Customer Acceptance of a Revenue Management Platform with Multi-Party Computation: Application of Multi-Party Computation to Revenue Management in the Semiconductor Industry

Master thesis submitted to Delft University of Technology

in partial fulfilment of the requirements for the degree of

MASTER OF SCIENCE

in **Management of Technology**

Faculty of Technology, Policy and Management

by

Vidyottama Faujdar

Student number: 4745272

To be defended in public on August 16th, 2019

Graduation committee

Chairperson	: Dr.ir. Mark de Reuver
First Supervisor	: Tobias Fiebig
Second Supervisor	: Dr. M.E. Martijn Warnier
External Supervisor	: Hans Ehm, Infineon Technologies AG

This page is intentionally left blank

Acknowledgements

Executing this research and writing this thesis has been an exhilarating ride. While research in a novel field is a challenge in itself, achieving this success despite the challenges of distance and time has been all the more gratifying. I would like to thank everyone who made this journey one worth cherishing.

To begin with, I would like to thank my Chair, Dr. Mark de Reuver and first supervisor, Tobias Fiebig for challenging me and giving me direction when I needed it. Thank you for sharing your expert knowledge and for your constant support despite all the hurdles. To my second supervisor, Dr. Martijn Warnier, for providing critical feedback to enhance the quality of my thesis.

I would also like to thank Infineon Technologies AG and my company supervisor, Hans Ehm for giving me this wonderful opportunity to conduct this research while enjoying my time in Munich. To my colleagues and now close friends at Infineon, thank you for encouraging me and being all ears when I wanted to discuss my ideas. Furthermore, I appreciate everyone who dedicated their valuable time for participating in my interview sessions.

Lastly, I could not have achieved this without the unconditional love and support from my family. Mom, Dad and my Sister - the amount you believe in me only encourages me to be the best version of myself. To my friends all across the world, cheers for being a part of this journey with me.

As I write this, I cannot help but think of how fast the last two years went by. TU Delft has given me countless opportunities to grow academically, professionally and personally, allowing me to spend the enriching two years across Delft, Aachen and Munich. I take with me friendships and fond memories to last a lifetime, while l look forward to new beginnings.

Executive Summary

Research Problem

In today's competitive and fast-paced nature of conducting business in the semiconductor industry, the discipline of revenue management (RM) is often mentioned. Through a dynamic pricing capability, RM enables firms to maximize profits by capitalizing on missed revenues. Moreover, RM enables customers to receive products on short notice, by allowing them to place orders with a(n) (earlier) delivery wish date, wish price and volume. Since the semiconductor industry is characterized by volatile market demand, long production times and high capital investment (Ehm & Ponsignon, 2012), the semiconductor industry is a model representation of the manufacturing industry. Despite the benefits of RM, the manufacturing industry has not yet witnessed a widely-adopted revenue management system.

In order to apply revenue management in the manufacturing industry, it is primarily important to understand that the data involved from the parties participating in the revenue management process is confidential. For manufacturers, the confidential data includes the daily unallocated available-to-promise data, which is available to commit to customers for orders on short notice. On the other hand, for customers, the maximum price that they are willing to pay for such products with a shorter delivery time is confidential. Hence, due to the confidentiality involved, as well as the need for enabling a more equal collaboration model between buyers and sellers, a secure technology that involves inputs from multiple parties is required in order to facilitate the implementation of revenue management in the manufacturing industry.

Multi-party computation is a promising cryptography technology which has been theoretically studied by researchers but has not yet been practically applied. This technology is a value-added tool in the use case of revenue management because it deals with multiple parties' confidential data and performs a computation with them securely. The outcome of the algorithm presents a revised price (based on the desired price adder range provided by the manufacturer, as well as the price wishes of the customer), a volume and a delivery date. This will allow manufacturers to secure their unallocated available-to-promise data, and customers to share the confidential maximum price they are willing to pay to receive products earlier. Multi-party computation has been proposed to be applied to revenue management by the EU H2020 SafeDEED project. We further build on this concept (SafeDEED, 2018).

As a consequence of multi-party computation being an up-and-coming technology, as well as revenue management being new to the business-to-business field, it is challenging to imagine what a possible implementation of their integration is. Furthermore, it is equally challenging and important at the same time to understand how this can be communicated to the customers as well as how they perceive the integration of these two paradigms. After studying the literature and the context of the case, as well as identifying the knowledge gap, we develop the following research question:

How can multi-party computation be applied to and visualized with revenue management as a platform interface in order to enhance users' trust in the system and supplier, as well as enhance perceptions of security, perceived usefulness, perceived ease of use and intention to use?

Through this research, we design mock-up interfaces with various visual implementations of revenue management and multi-party computation. Then, as a result of evaluating the artefacts, we propose a potential visual implementation of revenue management and multi-party computation as a platform interface for the manufacturing industry.

Background

We conduct this research with Delft University of Technology, in cooperation with Infineon Technologies AG, while also contributing to the research agenda of SafeDEED (SafeDEED, 2018). Infineon provides the use case for applying multi-party computation to its strategy for introducing revenue management as a platform technology to the semiconductor industry. Furthermore, this research is the first that proposes a potential visual integration of revenue management and multi-party computation, which is currently a challenge to communicate to customers.

Contribution

So far, the application of multi-party computation has not been studied and research is even further away from visualizing it and understanding how to communicate it. Our research proposes a potential platform visual implementation of revenue management using multi-party computation for the manufacturing industry. We apply multi-party computation to the use case of RM by defining its functionality in RM, as well as propose a potential visual integration of RM and multi-party computation. It has so far been a challenge to visualize and communicate cryptography technologies to novice users. Moreover, timely efforts not put into this, lead to failures of cryptographic implementations (Smith, 2003). Security and usability go together, and it is crucial to take both of them into account while designing and evaluating a secure system. We contribute to the field of human-computer interaction and security (HCISec) where we establish how to communicate the implementation of multi-party computation to new users. Through this, we identify the effects on usability factors such as perceived usefulness, perceived ease of use, trust, security and intention to use. We identify the relevant factors that influence customer acceptance of such an interface, based on communicating the introduction of RM and multi-party computation through visual aids, to customers.

This research is also an important milestone for the SafeDEED project, where one of the research objectives includes establishing the application of multi-party computation to the use case of revenue management.

Research Method

We adopt a design science research approach for our study, including the design and evaluation of potential platform mock-ups, which integrate revenue management and multi-party computation technology. We design four mock-ups, where one is identical to the current platform, and three are involved in the evaluation process. Our mock-ups' design is based on a literature review on revenue management, multi-party computation, auctions for visualizing revenue management, human-computer interaction and security, in addition to a study about the context of the case. The context study involves identifying the potential for revenue management and multi-party computation, the current processes and examining the current buying platform. Together, this knowledge leads us to establish the design requirements.

Then, we evaluate the mock-ups based on usability parameters that influence customer acceptance of new technology. These parameters as identified from the state of the art are trust, security, perceived usefulness, perceived ease of use and the intention to use. While these parameters have been researched through technology acceptance models in the literature, however, despite proving their importance in influencing new platform acceptance, these parameters have been studied independently. We evaluate our platform mock-ups using these aforementioned parameters altogether.

Our evaluation method consists of an experiment session, followed by an interview. The sample size is nine participants, which is considered sufficient for a usability study according to literature (Hwang & Salvendy, 2010). The sample includes people from the Supply Chain and Innovation Department of Infineon. This is because access to real customers is not granted at this initial stage, as it can harm the crucial manufacturer-customer relationship. Among the nine participants, five people from the lead time-based pricing team are requested to join due to their knowledge of real customers with respect to the introduction of revenue management. Moreover, the remaining four participants are selected by a first-come-first-serve basis, based on who replied to the mass email that is sent out for requesting participation.

Three people take part in the experiment and the interview at the same time. This is due to the resources involved, as well as to mimic the situation in reality, where customers will discuss the new platform with each other. According to the participants' availability, as well as the presence and individual resources of only one researcher to conduct the experiment and interview, we conduct the session in groups of three participants. Additionally, since we involve students for our study, it is more beneficial for the research to interview the participants together in small groups, where they can debate and discuss each other's viewpoints. This led to valuable insights which would not have been possible to obtain, had the students been interviewed one-on-one. The interview protocol is developed in order to be able to identify factors that are perceived to be vital for customer acceptance of the platform as well as for participants to express why they like or dislike a certain mock-up.

Findings and Conclusions

Our results indicate that customers value trust, security and the extent of control they have while evaluating the new platform that integrates revenue management and multi-party computation. Based on our mock-up designs, people find the *use of explicit text* (e.g., the mock-up which presents a disclaimer, explaining the new technology and the process) to prompt positive feelings pertaining to the security in the platform. Similarly, the *use of visual indicators* that give the impression of *transparency* of the process, are highly valued, for inducing trust in the platform. Regarding the extent of control in the platform, participants find that having basic *information about competing customers* makes them feel like they are in control of the process.

Following these findings, the mock-up that includes an explicit text explaining the process and technology was scored positively for security. Next, the mock-up that consists of a grid which automatically fills in the customers' inputs, is perceived to be transparent and fair, which leads to a high score with regards to trust in this platform mock-up. Lastly, two mock-ups perform well with respect to the perceived extent of control. Both these mock-ups have in common the

concept of showing the customers that a number of competitors are also interested in the product. This makes customers feel more informed about the setting, thus, they are better able to make choices about their own inputs.

Recommendations for further action and research

This study was a first to visualize and communicate the cryptographic technology of multi-party computation to users. Through this study, we contribute to the literature on human-computer interaction and security (HCISec) by incorporating usability and security together during the development and evaluation of the interfaces that integrate revenue management and multi-party computation. In line with past research on HCISec (Gunson, Marshall, Morton & Jack, 2011), we find that there is a trade-off required between communicating security to users and enhancing usability.

After completing the evaluation and analysis, we recommend a potential platform visual integration of revenue management and multi-party computation, including the features that we find to positively influence customer acceptance throughout all the mock-ups, as well as eliminating features that hamper it. We recommend practitioners to weigh the importance of trust, security and the perceived extent of control as well as to not neglect either of them while designing the future platform. We also suggest developing the lead time-based pricing algorithm before evaluating the acceptance of such a platform. Lastly, this study should be performed with real customers before introducing this radical change to the semiconductor industry.

