating on access controls, operational procedures and communication flows intrinsic to system functioning, this augmented technical delineation aligns precisely with the research's identification of these assets as pivotal technical components.

Moreover, Expert underlines the influence of human factors, noting that “human interaction is always the weakest link for whatever project or system we talk about", aligning with the research's emphasis on analyzing social dynamics. Additionally, his commentary expands on the governance architecture, clarifying the Eurosystem’s collective involvement and the ECB’s facilitating role. By covering the oversight processes and procedures that guide operations, he provides a wider aperture into TARGET2's administrative ecosystem.

Together, these perspectives validate TARGET2's socio-technical nature, with the additional specifics further solidifying the research's portrayal. Expert's insights substantiate the technical building blocks as well as social interfaces that critically undergird TARGET2's operation as a socio-technical system.

Operational Implications

Expert explores several operational responsibilities, including settlement processing, liquidity monitoring, and regulatory oversight. He notes how components like collateral management platforms and risk mitigation applications enable these processes.

These socio-technical dynamics directly influence operational effectiveness. For instance, communication protocols connecting participants facilitate efficient dispatch of liquidity status alerts. Meanwhile, well-integrated static data and algorithms uphold transaction accuracy.

However, vulnerabilities like technical glitches or miscommunication can equally compromise operations. Expert surfaces incidents where database access failures temporarily stalled auto-collateralization sweeps. Additionally, he flags past coordination issues around participant notification chains highlighting risks spurred by people-system interactions.

By examining these scenarios stemming from socio-technical dynamics, an enhanced perspective emerges on both the opportunities and threats. Optimized social-technical coordination can unlock operational responsiveness, while vulnerabilities at interaction points may equally destabilize operations. Ultimately, the extent of operational influence holds symmetry - whether positive or negative.

Functions Delivered

Expert explores TARGET2's scope in enabling liquidity management, emphasizing how the system equips banks to handle this process efficiently though not directly owning this functionality itself. As he clarifies, "Liquidity management is not a function of target 2, but the liquidity management function of banks is really helped and supported by Target 2".

Additionally, he notes ancillary functions facilitated, including settlement processing, regulatory oversight, collateralization and policy implementation made possible by TARGET2's socio-technical toolsets spanning interfaces linking players, control mechanisms driving compliance and algorithms upholding transaction integrity.

This wider functional range covers not only inner system operations but their ripple effect on entities like commercial banks and consumers, ensuring reconciliations, liquidity shuffling and broader continuity which Expert acknowledges can be impacted during disruptions, though durations may be contained.

By calling out the comprehensive set of functions, direct and indirect, core and ancillary, Expert underscores TARGET2's reach as a facilitator upholding critical financial workflows, not in isolation but as an deeply embedded component within a wider socio-economic fabric - an insight further strengthened by acknowledging downstream impacts when stability falters even temporarily.

In summary, Expert reinforces TARGET2's functional footprint as an enabling pillar supporting processes key to financial stability and economic security.

Vulnerabilities

In discussing vulnerabilities, Expert validates the identification of communication issues as a repeating problem area arising from complex human coordination needs, noting "the biggest problems were all in the field of communication about informing, not informing everybody".

Additionally, he spotlights risks of technical disruptions in databases and interfaces which can manifest in transaction delays and aborted settlement sweeps, indicating such "disturbances" tend to be rapidly detected given extensive monitoring.

Expert also underscores authorization management as an evolving threat with multivariate implications, necessitating constant upgrading of access controls. He cautions that while mitigation strategies are robust, threats like social engineering continue intensifying, affirming "the human interaction is always the weakest link for whatever project or system we talk about".

In summary, Expert covers a spectrum of vulnerabilities rooted in socio-technical dynamics, emphasizing both human and technical facets which interact and create risks. Importantly, his commentary also sheds light on the probabilities and intensities of these threats through examples like frequent communication breakdowns and rapid detection of technical disruptions. This additional context around both the identification and qualitative evaluation of vulnerabilities stemming from socio-technical interaction gaps provides invaluable practitioner validation of threat predictions. Further analysis can augment these initial assessments with quantified severity and impact interpretations.

The expert states that comprehensive metrics are challenging as TARGET2 "contains 2 big parts" spanning localized databases under decentralized control and collective components across jurisdictions. He notes that for in-country systems, "our operations risk manager has full control with all these metrics" including dashboards. However, for collective elements, visibility is obstructed where he has "never heard that there's a huge problem with it, but obviously that's not a guarantee that nothing has happened."