In addition to this, we recommend future research directions. Quantitative research can be undertaken to statistically validate the extent that trust, security and control influence customer acceptance. Having this research establish the influence of trust, security and control after evaluating the artefacts, can help take research to the next stage where the effects of these factors can be measured. Further research can also be conducted to understand the inter-relationship between these three factors (trust, security and control). Lastly, other predictors that can also explain customer acceptance of such a platform can be studied.

Lists of Figures

Fig 1: Opportunity for revenue management in the semiconductor industry 15
Fig 2: Practical contribution of the research (evaluating customer acceptance for the introduction of the lead time-based pricing platform) 20
Fig 3: Design Science Research Cycles (adapted from Hevner, 2007) 22
Fig 4: Potential for lead time-based pricing and RM 26
Fig 5: Potential for lead time-based pricing and RM based on product data 26
Fig 6: Landing page of current IFX ordering platform 28
Fig 7: Products search results 29
Fig 8: Reduced ordering quantity 29
Fig 9: Increased ordering quantity 30
Fig 10: Similarities and differences in RM attributes in the manufacturing and service industries (adapted from Zatta, 2016) 32
Fig 11: Computation with a trusted third party 33
Fig 12: Classification of auctions based on bidding sides, bid composition, the role of participants and security 35
Fig 13: Research model (adapted from Gumussoy & Calisir, 2009) 43
Fig 14: Research model (adapted from Gefen et al., 2003) 44
Fig 15: Research model (adapted from Lai, 2016) 44
Fig 16: Research Model 46
Fig 17: The functionality, inputs, outputs and parties involved in MPC with RM 49
Fig 18: RM setting with and without using MPC 50
Fig 19: Current buying platform 54
Fig 20: Potential platform mockup 1 - Disclaimer 55
Fig 21: Disclaimer text and padlock symbol 55
Fig 22: Potential platform mockup 2 - Blurry 56
Fig 23: Potential platform mockup 3 - Clear 57
Fig 24: Stages of thematic analysis 65
Fig 25: Development of themes 65
Fig 26: Example of codes, categories and theme 65
Fig 27: Proposed platform design for RM with MPC to facilitate trust, security and control .. 89
Fig 28: Dynamic price adder set by the manufacturer 91
Fig 29: Concept of reserved ATP 91
Fig_of_Appendix 1: Simplified order management process 107
Fig_of_Appendix 2: From order entry until order promised (Manual activity from Sales) ... 107
Fig_of_Appendix 3: Customer types 108
Fig_of_Appendix 4: Quote verification and generation 109
Fig_of_Appendix 5: Agenda for the session 110
Fig_of_Appendix 6: Introduction of goals and participant role 110
Fig_of_Appendix 7: Document provided to the participants to read and understand the setting 111
Fig_of_Appendix 8: Recap of the document read by the participants 112
Fig_of_Appendix 9: Video of interface 1 112
Fig_of_Appendix 10: An input guide for the participants for the revenue management interfaces 112

Fig_of_Appendix 11: Instructions to use the mock-ups and change the display resolution to fit the mock-ups best 113
Fig_of_Appendix 12: Artefacts screen 1 114
Fig_of_Appendix 13: Artefacts screen 2 114
Fig_of_Appendix 14: Artefacts screen 3 115
Fig_of_Appendix 15: Artefacts screen 4 115
Fig_of_Appendix 16: Artefacts screen 5 116
Fig_of_Appendix 17: Artefacts screen 6 116
Fig_of_Appendix 18: Artefacts screen 7 117
Fig_of_Appendix 19: Artefacts screen 8 117

Lists of Tables

Table 1: Design principles that positively influence user feelings 40
Table 2: Requirements to inform the design of the artefacts..... 51
Table 3: List of interviewees..... 64
Table 4: The themes, categories and respective codes, with the number of times each code was mentioned by session and participants, along with a breakdown of the number of times each mock-up was positively and negatively chosen 70
Table 5: Comparison of mock-ups with respect to trust..... 84
Table 6: Comparison of mock-ups with respect to security..... 84
Table 7: Comparison of mock-ups with respect to control 85
Table 8: Positive and negative attributes that influence trust, security and control 86

List of Abbreviations

Abbreviation	Meaning
ATP	Available To Promise
B2B	Business To Business
BPM	Business Process Management
DSR	Design Science Research
HICSec	Human-Computer Interaction and Security
IFX	Infineon Technologies AG
LTBP	Lead Time-Based Pricing
MPC	Multi-Party Computation
OLT	Order Lead Time
RM	Revenue Management
Safe-DEED	Safe-Data Enabled Economic Development
TAM	Technology Acceptance Model
TTP	Trusted Third Party

Contents

Acknowledgements 3
Executive Summary 4
Research Problem 4
Background 5
Contribution 5
Research Method 5
Findings and Conclusions 6
Recommendations for further action and research 7
Lists of Figures 8
Lists of Tables 10
1. Introduction 14
1.1 Revenue Management in the Semiconductor Industry 14
1.2 Multi-Party Computation – a tool for implementing revenue management 15
1.3 Safe-Data Enabled Economic Development (SafeDEED) 15
1.4 Knowledge Gap 16
1.5 Problem Statement 17
1.6 Research Objective 18
1.7 Research Question 18
1.8 Approach 18
1.9 Research Contribution 19
1.10 Structure 21
2. Design Science Research 22
3. Use Case (Relevance Cycle) 25
3.1 Potential for LTBP and RM 26
3.2 Volume-based Pricing versus Lead time-Based Pricing 27
3.3 Current Processes 28
3.4 Current Buying Platform 28
4. Literature Review (Rigour Cycle) 31
4.1 Revenue Management 31
4.2 Secure Multi-Party Computation (MPC) 33
4.3 Auctions 35
4.4 Human-Computer Interaction and Security (HCISec) 38
4.5 Platforms and Consumer Acceptance 41

4.6 Conclusions 46
5. Artefact Design (Design Cycle) 48
5.1 Developing the functionality of MPC in the use case 49
5.2 Design Requirements 50
5.3 Description of the artefacts 52
6. Evaluation of the artefacts 58
6.1 Experimental approach 58
6.2 Interviews 61
6.3 Data Analysis 64
6.4 Assumptions 66
6.5 Advantages and limitations 67
7. Results 69
7.1 Perceived usefulness, perceived ease of use and intention to use 71
7.2 Trust (consideration of customer's best interests) 71
7.3 Security 76
7.4 Extent of control 81
8. Discussion 86
9. Limitations 92
10. Conclusion and Further Research 94
10.1 Conclusion 94
10.2 Further Research 95
11. Reflection 97
11.1 Contribution to literature 97
11.2 Recommendations to Practice 99
Bibliography 101
Appendix 107
Appendix 1. Current Processes at Infineon 107
Appendix 2. The preparatory material for the experiment and interview 110
Appendix 3: Artefact screens common to the three mock-ups 114
Appendix 4. Word cloud of the interviews (keywords) 118

1. Introduction

In this chapter, we briefly introduce the concepts and context involved in this work. This includes a description of revenue management in the semiconductor industry, the cryptography technology called multi-party computation and an introduction to the EU-funded project that this thesis also contributes towards. We then explain the knowledge gap, the problem statement and the research questions of this study. We conclude after discussing the research approach, the research contribution and the structure of this thesis.

1.1 Revenue Management in the Semiconductor Industry

The field of revenue management (RM) is widely applied in the service industry. It was first introduced in passenger airlines in the late 1970s when companies were permitted to configure the ticket prices by themselves, according to customer demand. Proving its potential, it expanded to hotels, railways, car rentals etc. However, state of the art shows that RM has not yet been successful in the semiconductor industry (Zatta, 2016). This industry faces long production cycles and limited product lifecycles. Thus, it is complex and necessary to consistently match supply with demand while avoiding the risk of obsolete semiconductors.

RM takes an analytical approach to management science, using dynamic pricing in complex environments. As it allows for relocating capacity, RM improves the reliability and speed of deliveries, allowing firms to utilize profit-making opportunities through any change in orders (Harris & Pinder, 1995). RM transforms the objective from maximizing utilization to maximizing profit (Infineon, 2019a). In fact, data shows that businesses that have adopted RM systems are able to enjoy an increased revenue of about 3-7%, with nearly no significant capital expenditure (Wang & Bowie, 2009). Hence, the manufacturing industry too may greatly benefit in revenues and smoother management through price and capacity optimization. Especially Infineon Technologies AG (IFX), as it is the pioneer in its field and is moving towards the data-driven economy through potential revenue gains for the semiconductor industry.

Given that manufacturing cycles are prone to be significantly long in the manufacturing industry (Berger, 2017), an important measure and a key characteristic of effective RM is ‘lead time’. This is the duration between the customer’s order entry and the different dates of action (requested order lead time/confirmed order lead time/contractual order lead time, further explained in Chapter 3).

Subsequently, orders are sometimes cancelled and often modified in the semiconductor industry. Furthermore, customers often request for finished products at an earlier date, than the date stated in the master contract (Berger, 2017). In some cases, businesses can deliver completed products before the contractual date of delivery. For instance, in case of cancelled or changes in orders by one customer (for instance, reduced quantity), (almost) ready products are available for another customer requiring the same product. Provided this earlier delivery can be made, this situation leads to an opportunity for the business to make a profit. Currently, this enhanced service in reduced time comes with no additional payments by customers (Berger, 2017). Hence, the adoption of a RM system with dynamic price setting which incorporates a mark-up price would allow the firm to leverage higher revenues in return for faster than contractually dated deliveries.

While RM is certainly useful for businesses, its success still depends on the customers' willingness to pay for such improved services. While overpricing may cause customers to be uninterested in the firm's products, forcing it out of the market, a correct pricing strategy would lead to more loyal customers. This is possible provided the required products are delivered in the requested earlier time and in good quality. This is known as lead time-based pricing (LTBP) (Berger, 2017). The opportunity of applying revenue management at Infineon is seen in Fig 1, when deliveries can be made before the contractual delivery date.

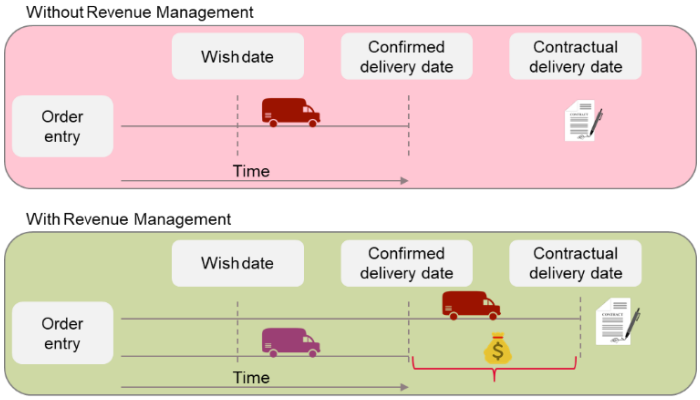


Fig 1: Opportunity for revenue management in the semiconductor industry

1.2 Multi-Party Computation – a tool for implementing revenue management

Secure multi-party computation (MPC) is a cryptographic technique that allows distributed parties to jointly compute a function without disclosing their private inputs. MPC, as a tool for computing with confidential data, has an advantage in overcoming security and privacy concerns in situations where owners of different types of data would like to compute cooperatively. This allows the integration of resources while preserving confidentiality, and resultantly obtaining more valuable information (Zhao et al., 2019). SafeDEED (further explained below) proposes MPC as a solution to implement revenue management, as it provides an added value and would simplify the computation process while safeguarding customers' and suppliers' confidential data (SafeDEED, 2018). Both parties would remain anonymous to one another during the process in order to preserve existing customer-manufacturer relations. Not only would this enable the manufacturers to securely expose their unallocated Available-To-Promise (ATP) data on a daily basis, but also provide customers with the opportunity to view and buy from this inventory of uncommitted stock of the manufacturer by sharing the confidential maximum price that they are willing to pay. The outcome of the computation will provide a revised price, delivery date and quantity.

1.3 Safe-Data Enabled Economic Development (SafeDEED)

Delft University of Technology and Infineon Technologies AG participate in the Safe-DEED project funded by the European Commission as part of the Horizon 2020 consortium. The project presents the opportunity to collaborate with parties who bring various expertise to this project, ranging from technical support, business modelling, data valuation to multi-party computation. Within the project, it is one of the objectives to integrate the new MPC technology into an order management platform with an analogous functionality to an e-commerce store

where customers of a manufacturer can buy from the unallocated ATP from the manufacturer, securely and privately.

1.4 Knowledge Gap

Need for trust and confidentiality in the business-to-business (B2B) scenario
Dynamic pricing (which is the foundation of revenue management) causes uncertainty where buyers regard a bigger risk of overpaying as well as sellers are afraid of not receiving the desired amount for their products (Chakravarty et al., 2014). It could also be that the manufacturer and its customers engage in a (reverse) auction for earlier delivery dates. Then, the manufacturer and the customers would want their contracts and the bids to remain confidential while also providing the manufacturer with an opportunity to increase its revenue (Kenton, 2018). Therefore, the complexity in managing various customer sides with diverse and conflicting demands remains a marketing challenge for B2B platforms, where customer orientation is the main mechanism for engaging customers. Thus far, research has not addressed how B2B platform firms manage their customers (Chakravarty et al., 2014). Luca (2016) further describes that building enough trust to facilitate transactions between strangers in online platforms is still an issue. Essentially, trust between buyers and sellers is aided by reputation mechanisms and careful design choices made by the platform. Further research would be useful to analyze platform design choices and to monitor their effect on the eventual success of the platform. Moreover, qualitative research could demonstrate how different actors perceive the design choices (Tura et al., 2018).

Human-Computer Interaction and Security
Additionally, there are challenges revolving around comprehension and usability that are neglected in the design of existing MPC frameworks. While security is of prime importance, the usability of systems employing MPC is equally vital, so that users are precisely able to understand what is guaranteed. Furthermore, Lapets et al. (2016) prove how two off-the-shelf MPC solutions fall short of meeting the usability requirements. One of the solutions fails to meet the accessibility criteria as it is not easily accessible by novice users who lack the technical expertise to use the system. At the same time, the second solution is complex, its closed-source design hinders comprehension, as well as its deployment demands advanced technical expertise. Therefore, general-purpose MPC platforms require strong UI/UX features before deployment. The necessity for this is emphasized because participants still require that the service provider sign a non-disclosure agreement regarding the data submitted by these parties, despite the guarantees provided by secure MPC (Lapets et al., 2016). Therefore, there is a gap between designing usability and security together during the development of secure systems (Kainda, Fléchais & Roscoe, 2010). The field of human-computer interaction and security (HCISec) demands attention in incorporating both, usability and security, in order to communicate security implementations to new users. Consequently, this would lead to successful implementations of cryptographic technologies (Smith, 2003). Overall, website usability and security have a positive impact on customers' trust in the firm (Kim & Ahn, 2007).

Use case
Concisely, there is a lack of trusted and secure platforms in data aggregators and suppliers. MPC has not yet been visualized and is difficult for users to imagine, similar to RM in the manufacturing industry. Two issues are the lack of trust in data sharing in personal and

business virtual environments, as well as people being afraid of external control and loss of self-determination due to data abuse. Employing MPC will allow Infineon to execute improved business without having to disclose confidential data. Consequently, daily unallocated ATP data is provided by the manufacturer, which relates to order, customer and product data. This is confidential corporate data which also includes information about product demand, annual total sales and customer price sensitivity, implying the importance of confidentiality in this case.

1.5 Problem Statement

Revenue management holds the potential for businesses to capitalize on missed revenue and for customers to receive their products faster and/or on short notice. A RM platform is valuable for the industry as the manufacturers can share their expected prices, unallocated ATP and possible delivery dates, anonymously. The platform can then match customers to the firm according to customer demands. The SafeDEED project proposes multi-party computation as a solution to implement revenue management due to its applicability in computing on confidential data from multiple parties, which is crucial in the case of RM (SafeDEED, 2018). However, as MPC is a new and developing technology and RM is new for the semiconductor industry, we do not yet know what this implementation would look like, especially how it would be perceived by customers. While online communities of users and their interaction with businesses are encouraged by digital platforms (Reuver, Sørensen & Basole, 2017), it is important for the platform to facilitate the acceptance of this technology.

A major challenge remains regarding customer acceptance towards a new RM platform and gaining customers' trust. Customers' acceptance of this platform could make or break companies in the industry. As we can see in the case of the airline industry, the introduction of RM led to companies either adopting it and emerging successful, or declaring bankruptcy by failing to adopt RM (Talluri & van Ryzin, 2004). While customers should not feel like they are being overcharged, semiconductor firms should be able to make higher profits through faster deliveries. Currently, manufacturers are wary of customer reactions and any mistakes could cost them their reputation in an already tough market with small margins. Additionally, the manufacturer wants to keep the unallocated ATP information confidential, while the customers want to keep the maximum price they would be willing to pay for earlier deliveries, confidential. Therefore, the manufacturer and its customers would participate in the MPC protocol to compute a revised, earlier delivery date and an increased price. In the end, both parties would learn the new delivery date and an updated price (SafeDEED, 2018).

The introduction of RM with MPC would significantly change the manner of how business is conducted in the manufacturing industry. The first step in order to understand customer acceptance of these two technologies is to establish what a potential implementation of their integration would look like and communicate this to users. At present, there is extremely limited literature in the field of applying MPC to a use case, visualizing and communicating it to users. RM and its advantages suited to the manufacturing industry, are studied in depth (Chiang, Chen & Xu, 2006; Kimes & Wirtz, 2015; Zatta, 2016), however, MPC has only been theoretically studied and not yet practically applied or visualized for any real case (Roman & Vu, 2019; Sousa, Antunes, & Martins, 2017; Zhao et al., 2019). Establishing this visual integration would help to further study how this platform is perceived by customers in terms of usability and acceptance.

1.6 Research Objective

It is seen that there are major challenges when it comes to visualizing a(n) (upcoming) secure technology (such as multi-party computation), communicating this to customers while ensuring it is usable. Establishing this is important for understanding customer acceptance of such a technology. The research objective is to outline the application of multi-party computation to revenue management, which adds value and facilitates achieving the functionality of revenue management in reality. Furthermore, the objective is to design, evaluate and propose a visual representation and integration of multi-party computation and revenue management, in order to understand customers' trust in the system and supplier, perceptions of security, usefulness, ease of use and intent to use revenue management with multi-party computation.

1.7 Research Question

Following are the main research question (RQ) and sub-questions (SQ) to guide the research:

How can multi-party computation be applied to and visualized with revenue management as a platform interface in order to enhance users' trust in the system and supplier, as well as enhance perceptions of security, perceived usefulness, perceived ease of use and intention to use?

1. What is MPC and what is its functionality in RM and the use case?
2. What data is required to simulate the result of MPC and what data involved is confidential?
3. What are the different customer types of Infineon and what is the targeted customer segment for participating in RM?
4. What attributes can enhance trust and acceptance?
5. How can the mock-up artefacts be evaluated?

1.8 Approach

The semiconductor industry is facing challenges in understanding how a potential RM with MPC platform would look like, and how this would be perceived by their customers. To answer the research question, we adopt the design science research (DSR) approach to present artefacts in the form of mock-ups that for the first time, combine and visualize RM and MPC. To conduct this research systematically, we adopt Hevner's (2007) three stage design process, which involves the relevance cycle, the rigour cycle, and the design cycle. DSR involves creating and evaluating IT artefacts intended to solve organizational challenges (Hevner, March, Park & Ram, 2004). We further evaluate the mock-ups through experiments in order to propose a platform mock-up that addresses the challenges relating to customer acceptance of such a platform. Moreover, the results of design science research include the artefacts as well as the knowledge of how other artefacts can be designed in the same class of problems (Hevner et al., 2004). This approach is further suitable for the problem at hand because it involves managing the requirements and overcoming the challenges of the different people involved (customers and manufacturers) to address a complex industry-wide challenge.

We design and evaluate three different mock-ups so that participants can experience new and varying visuals of the integration of the upcoming technologies (RM and MPC). The three different artefacts also allow room for an open discussion to include all the important factors

that can influence acceptance. Participants first use the three different mock-ups and then participate in an interview to discuss their choices. We opt for this method instead of direct interviews or surveys prior to designing the mock-ups because presenting the artefacts first, and then evaluating them allows the participants to visualize something very new for them so that they can more concretely describe their feelings in the interviews that follow the experiment. As MPC is not yet practically developed and the semiconductor industry has not yet adopted RM, this study takes a design science approach to present the first scientific step in understanding how such an implementation would look like and how customers perceive this, leading to new areas of inquiry. Based on the literature on multi-party computation, technology acceptance, revenue management, human-computer interaction and security as well as the context of the case, we deduce the design requirements and proceed to design and program four digital platform mock-ups (current buying platform and three potential future platforms) via Visual Studio. Learning C# was essential for the research in order to design the mock-ups as realistically as possible to allow participants to interact with these during the evaluation stage.