He further explains that given decentralized setups, "it's difficult for me to have a a Clearview on on how that is maintained" across boundaries. While reassuring base resilience by adding "I have never heard that there's a huge problem with it," he qualifies that in the absence of guarantees of anomaly-less operations, "you have these two this difference between the, the local locally maintained databases and the and the common elements."

By surfacing the inherent constraints around comprehensive assessment stemming from decentralization alongside dependence risks from cross-system reliance, the expert's commentary cautions that in complex environments like TARGET2, relying on quantitative metrics alone remains insufficient from a localized and system-wide perspective. Rather, layered social and technical assessments provide operational rigor as no solitary measure can reflect health definitively.

Impact of Vulnerabilities on Economic Security

Expert discusses both contained and cascading impacts from vulnerabilities, noting immediate reconciliation issues facing banks to broader systemic risks that ripple across trade flows and financial markets. He cautions vulnerabilities typically manifest as operational disruptions though second-order effects can rapidly emerge, stating if problems "occur on a Monday...you can solve it only during the night" then by next day "consumers or or or companies would not have the proper balance or available in the morning."

While reassuring that response protocols focus on swift issue containment, Expert acknowledges downstream processes still endure turbulence, evidenced by bank reconciliation impediments and consumer account uncertainties visible in past incidents based on day of the week. There remain possibilities of exacerbated scenarios where outages overlap leading into closing or opening hours.

Additionally, in describing tail risks, Expert observes that if "[databases] are really destroyed" then "the impact would be bigger" including downstream abilities "to have the proper balance...in the morning when [consumers check] their phone or their or their or their account" - underscoring systemic implications of integrity compromise cascading to users.

In summary, Expert carefully delineates a spectrum of impacts tied to vulnerabilities while underscoring safeguards aim for minimizing consumer and market disturbances through rapid issue resolution before systemic implications manifest.

Financial Economist

Socio-Technical Integration

The expert emphasizes the value of analyzing Target2's socio-technical intricacies by stating "I think it sounds like a very valuable approach that you really go into the details of the different elements and to understand them." This perspective further affirms the research's approach of delving deeper into

the technical components as well as social aspects, which provides a more nuanced understanding compared to traditional economic literature.

Furthermore, the expert notes that most economists do not explore these technical nuances in detail, highlighting a prevalent gap as he says "Most academic researchers, they just yeah mentioned the central bank or the commercial bank and that's it." Bringing in the socio-technical perspective addresses this gap and enhances the comprehension of system functionality.

At the same time, the expert acknowledges that this is one analytical approach, noting "So I I think that kept the, IT sounds like a very valuable approach." This indicates recognition that while a socio-technical perspective offers useful insights, it is not the only lens for analysis.

In summary, the expert strongly validates the value of a socio-technical approach that unravels the complexity of interactions between technical and social components. The expert's insights also reveal a shortcoming of existing literature that often does not bridge this gap. By emphasizing the importance of detail and interconnections, his viewpoint further strengthens the research's perspective and contributions.

Operational Implications of Socio-Technical Interactions

The document analysis discusses critical platform-level operations within TARGET2 system, including real time gross settlement management, liquidity control, transaction monitoring and processing, risk management, and business continuity measures during unexpected disruptions.

However, the expert singles out one operation - settlement - as paramount. He states "Settlement is really at the essence of Target2" highlighting its centrality in executing system operations. The expert underscores settlement as the core operation, emphasizing its critical implications in facilitating transactions.

While introducing some nuance regarding complementary roles in liquidity management, the expert validates the prominence of settlement functionality for TARGET2 itself. His focus spotlights this singular operation among the range identified in the document analysis.

In conclusion, while settlement may interface with ancillary mechanisms for liquidity control, the expert affirms it to be at the heart of TARGET2's operations, rather than elaborating on the other operations highlighted in the document analysis. His perspective centralizes this functionality within the socio-technical configuration of the system.

Functions Delivered by TARGET2 to Stakeholders

The document analysis outlines a range of functions facilitated by TARGET2 for stakeholders within the Dutch financial ecosystem. These encompass:

- High-value transaction settlement, liquidity management etc. for institutions like ECB and DNB
- Secure payment guarantees enabling trade and investments for corporations
- Infrastructure for regulatory oversight bodies to monitor systemic risks

Additionally, specific functions identified include enabling monetary policy transmission and interest rate signaling carried out by the ECB.