1.9 Research Contribution

The contribution of this research is twofold, in terms of scientific as well as practical contribution.

Scientifically, the research sheds light on visualizing and communicating the cryptography technology of secure multi-party computation along with revenue management. This study is a first that presents a potential user interface of RM and MPC. We propose such an implementation on the basis of understanding customers' trust and acceptance of revenue management as well as data protection through secure multi-party computation. This research takes a leap forward by combining and visualizing MPC with RM in various ways, taking a step ahead of conceptualization and understanding the factors relating to customer acceptance towards such a revolutionary platform that will reform exchanges across the industry. Human-computer interaction and security (HCISec) is a challenging research field where researchers continue understanding how security and usability can both be incorporated during the design and development of security systems (Kainda et al., 2010; Smith, 2003; Yee, 2004). Therefore, as we incorporate usability in the design of the integration of MPC and RM, the artefacts of our research can be seen as a significant contribution developed via the design science approach along with understanding the factors that could facilitate the customer acceptance of such a platform. MPC has not yet been visualized, applied or communicated to customers. As usability plays a significant role in the success of cryptographic implementations (Smith, 2003), we present a first step in incorporating usability factors in designing, visualizing and communicating MPC to users.

Usually, the contribution of design science research is the artefact itself. Effective design science research has at least one of the three types of research contributions based on the novelty, generality and significance of the designed artefact (Hevner et al., 2004). The artefact enables the solution of problems being faced. According to the authors, this could either be through extending the knowledge base or by applying existing knowledge in an innovative way. The mock-ups designed in this research are an example of this. We extend the presently lacking knowledge base in visualizing cryptographic technologies (specially MPC) by

proposing a potential visual implementation of RM and MPC to facilitate understanding customer acceptance of such a platform.

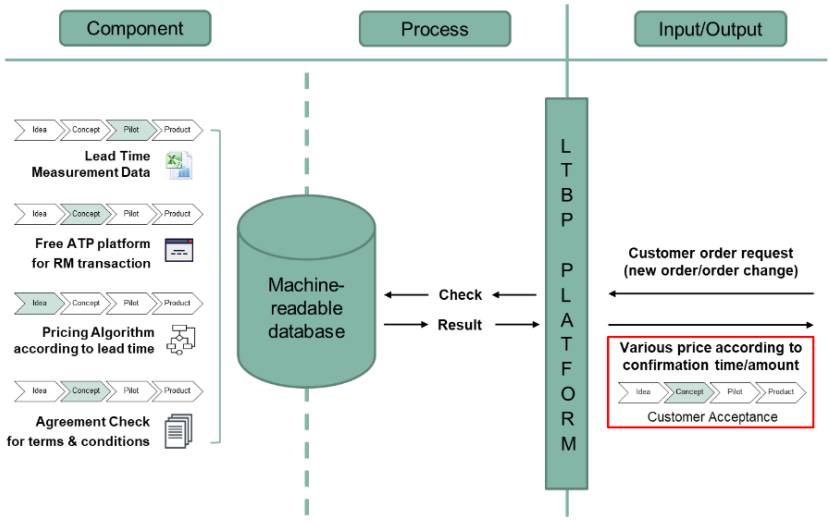


Fig 2: Practical contribution of the research (evaluating customer acceptance for the introduction of the lead time-based pricing platform)

Practically, the research is a step forward towards implementing RM along with MPC as a platform technology in the semiconductor industry. As one of the major barriers preventing its introduction in the industry is company's wariness pertaining to customer's trust and acceptance, this research will be able to guide the design and implementation of such a platform, taking into account customers' perceptions. Infineon is on the journey of digital transformation and sees the potential implementation of RM and MPC as a value addition to its business and the manufacturing industry. Several initiatives around lead time-based pricing are in the pipeline at Infineon. While there is a lot of work being done in most of the projects, the pricing algorithm for lead time-based pricing is still in its ideation stage. This research helps in taking the project about customer acceptance, from ideation to conceptualization (as seen highlighted in Fig 2) and visualizes RM with MPC for the first time. In the long run, a digital platform will facilitate in maintaining anonymity and matching consumer demands to firm's supplies, creating a win-win situation for consumers and businesses. This study proposes a potential integration of RM and MPC and is a significant initial step from manufacturers in order to enter today's data-driven economy via such a platform.

Essentially, representational fidelity and implementability form the basis for assessing the contribution of design science research, implying that the artefacts should represent the business and technology case setting used for the research, accurately (Hevner et al., 2004). We conducted this research directly in the field setting, signifying the reliability of the obtained data. Additionally, these artefacts are implementable, emphasizing the significance of instantiating design science artefacts. Apart from these, the research demonstrates a contribution to the business environment, solving an important and previously unsolved problem of visualizing RM and MPC together in a platform. It contributes in terms of the artefacts themselves, wherein a RM platform with MPC is modelled for the first time, to the best of our knowledge. The evaluation of these artefacts via experiments enable assessing customers trust in such a new platform and it which will help to guide the design of the future platform while keeping in mind the important factors relating to customer acceptance that are discovered in this research.

1.10 Structure

This research focuses on designing, evaluating and proposing a visual integration of RM and MPC, accounting for customers' acceptance of such a platform in a B2B setting. Chapter 2 details the research method we adopt for conducting this study, following Hevner's (2007) three stage design process. Following this, the next four chapters include the Relevance cycle, Rigour cycle, Design Cycle and Evaluation. In Chapter 3 (Relevance cycle), we discuss the use case, the current ways of practice and the potential to implement revenue management and multi-party computation. Then, Chapter 4 (Rigour cycle) provides an overview of the necessary background related to revenue management, secure multi-party computation, auctions and customer acceptance. Together, these build the foundation which guides the knowledge gap, problem statement as well as the research question and sub-questions of this research. Chapters 5 and 6 explain the Design Cycle, including the artefact design as well as the evaluation. We then proceed to present the results and discuss these in Chapters 7 and 8 respectively. After reflecting on the limitations of our research in Chapter 9, we discuss the conclusions and recommendations for further research in Chapter 10. Lastly, we conclude with reflecting on our research, both, scientifically as well as practically.

2. Design Science Research

In this chapter, we describe our design science research (DSR) approach according to Hevner's (2007) three cycle view of DSR. We present the three cycles (Relevance, Rigour and Design) suited to our research in the next four chapters. Firstly, the Relevance cycle includes the context of the case, where we examine the potential of applying revenue management and identify the current business process flows, as well as the current buying platform of Infineon. Then, in the Rigour, Design and Evaluation chapters we elaborate on the state of the art in revenue management, multi-party computation, technology acceptance and human-computer interaction, while we also establish the research model, design the artefacts and discuss the evaluation method.

We use the three cycle view of DSR as proposed by Hevner (2007). According to the author, there are three inherent research cycles that holistically make up the design science approach. They are the Relevance cycle, the Rigour cycle and the Design cycle (Fig 3). The Relevance cycle is related to the environment in question and it bridges the design activities together with the knowledge base, by presenting a contextual environment of the research project with the design science activities. Then, the Rigour cycle pertains to the knowledge base and connects the design science activities with the knowledge base of scientific foundations that informs the research project. Lastly, the Design cycle involves the building and evaluation of the design artefacts and/or processes of the research. The author elaborates that these three cycles must exist and be clearly identifiable in a design science research project. We follow a similar design cycle and present our methods in the following four chapters.

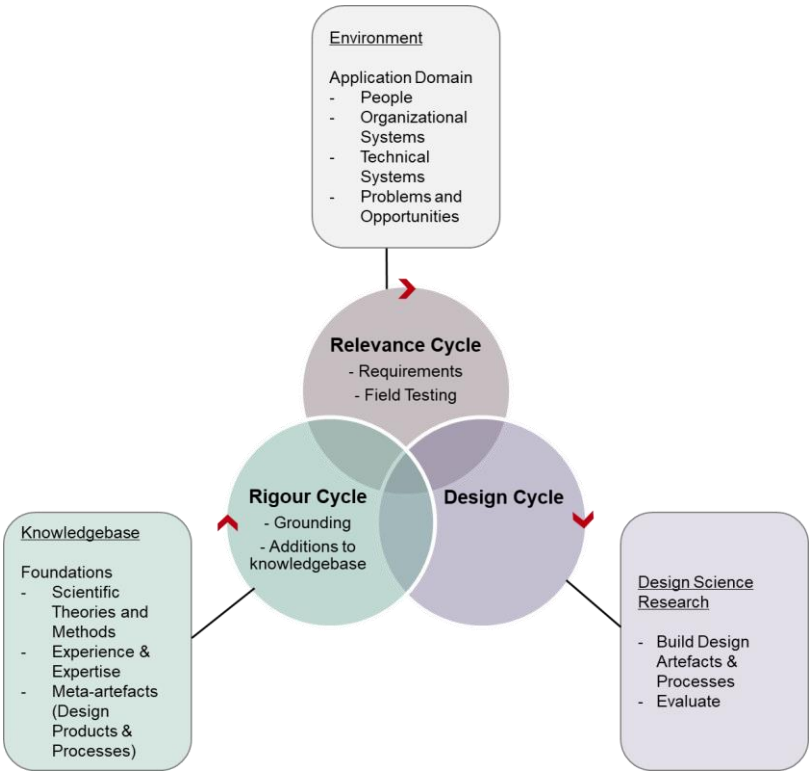


Fig 3: Design Science Research Cycles (adapted from Hevner, 2007)

To answer the research question, the research follows a three step process. Firstly, as per the Relevance cycle, our research commences with the identification of a practical problem; the challenges related to visualizing a potential integration of revenue management and secure multi-party computation in order to understand customer acceptance. The goal of design science research is to develop technology-based solutions for critical and relevant business challenges (Hevner et al., 2004). The research also fits the agenda of the fully-funded EU-wide SafeDEED project (SafeDEED, 2018) which proposes MPC as a tool for adding value to RM. The environment can be understood to be the field where field research needs to be undertaken to apply the learnings in a real-life setting. The field, being the other facet of design research aids in further grounding of the research and ensures relevance by tying it to the reality organizations are facing in practice (Hevner, Ram, March, & Park, 2004).

Secondly, once we understand the context of the case, the Rigour cycle involves deep-diving into scientific research in the fields of revenue management, secure multi-party computation, human-computer interaction and security as well as technology acceptance. This knowledge base played a role in developing the research model (Fig 16) for understanding the concepts related to secure platform technology acceptance. After identifying the knowledge gaps, the research question is developed, along with the formulation of sub-questions. The design requirements address the innovate artefact to be designed, the issue it solves, the criteria of evaluation for success, the research contribution, the rigour of the research methods used, the design approach itself and the communication of findings (Hevner et al., 2004). To combine rigour and relevance, the research needs to be firmly grounded in state of the art in the field and the current environment. By analyzing the literature and the recognized approaches of conducting research, one can ensure rigour in the design. Learning from a design effort is a key part of the design science research. For this, desk research is vital, to understand the current processes and state of art. We use this knowledge along with the context of the case as well as the researcher's creativity for the third part of the study – artefacts' design and evaluation.

According to Cross (1993), both these facets (literature and field research) are crucial for design science research and design as a scientific activity does not only entail problem-solving, but it also entails the application of existing knowledge to solve a prevailing challenge. Therefore, we use a combination of desk research, the case context and interviews to develop, evaluate and propose a platform mock-up that establishes a potential visual implementation of RM and MPC with respect to usability factors (trust, security, perceived ease of use, perceived usefulness and intention to use). Subsequently, the design is a solution to an organizational or industrial challenge, for which a solution in the literature does not exist yet (Lu, 2010). Design science is particularly apt for developing supporting tools that can be deployed in organizations to enhance current ways of practice. In situations where complex and relevant-to-stakeholder solutions must be rigorously designed, design science provides the basis for research (Lu, 2010).

In our final Design cycle, we create the artefacts that integrate RM with MPC in various ways to understand customers' usability perception. Then, we take a qualitative approach for evaluating the artefacts, where participants are interviewed after they take part in the experiment which involves using the various mock-up artefacts. Through the analysis, we consolidate participants' feelings and concerns as well as present them, so as to identify the factors that enhance or hamper usability concepts (trust, security, perceived usefulness,

perceived ease of use, intention to use) with respect to each mock-up. In the end, we propose an artefact that visualizes the integration of RM and MPC as a platform technology that combines the best performing features of each mock-up and drives customer acceptance. In this manner, we integrate usability in the applicability of the cryptographic technology of multi-party computation to revenue management.

Hevner et al. (2004) elaborate that artefacts can differ in form, from software and logic to informal language descriptions. The design of the artefacts in our study focusses on the look and feel as well as the logic of RM and MPC from the customer's perspective. The literature review and context of the case, together, led us to identify the usability requirements that inform the design of our artefacts, including the final artefact that we propose in Chapter 8. The evaluation of the designed artefacts plays an important role in the holistic process of designing, implying that the design should satisfy a set of design requirements. Thus, we then conduct interviews for collecting data for evaluation. The challenge lies in defining these requirements due to the limited literature in the field of practically applying MPC to RM. We evaluate the mock-ups based on the usability aspects that drive acceptance.

Venable, Pries-Heje, & Baskerville (2012) discuss the purposes of evaluation in design science research, explaining that evaluation is the "science", in design science. Accordingly, the mock-ups are evaluated via experiments, where participants use each platform mock-up and complete the entire buying process each time. The artefacts are evaluated in comparison to the other designed artefacts' ability to achieve a similar purpose. Moreover, a new proposed artefact should provide higher relative utility than the other artefacts that could be used to achieve the same purpose. Along with comparison of artefacts with each other, another purpose suitable to this study is to evaluate an instantiation of a designed artefact to establish its utility and efficacy (or lack of thereof) for attaining its specified purpose. In this case, the purpose is not only to establish a potential implementation of RM and MPC but also to evaluate the artefacts with regards to trust, security, perceived ease of use, perceived usefulness and intention to use. The participants of the experiment evaluate the designed artefacts against each other and also in comparison to the current buying system according to what provides a higher relative utility in terms of customers' trust, security, perceived ease of use and usefulness, intention to use leading to the adoption of RM and forming a perception of Infineon's image.

Utility depends on several characteristics of the artefact and the desired outcomes through using the artefact. Essentially, "utility" is a complex concept and is not the only thing being evaluated in design science research. Therefore, it is vital to identify how utility for achieving the artefact's purpose can be evaluated and the characteristics that can be assessed. Extending this, we establish the usability criteria, informed from the literature review. Every evaluation is specific to the artefact, its purpose and the purpose of evaluation (Venable et al., 2012), which in this case, is usability (perceived usefulness, perceived ease of use, intention to use, trust and security) and customer acceptance of the platform. According to the three cycle view described in this chapter, we now describe the Relevance, Rigour and Design cycles in the following chapters.

3. Use Case (Relevance Cycle)

This chapter discusses the potential of applying lead time-based pricing and revenue management in Infineon, proving its practical relevance. We begin by identifying and reporting the present situation of the actual application environment and the opportunities and problems as indicated by Hevner (2007). The relevance cycle initiates DSR with an application context that provides the requirements for the research. Infineon Technologies AG, a pioneer business in the semiconductor industry, is adopted as a use case for this research because the semiconductor industry is characterized by volatile market demand, long production times and high capital investment (Ehm & Ponsignon, 2012), which together, are a model representation of the manufacturing industry. Furthermore, multiple initiatives by Infineon prove their business goals of introducing revenue management, as well as multi-party computation as a tool to implement revenue management.

We begin by demonstrating the potential for RM and lead time-based pricing (LTBP) at Infineon. Then, we compare the current volume-based pricing versus the new lead time-based pricing (LTBP), which is still under development (at the ideation phase in the project). LTBP is the foundation of RM and it is helpful to recognize its differences against the conventional volume-based pricing, in order to understand the huge change that this pricing system will be for customers. Then, the business processes for order management are briefly discussed, along with an explanation of the current buying platform of Infineon. Understanding these are necessary for grasping the case setting, planning the artefacts' design and understanding the advantages of a RM platform with MPC in comparison to the current business practices. Presenting the current processes prove that there would be a revision in the methods of practice with the introduction of revenue management and multi-party computation. Subsequently, the involvement of the Sales department would reduce, as MPC would proceed with the computations automatically. Furthermore, the current order management process would need to expand in order to accommodate the introduction of revenue management and multi-party computation. This means that in addition to the price quotes being checked internally for acceptance or rejection, bids would now not only need to be compared with the internal dynamic price adder range set by Infineon, but also among other customers in order to accept the most suitable quote. This highlights the change in processes with the introduction of RM and MPC.

For the data collection, Infineon's intranet is greatly used. All the current order management flowcharts are adapted from the ARIS platform, which is a powerful and intuitive tool for business process modelling (BPM) for enterprises. The graphs that visualize the potential of RM (Fig 5) are generated based on the order lead time data that was is recently obtained through the progress of the order lead time tool. In addition to this, previous theses and internal company presentations also help to build knowledge of current practices.

The purpose of DSR is to develop solutions to solve critical and relevant challenges for organizations (Lu, 2010). Similarly, design science, as explained by Hevner et al. (2004), crafts and assesses IT artefacts that are meant to resolve already recognized organizational challenges. Accordingly, the practical essence of this research roots from the challenges in anticipating customer perception and acceptance of a RM platform using MPC, in the manufacturing industry. The fundamental design and functionality of the integration of these

two technologies are novel to the industry. Additionally, Simon (1996), laid the basis of the role of science of design in mathematics. He explains designing as a search process within a closed solution space, consequently establishing an optimized design or respective optimum (Simon, 1996). Not only does this DSR contribute through developing artefacts for RM with MPC in the form of platform mock-ups, but also, we propose a potential visual implementation of RM and MPC at the end of our study, referring back to Simon's (1996) "optimized design or respective optimum".

3.1 Potential for LTBP and RM

Through analyzing the current data for order lead times at Infineon, the need for both RM and MPC is visualized in Fig 45. To understand further, the following explanations are important (Berger, 2017):

- Requested order lead time (OLT_req) is the difference between the requested date (by the customer) and the purchase order date.
- Confirmed order lead time (OLT_cmfd) is the difference between the confirmed date (by Infineon) and the purchase order date.
- Contractual order lead time (OLT_sales) is the delivery time communicated by sales, to the customer.

As seen in Fig 4, firstly, when the contractual date is greater than the wish date, it presents the theoretical potential for RM (OLT_contract – OLT_requested). Secondly, the difference between the contractual date and delivery date represents the practical potential of RM (OLT_contract – OLT_actual). Lastly, the difference between the contractual date and the confirmed date from Infineon represents the reality RM offers (OLT_contract – OLT_confirmed). Putting this altogether, for RM to be applicable, the condition is: OLT_contract > OLT_confirmed ≥ OLT_requested.

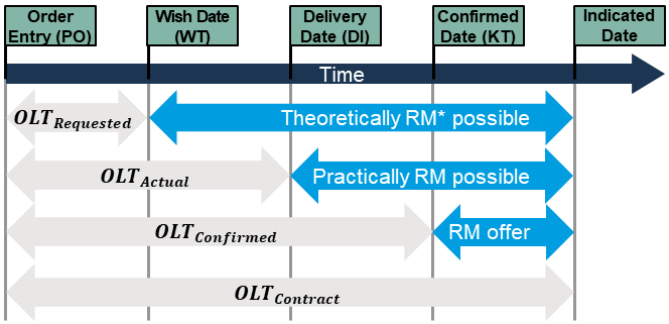


Fig 4: Potential for lead time-based pricing and RM

The graphs below depict the opportunity to implement a revenue management system. When the customer requests for an earlier delivery (OLT_requested) and Infineon is able to confirm the order (OLT_confirmed) short of the contractual order lead time (OLT_sales), the lead time difference between the contractual and confirmed dates presents the applicable potential for revenue management. The theoretical potential lies in the difference between the requested and contractual dates (Infineon, 2019b). This analysis is based upon recent historical data for a package within one product line. In reality, there are multiple packages within multiple product lines, exemplifying the extent of the potential of implementing a revenue management system.