Elaborating on monetary policy roles, the expert notes uncertainties around precise mechanisms for interest rate transmission via TARGET2. As he states "I've never fought through how that works via Target 2..." More examination is required here.

Additionally, while the system's settlement functionality may allow monetary policies to work despite imbalances, the expert points to design flaws in the Eurozone structure itself that require alternatives like TARGET2.

Regarding settlement, the expert underscores its foundational role in serving the transaction needs of wider economic entities beyond banks and regulators.

In conclusion, the discussion reveals interdependencies between TARGET2 operations like settlement and the ECB's monetary policy signaling functionality. But gaps in understanding transmission mechanisms indicate more research needed on this function. Additionally, flaws in wider Eurozone systems precipitate corner solutions like TARGET2 itself.

Functions Delivered by TARGET2 to Stakeholders

The expert's insights reveal a nuanced understanding of TARGET2's roles, especially regarding settlement processes and liquidity management. The expert singles out settlement as being the core of TARGET2's functionality, stating "Settlement is really at the essence of Target2...it's fundamental." This further validates the finding from the document analysis that highlighted settlement as a vital operation.

Additionally, while the documents emphasized TARGET2's key function in liquidity management, the expert notes that "There are other ways [than TARGET2] for managing liquidity." This suggests that alternative mechanisms outside of TARGET2 also enable liquidity management. Therefore, the expert introduces more complexity and diversity of roles, beyond just TARGET2, that drive critical operations like liquidity management in the financial ecosystem.

Regarding monetary policy transmission, the expert states "I've never fought through how that works via Target 2..." indicating more examination needed on the mechanisms enabling this functionality. As he further notes, imbalances revealed flaws in the Eurozone structure itself that require bridging solutions like TARGET2.

In conclusion, the expert affirms the vital position of key functions like high-value settlement while painting a more interconnected picture with external systems that facilitate operations like liquidity management. Complex interdependencies are revealed between TARGET2's functions and the ECB's policy signalling capacity.

Vulnerabilities within TARGET2's Socio-Technical Framework

In addressing the economic vulnerabilities and systemic risks of TARGET2, the expert provides critical insights that deepen the understanding of these aspects.

The expert identifies a significant political risk as a primary vulnerability for TARGET2, highlighting the potential impact of a country's decision to exit the Eurozone. "The main risk is...when one country decides to leave the euro...that can lead to really stress in the system and even lead to a collapse," the expert notes. This statement sheds light on the interconnected nature of the Eurozone's financial systems and how political decisions in one member state can have profound implications for the entire system, including TARGET2.

Moreover, the expert discusses the broader implications of such vulnerabilities, stating, "It's not just about the money...it's about the stability of the whole system." This remark underscores the systemic

nature of the risks involved, where the repercussions extend beyond financial losses to potentially jeopardize the stability of the entire financial ecosystem.

These insights from the expert align with the research's findings on the systemic risks associated with TARGET2. They reinforce the notion that the system's vulnerabilities are deeply rooted in the socio-political context, with potential cascading effects across the European financial fabric. The expert's perspective validates the research's emphasis on assessing such risks holistically by evaluating the wider impact on financial stability.

Operational Indicators of Economic Security

The expert recognizes system uptime and error rates as useful operational metrics that provide signals about the system's management and potential economic impact.

Elaborating on economic security, the expert notes that it encompasses multiple facets. He discusses how while traditional definitions focus on production, consumption etc., the research's attention is on foundational infrastructure resilience.

When the research definition is articulated as "resilience of vital systems against vulnerabilities and threats," the expert agrees with its specificity, stating "Yeah, resilience, of course, that's also when you look at the complexity, science and all those insights. That's just a very important concept that's the core of the systems are resilient."

Through the dialogue, there is acknowledgement on both sides about the multi-layered nature of economic security. The discussion reflects alignment on emphasizing resilience of core critical infrastructure systems as an accurate narrow definition relevant to this research context.

In conclusion, by linking vital system resilience to economic security, the operational health indicators take on more profound meaning - signifying not just the system's stability but that of larger economic structures that depend on this critical backbone.

Impact of Vulnerabilities on Economic Security

The expert outlines the severity of risks from potential vulnerabilities in TARGET2, emphasizing system-wide impacts beyond isolated financial losses. He notes that exit of a Eurozone member country, as a political contingency, could trigger collapse of the common currency itself. This existential threat underscores risks that can cascade across the interconnected financial landscape, leading to widespread instability.