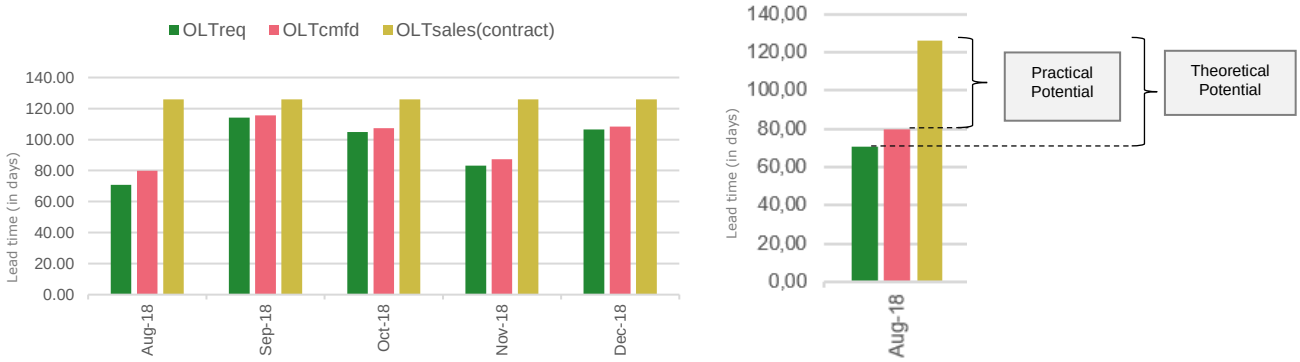


Fig 5: Potential for lead time-based pricing and RM

In addition to the above-identified potential, the semiconductor industry faces diverse customer demand and a high fixed cost. This relates to the bullwhip effect, which is the phenomenon referring to increasing swings in inventory in response to shifts in customer demand as one moves further up the supply chain. The bullwhip effect is evident throughout the supply chain because the supply and demand do not usually synchronize in real-time (Infineon, 2019a). Furthermore, the supply chain is complex because of long production times and low flexibility.

Implementing RM at Infineon will help in steering demand which in turn, will reduce the bullwhip effect and demand fluctuation. Secondly, Infineon can generate more revenue with an unchanged capacity, consequently, increasing the business' profitability. Lastly, it will reduce individual negotiations and thus, will enhance operational efficiency (Infineon, 2019a). Therefore, monetizing lead-time and the development of LTBP would by key for introducing RM.

3.2 Volume-based Pricing versus Lead time-Based Pricing

Volume-based pricing at Infineon is based on the customer's promise to purchase a particular volume of product over the life of the contract. Based on the volume, a discount is deducted from the product's unit price upfront. However, it is risky for the supplier, as it is possible that the customer does not fulfil orders of the volume they promised. According to the sales analysis, it is learnt that by the end of the aggregation period many customers do not purchase the amount of quantity as they quoted (Ma, 2008). During the quoting process, the customer states a higher volume in order to receive a good quoting price from Infineon. Once Infineon confirms the customer's quote, the quoting price is stored in SAP (System Applications and Products) for the entire aggregated period. During this period, the customer frequently orders all volumes based on this quoting price, which is lower than the original list price.

As the supplier has already offered the discount based on the estimated demand volume upfront, the supplier must decide whether or not to include penalties for buyers that are unable to attain the agreed-upon purchasing volume. A penalty is particularly essential for contracts that entail high product customization or involve a significant upfront cost. However, it is challenging to impose penalties on contracts where the supplier has low bargaining power. As for the semiconductor industry, where competition is tough and margins are tight, the suppliers do not have high bargaining power against their customers. Therefore, most long-term contracts do not involve penalties and are principally built upon trust. In cases where the

customer falls short of purchasing the promised volume, the supplier would only consider increasing the unit price during the negotiation cycle of the next contract.

In addition to volume-based pricing, other pricing initiatives at Infineon include lead time-based pricing. While lead time-based pricing is applied before the product's list price, targeted towards customers who request for a shorter lead time, volume-based pricing is applied after the list price (Ma, 2008). Revenue management is an application of lead time-based pricing, and its algorithm has not yet been fully developed at Infineon. RM involves including customers in the price, volume and delivery date quotation, allowing them to put forth different choices and ensuring them that a fair output will be reached via secure MPC. Customers need to trust and believe that they are being charged fairly, in order to nurture the supplier-customer relationship while allowing them to receive earlier deliveries as and when required. This also depends on Infineon's confirmation about the ability to deliver.

3.3 Current Processes

The current order management process at Infineon is elaborated in Appendix 1. Current Processes at Infineon. Comprehensively, the Sales department is currently involved with taking and confirming orders. They are the point of contact for any communication with the customers, carrying out manual checking in the system for the price, volume and delivery date quotations. Additionally, the orders are eventually promised to customers by Sales too. Through the new RM platform with MPC, the combination of having the daily unallocated ATP data and MPC computing the optimal output will greatly ease the work of the Sales team. Furthermore, with the introduction of the new system, bids would not only need to be compared with the internal dynamic price adder range set by Infineon but also against other customers in order to accept the most suitable quote. These reasons highlight the changes in processes required due to the introduction of RM and MPC.

3.4 Current Buying Platform

Commonly, Infineon's business is conducted via EDI (Electronic Data Interchange) and SAP (System Applications and Products). Nonetheless, a portion of the business uses the following buying platform. With the introduction of RM, this platform has the potential to grow and expand.

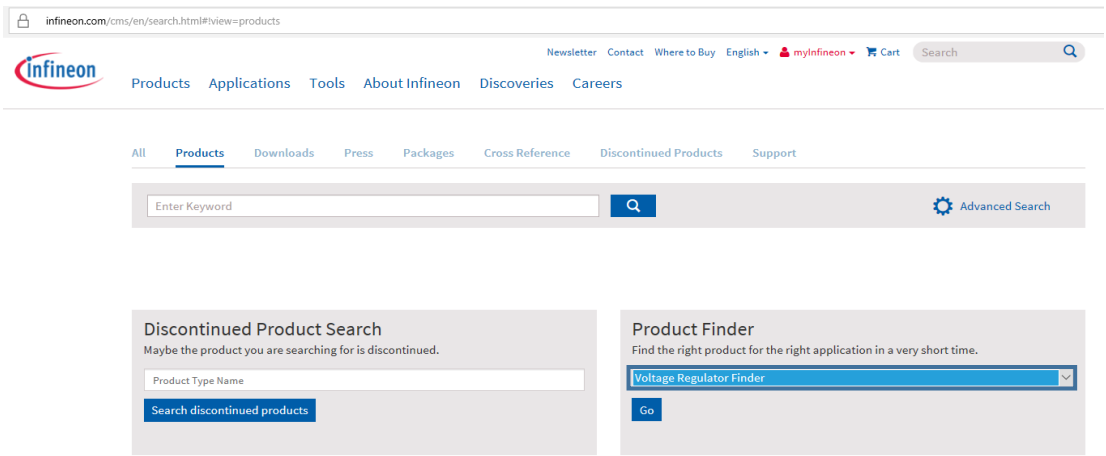


Fig 6: Landing page of current IFX ordering platform

The current buying platform of Infineon which allows customers to place orders is shown in the image above. On this landing page, there are options to search for discontinued products, as well as current products. In this picture, “Voltage Regulator Finder” is being searched for, chosen from the drop-down menu of products.

On the next screen (Fig 7) a list of all the products is made available, along with all their characteristics. For more precise searches and results, various parameters can be selected and the display table can be configured.

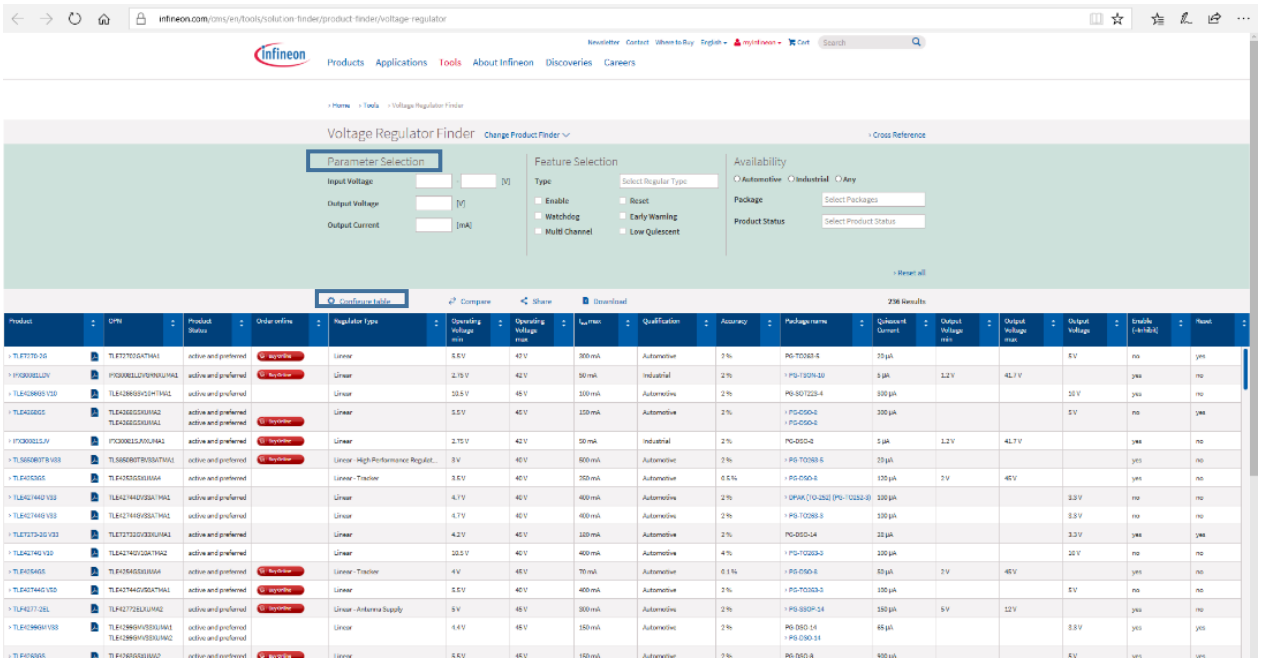


Fig 7: Products search results

Fig 8 and Fig 9 depict the ordering system. On clicking “Buy Online” for one of the products (row 2), Fig 8 shows the price of 1 unit as $0.99, with $4.99 shipping charges. Additional information available includes the stock available for purchase.