Additionally, the expert highlights that persistent operational issues could accelerate migration to alternate systems like cryptocurrencies. Such transitions, spurred by eroding trust, could undermine the currency structure further. This perspective reveals individual decisions can have macro impacts, compromising the position of formal infrastructures like TARGET2 through socio-technical shifts towards decentralized platforms.

In essence, the vulnerabilities illuminated in the discussion can destabilize the foundation of existing financial architecture. The expert emphasizes that while seemingly isolated occurrences, these risks carry the capacity to transform economic structures rapidly. Safeguarding resilience, therefore, involves monitoring early warning signs and adapting with agility to manage such complex shifts stemming from systems failure.

Payment Systems Expert

Validating the Socio-Technical Perspective

The expert affirms that "looking at TARGET services as socio-technical systems is a good way to look at any business." This directly validates the suitability of the research's socio-technical lens for assessing a complex system like TARGET2. However, they caution that it "may not be the only way", underscoring the need for conceptual openness and avoiding theoretical silos when evaluating intricate ecosystems. This advice reinforces the analytical imperative of multifaceted appraisals harnessing complementary intellectual frameworks.

Additionally, the expert crystallizes TARGET2's essence, stating it "is of course a technical system. But the most important part...is that is has a purpose" - facilitating secure bank transactions. This viewpoint encapsulates the socio-technical philosophy which recognizes that while technical infrastructure is operationally essential, systems are socially actualized towards fulfilling functional purposes within organizational contexts.

The expert further compares TARGET2's interdependent elements to synchronized biological systems, noting "you need all the organs you have". This organic analogy is uniquely apt from a socio-technical perspective emphasizing integrated technical-social harmony. It alludes to risks emerging from asymmetries where an isolated enhancement or deficiency within a social or technical dimension cascades towards systemic performance deficiencies. Such failures may transpire despite other elements operating at peak efficiency, much like organ impairment triggering multi-causal mortality despite an otherwise physiologically sound patient. This systems-based metaphor offers an adjacent evaluative approach harnessing principles applicable across biological, technological and social collectives.

In summary, the expert espouses perspective congruent with socio-technical precepts, while prudently advising against intellectual monocultures given the multidimensional complexity of systems like TARGET2. Their guidance to recognize purpose-driven social actualization amidst operational intricacy offers an analytical anchor for applying socio-technical ideas across payment infrastructures, and potentially at a theoretical scale, across interdependent networks spanning technology, business and society.

Assessing Operational Dynamics

The expert's insights add pragmatism to balance the document analysis' abstraction. Their explanation that "day-to-day is the system is fully automatic...if there's incidents then there is manual interventions" substantiates the coordinated oversight model of automated efficiency balanced by active human interventions when necessitated. This encapsulates the operational interplay of technical and social elements.

Additionally, envisioning TARGET2 as "a business and we have clients and the clients are the commercial banks" provides an adjacent frame for assessment beyond technical metrics towards service orientation focused on fulfilling stakeholder needs. This business model thinking introduces organizational and commercial principles to optimize value delivery by alignively addressing social interests and technical capabilities.

Furthermore, the expert outlines that "there is a whole cascade of testing phases which is usually manual work". Such insights substantiate conceptual identification of situating technical upgrades within concomitant social elements like user preparedness and policy guidance to enable smooth transition management.

In summary, the expert adds operational grounding through quotes like "day-to-day fully automatic" and "manual interventions when incidents" which validate coordinated systemic efficiency, while qualitative guidance towards a customer-centric business mindset provides an adjacent analytical vector harnessing entrepreneurial thought.

Functions Delivered by TARGET2 to Stakeholders

The interview distills TARGET2's purpose as interbank funds transfers, with the expert explaining "TARGET2, in effect, only does one function...transferring money funds from one account to the other." This divergence from the document analysis' multi-capability taxonomy warrants reconciliation regarding the system's functionalities.

An insightful inference emerges as the expert elucidates "you need all the organs you have" when discussing ancillary operations. TARGET2 manifests an array of capabilities synergizing specifically towards fulfilling its solitary core function of secure bank transactions rather than being segregable discrete functions.

In fact, the expert uses the metaphor of "a whole Christmas tree of correspondent banking relations" to describe the complex, opaque funds transfer arrangements between banks in TARGET2's absence rather than implying impossibility without it. This analogy implies the system's differentiated value lies in streamlining and systematizing interbank transfers through integrated technological and oversight capabilities tailored for this purpose.