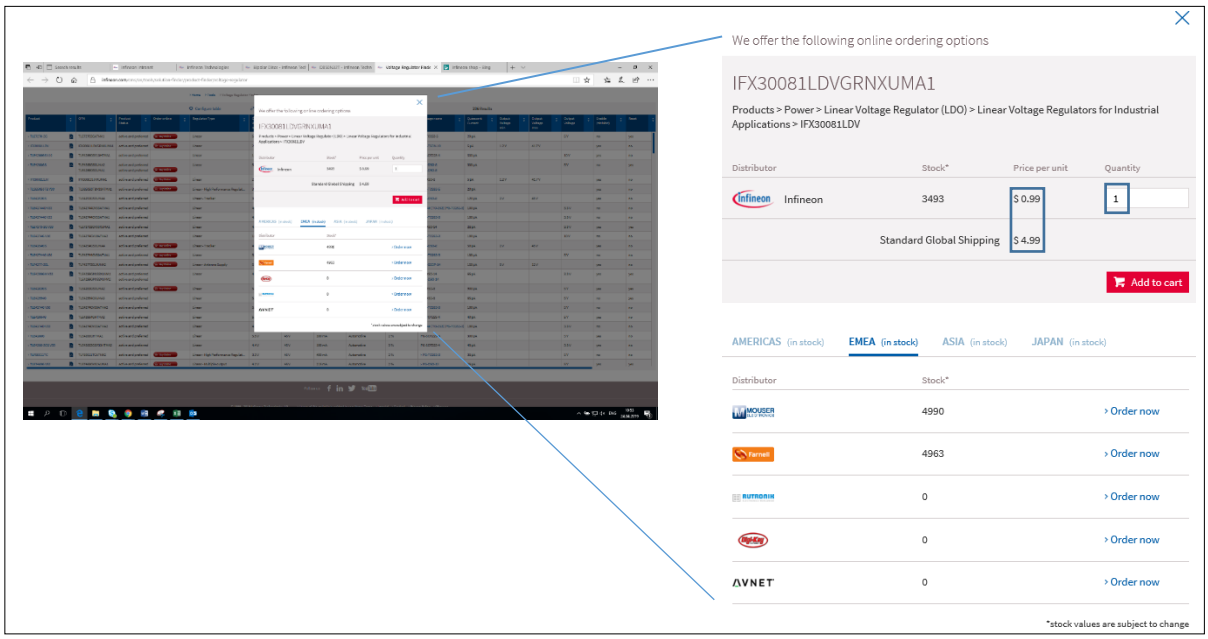


Fig 8: Reduced ordering quantity

Below, the change in price is visible when the intended ordered quantity is increased to 1000 pieces (in comparison to 1 piece in the previous figure). The price now drops to $0.455 with shipping charges remaining the same. This clearly depicts the application of volume-based pricing as discussed above.

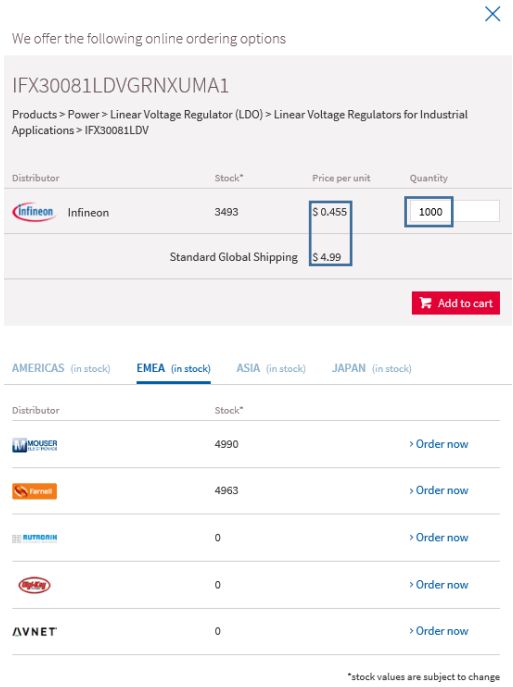


Fig 9: Increased ordering quantity

As it is visible, customers are only able to enter their desired quantity via this platform. This platform does not have dynamic pricing functionality which is the essence of lead time-based pricing. This is the foundation of revenue management. In order to enable customers to have their orders earlier and for Infineon to capitalize on missed revenues, an innovative, novel platform that enables RM is required. Through this section, we understand how orders are currently placed and processed, without the ability to involve customers in setting the price, quantity and delivery date altogether. Currently, this is not an auction, and every quote is checked internally before it is accepted, rejected or revised. The integration of RM with MPC will simplify processes, should RM be implemented. For instance, without MPC, the sales department would have to be more involved, performing manual tasks which can be simplified with the integration of MPC. Moreover, after understanding the current buying process and platform, we have established the applicability of MPC to RM, which is further described in the design cycle.

4. Literature Review (Rigour Cycle)

In this chapter, we provide an overview of revenue management, secure multi-party computation, auctions as a tool for revenue management, human-computer interaction and security, as well as factors influencing customer acceptance. The artefacts and the interview protocol are designed based on literature and the context of the case, described in Chapter 2. We start by identifying the attributes of RM, proving the similarities between the service and manufacturing industries for the applicability of RM. We then explain multi-party computation and its relevance to this use case. After explaining what are auctions, the different types of auctions are described, which help to later outline the precise auction setting to implement RM for the use case. We proceed with discussing literature on human-computer interaction and security along with customer acceptance of technology. A few Technology Acceptance Models (TAMs) are identified, which are used to build the research model for this study.

Design science relies on the knowledge base of scientific theories in order to provide the foundation for rigorous design science research. We now describe the approach for obtaining the data for our literature review. The apt selection and application of relevant knowledge determine the rigour of our research. For the literature review, different keywords were used to identify the relevant literature for this research. These included but were not limited to “multi-party computation”, “multi-party computation auctions”, “sealed-bid multi-attribute auctions”, “acceptance of multi-party computation”, “revenue management in the manufacturing industry”, “trust and TAM of information systems”, “customer intention to use B2B secure platforms”, “human-computer interaction and security” and “design science research”.

4.1 Revenue Management

There are certain attributes of RM that are required to be present for its applicability. Firstly, customer segmentation plays a vital role in the successful implementation of RM. The foundation of RM is based upon customer heterogeneity. Segmentation can be carried out by analyzing the likelihood of cancellation, timing of reservation, different channels, group discounts, purchasing size, delivery time and loyalty (Infineon, 2019). Another initiative in its conceptual stage at Infineon is the customer and product segmentation for the RM pilot. It is critical to identify which segment and which products as per past performance are most likely to be successful with RM. In addition to this, further attributes of RM include (Kimes & Wirtz, 2015; Chiang et al., 2006):

- *Relatively fixed capacity*

Typically, capacity refers to the physical attributes of businesses (such as fabs, for Infineon). It is vital to define what the capacity constraint is for the firm. For instance, a restaurant may have 100 seats, however, if it has a poor configuration of table sizes, a small kitchen unable to service 100 seats, or insufficient staff, the capacity constraint no longer remains the 200 seat inventory. Generally, capacity is fixed over the short-term, but certain businesses have some flexibility to be able to add additional short term capacity or reconfigure their capacity.

- *Perishable inventory*

Another critical characteristic of firms that are capable of adopting RM, is that their capacity (physical or non-physical) is perishable and cannot be stored for later use. This could be an

empty airline seat or in this case, Infineon's unallocated ATP products that run the risk of becoming obsolete. This represents foregone revenue that cannot be recovered.

- *Time-variable demand*

Customer demand includes the timing of demand and the duration of the customer experience. Demand by customers can vary depending on the time of year, day of week or time of day. Firms should be able to forecast such time-dependent demands so that they are able to establish an effective pricing mechanism and make allocation decisions. Time can be sold either explicitly or implicitly. An example of time sold explicitly is when customers pay by the minute, such as in spa treatments. With Infineon, the products themselves are the explicit sale, whereas time is sold implicitly in the form of order lead times. It is critical for customers in the supply chain to get their products on time, and prices can fluctuate depending on the order lead times. This is lead time-based pricing, where the pricing depends on lead time, and this is currently a key development focus for Infineon.

- *Varying customer price sensitivity*

The foundational environment to implement dynamic pricing is comparable to the one of revenue management, typically relating to the limited capacity and stochastic demand (Bitran & Caldentey, 2003). Furthermore, Talluri & Van Ryzin (2006) identify demand variability and uncertainty, customer heterogeneity, production inflexibility and data system infrastructure as some of the conditions for revenue management.

RM has only recently been discovered by the manufacturing industry and quite a few companies fulfil the prerequisites to successfully apply RM. Despite this, and the profit potential of RM, it is in a very initial stage in the manufacturing sector (Zatta, 2016). The above-discussed attributes are summarized below in Fig 10 along with a comparison of the presence of the attributes in the service industry and the manufacturing industry:

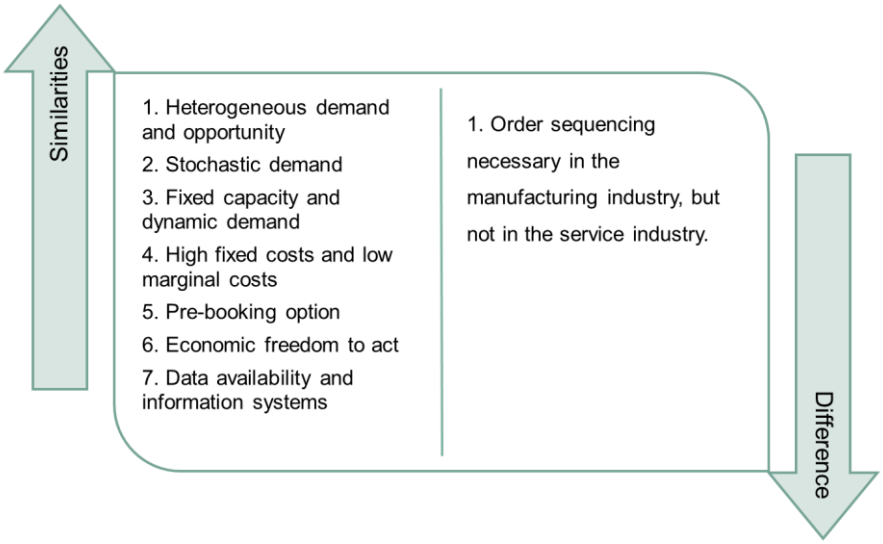


Fig 10: Similarities and differences in RM attributes in the manufacturing and service industries (adapted from Zatta, 2016)

For similarities, both the service and manufacturing sectors require that a service or product is booked or purchased in advance of consumption. This refers to the pre-booking option. Moreover, both industries have the economic freedom to act to withhold their services and products in order to make them available to future, more profitable customers without being

morally irresponsible or acting illegally. Lastly, while the service industry is booming in successful data management, information technology and system support, the manufacturing industry today has an equal potential to leverage data availability and information systems.