In summary, while the document analysis offers a modular functional decomposition, the interview steers analytical thinking towards visualizing TARGET2 as an institutional consolidation of transaction-centric capabilities allowing componentization but not detachment from the core funds transfer purpose. This harmonization of technical and social capabilities uniquely addressing this need is what distinguishes TARGET2's role in the financial ecosystem.

Vulnerabilities within TARGET2's Socio-Technical Framework

A nuanced assessment of vulnerabilities emerges from the discussion, as the expert acknowledges both likelihood and impact levels across various identified threats. Statements like "Technical disruptions are quite likely. Usually impact is usually low...but it can be high as well" underscore a calibrated view admitting infrastructural exposure while highlighting mitigating protocols if activated. This viewpoint aligns with the research premise regarding assessing multifaceted risks stemming from socio-technical asymmetries.

Additionally, the exposure specificity around crisis situations leading to "miscommunication and misalignment" offers an analytical basis to trace system perturbations during exceptions directly back to coordination deficiencies between interdependent components. Such clarity helps evolve theoretical arguments that financial stability investigations must scrutinize both isolated and interactional vulnerabilities, particularly human-technical disconnects being probable failure points.

Furthermore, the vulnerability acknowledgment is weighed against highlighting resilience. The expert notes "very unlikely" security breaches due to robust protection, signaling analytical priority towards handling exposure likelihood through preemptive threat modeling beyond just impact critiquing. This guidance reinforces balanced analytical thinking that avoids viewing vulnerabilities predominantly through isolated impact severity.

In summary, the calibrated assessment of vulnerabilities admits infrastructural risks while emphasizing resilience capabilities, guiding socio-technical analysis towards multidimensional

evaluations of likelihood-impact combinations to enable preventive anticipations along with reactive impact minimization.

Operational Indicators of Economic Security

The expert strongly endorses system reliability metrics like uptime and recovery times as key indicators, noting “that may be problematic for banks” if downtime is prolonged, affecting reporting needs. This directionally aligns with the identified indicators in the document analysis centered around settlement efficiency. However, an analytically meaningful divergence is the underemphasis of policy alignment indicators as prominently featured in the documents.

Inferences could be drawn that technology-first perspectives tend to prioritize reliability-centric indicators over externality-focused measures like regulatory conformance. This analytically informs debates regarding myopic assessments of critical infrastructure isolated from adjoining ecosystem impacts, often overlooked till disproportionate failures materialize. Experts immersed within infrastructure management may require conscious contextualization of their technology-focused monitoring Against indicators tracking holistic well-being spanning interconnected human and technical variances.

The discussions also showcase opportunities for complementary indicator development monitoring both intrinsic consistency like uptime as well as extrinsic alignments to user and governance requirements. Analytically integrating reliability indices with robustness measures tracking socio-technical synergies could enrich economic security frameworks for financial systems, avoiding lopsided approaches tilted purely towards either operational or policy perspectives.

In summary, while the focused direction on reliability indicators is pragmatically reasonable, analytical reasoning reveals possibilities to consciously couple technology-centric monitoring with socio-technical health tracking to enable holistic assessment of financial critical infrastructure stability beyond isolated metrics.

Impact of Vulnerabilities on Economic Security

The interview unravels the depth of economic debilitation risks from settlement disruptions, as the expert notes banks “may get into trouble” necessitating “central bank support” during TARGET2 downtime. This underscores systemic stability threats by clarifying individual bank wellbeing relied on the infrastructure's integrity.

Elaborating how settlement inoperability challenges treasury management and balance reporting draws direct links between technical deficiencies manifesting into enterprise-level operational paralysis. The emphasis on overnight batch processing impact, where "data is being extracted, stored in data warehouses...used for billing, accounting...balance sheet reporting..regulatory needs” analytically ties system outages to organizational outcomes spanning financial, managerial and audit processes.

Additionally, highlighting the loss of settlement finality eroding liquidity transparency points to market structural degradations through magnification of Herstatt risks, transaction counterparty exposures and settlement delivery uncertainties that banks currently avoid by relying on TARGET2's purpose-built resilience. Together, these risks could necessitate thedescribed “crisis management” response across multiple levels to prevent cascading economic meltdowns.

In summary, the expert repeatedly traces arteries connecting TARGET2’s operational heart to the financial system’s economic health. This pathological perspective informs socio-technical analytics to

anticipate points of failure transmission from infrastructure vulnerabilities through enterprise risk accumulation towards market collapse to appropriately safeguard economic security through preemptive resilience.

10