On the other hand, order sequencing is not required in the service industry because capacity is available in distinct periods and it expires at the beginning of a period. Orders are assigned specifically to individual periods. However, in the manufacturing industry, capacity is constantly available and constantly expires. Order deliveries take place at a particular point in time. Hence, order sequencing is necessary (Zatta, 2016).

Due to all the similarities between the service industry, which has successfully established and thrived with RM, and the manufacturing industry, it makes the latter an equally attractive industry to implement RM. Groundwork is required to identify the current barriers pertaining to customer acceptance as its applicability heavily depends on customer acceptance.

4.2 Secure Multi-Party Computation (MPC)

Presently, organizations depend on trusted third parties (TTP) to manage sensitive data, allowing for single points of failure with chances of grave consequences on data privacy and security. The dearth of technical solutions enforcing security and privacy guarantees leaves parties vulnerable while transacting (Roman & Vu, 2019). Organizational internal data is usually confidential and proprietary, wherein the disclosure of such data can prove detrimental to the organization. While organizations have the option to reveal this data selectively to agents entrusted with its analysis, it is often costly, risky if the data is not protected and requires that the organization strongly trust this TTP (Lapets, Volgushev, Bestavros, Jansen & Varia, 2016). MPC as an emerging technology overcomes this challenge and has the potential to compute aggregate data while safekeeping the privacy of organizations' confidential internal data (Roman & Vu, 2019).

MPC eliminates the need for a TTP (Sousa et al., 2017). Fundamentally, it involves two or more parties, wherein each party has their own secret input. On completion of the protocol via a joint function *f* that obtains its inputs from the secret data of each party, users only find out the final output of the function *f* and their own input, without any information about the other parties' inputs. Each party shares their input without reveal and hence, MPC is a viable option for building the foundation of decentralized privacy-preserving computational frameworks. The security of the protocol is interpreted with respect to the ideal model where the function *f* is computed by a trusted third party, T_f (Fig 11). The parties do not get information about others' inputs and T_f computes *f* after gathering inputs from the parties, sending the output back to them.

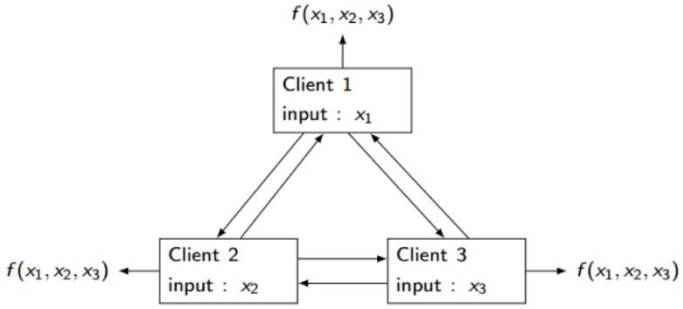


Fig 11: Computation with a trusted third party

Real-life examples for the application of MPC include the situation wherein patients wants to access their clinical records. They are able to make a query to the medical database of DNA related diseases by using their own private DNA code, while not wanting the hospital and others to know about their DNA and their potential disease. Simultaneously, the hospital would not want to reveal its database to the patients. Hence, where privacy is of utmost importance, MPC can solve the problem (Sousa et al., 2017). These applications are an extension to the original millionaire's problem, as described by Yao (1982). The problem involves two people - Alice and Bob, who want to find out who is richer among them without revealing to each other or to a trusted third party, information about their own money. The function computes the inputs and consequently outputs the name of the richer party. Eventually, they know Alice is richer, but have no information about the amount of money. This is an example of how the privacy of data is preserved. Other examples include secret voting. Though research on MPC technology and its applicability to real-life use cases is still growing, Sousa et al. (2017), test different MPC frameworks, compared on the basis of programming languages, techniques and the number of parties.

People are wary of giving access to their data to a third party, bearing the risk of the third party selling their data further or misusing the data. Contrarily, MPC allows such data to be shared in a secret, encrypted form while executing meaningful computations. The results of this are shared with the parties. By allowing computation without eliminating encryption, MPC is the first cryptography-based technology that allows multi-party data sharing and processing, guaranteeing that only data owners are permitted to access their data (Roman & Vu, 2019).

To ascertain whether a protocol is secure, researchers have established various security requirements (Zhao et al., 2019):

- Privacy: no party should be able to get information apart from their own
- Correctness: the output obtained by each party must be correct
- Independence of input: the input of a corrupted party must be independent of the inputs of the honest parties
- Guarantee of output: Corrupted parties should not be able to stop honest parties from receiving their own outputs.
- Fairness: Corrupted parties should obtain their outputs if and only if the honest parties obtain their own outputs.

For Infineon, this includes confidential ATP data, including production cycles data, end-user purchase patterns etc. On the other hand, for customers, it is the maximum price that they would be willing to pay for earlier deliveries. Parties remain anonymous to each other, meaning that the customers will neither know who else is using the platform, nor information about their data. As a solution, both parties engage in the MPC protocol to compute an earlier due date and the new, increased price based upon the unallocated ATP and the customer's price flexibility for earlier delivery dates. After the protocol, both parties shall learn the new date and an updated product price. Not only will it allow the manufacturer to securely expose their free ATP on a daily basis, but it will also offer customers a way to view and purchase from this inventory. In turn, this will help preserve existing customer-manufacturer relations. Customers will have the option to purchase more products and/or move forward their initially agreed upon delivery date (SafeDEED, 2018).

This research will use MPC in a black-box manner hereon and will not focus on the underlying technology that is MPC because there is sufficient ongoing theoretical research on the security and robustness of the technology. The focus would instead be on its visualization in the front-end and the variation of customer acceptance with its use. To the best of our knowledge, research has not yet been done to understand how an implementation using MPC can be visualized. It is critical to understand what customers look for while determining the technology's acceptance, as all the computation and processing takes place in the back-end, out of sight of the customer. Hence, incorporating usability while designing security systems is of utmost importance (Kainda et al., 2010). This research aims to visualize MPC with the use case of revenue management because MPC as a tool enhances computation and addresses privacy concerns.

4.3 Auctions

Different types of online auctions are often used in the business-to-business setting for manufacturers to sell to buyers. This section provides an overview of the different types of auctions, which help to outline the precise auction setting to integrate with RM for the use case. As RM uses unallocated ATP from the manufacturer, identifying the precise auction setting will allow the integration of dynamic pricing in a competitive environment where customers compete for products to be delivered on short notice. An auction setting for this research will enable access to the demand for goods in a timely and transparent manner. Auctions are a method for buying and selling goods through a bid system wherein the winning bid obtains the auctioned goods (Krishna, 2002). This sub-section allows us to identify a suitable auction setting that would be used for implementing revenue management where customers compete for earlier delivered products.

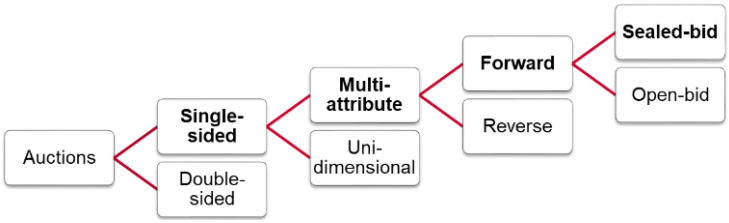


Fig 12: Classification of auctions based on bidding sides, bid composition, the role of participants and security

As illustrated in Fig 12, there are several auction types depending on different criteria:

Single-sided vs. double-sided

Conventionally, auctions include a seller for whom multiple buyers compete (Tarazona-Bermudez, G-Bustelo, Martínez, Alvarez & Rojas, 2014). One-sided auction protocols consist of a single seller or buyer accepting bids from multiple buyers or sellers. Contrarily, in double auctions, multiple buyers and sellers are allowed to bid for goods (Shi, 2013).

Multi-attribute vs. Uni-dimensional

The bids in uni-dimensional auctions comprise of only the price, whereas the bids in multi-attribute auctions consist of other attributes (Pla, López, Murillo & Maudet, 2014). Multi-attribute auctions enable the consideration of attributes other than prices, such as delivery time or quantity. This is useful for many industries for whom focusing on delivery times is as important as price (Torrent-Fontbona, Pla & López, 2015). In the B2B sector, there are several other important attributes apart from the price that must be considered for decision making.

The field of multi-attribute auctions is gaining greater interest in the scientific community as well as from software vendors of electronic business products (Burmeister, Ihde, Kittsteiner, Moldovanu & Nikutta, 2002). Reasonably, comparing bids and reaching the result is cumbersome in multi-attribute auctions in comparison to uni-dimensional auctions where the lowest or highest price directly wins. Whereas in multi-attribute auctions, a combination of multiple variables has to be considered to identify which bid fits the auctioneer's requirements. Similarly, for bidders too, it is not an easy task to bid in a multi-attribute auction. The bidder must adapt their bid to the attributes and possible valuations of attributes, in order to beat the leading bid (Burmeister et al., 2002). Commercial approaches for analyzing multi-attribute bids include the weighted-sum approach where parameters or attributes of the goods are associated with a numerical or non-numerical weight. Then, the best bid is one with the best value for the overall weighted sum. The second approach is the total-cost approach where all the attributes have monetary values or can be associated with some monetary value. The bid with the best total cost wins. This approach is applicable when monetary values are easily attachable to attributes, or the calculation of monetary values is not complex. Burmerister et al. (2002) lay out a practical approach to multi-attribute auctions, including bidding and evaluation. Infineon is yet to finalize if auctions are the best method to visualize and implement RM. However, it is a starting point for understanding the potential implementation of RM. Therefore, at this initial stage, there would be no algorithm at play to weigh the multi-attribute bids. Rather, the outcome would be a realistic but random multi-attribute outcome. The weighing, in reality, would largely depend on lead time-based pricing, which is also yet to be developed.

Forward vs. Reverse
In forward auctions, the auctioneer sells goods or services and the bidders compete for them. In reverse auctions, the auctioneer is the buyer and the bidders compete to sell their services.

Sealed-bid vs. Open-bid
Security remains one of the biggest issues of online auction protocol (Shi, 2013). A sealed-bid multi-attribute auction protocol focusses on dealing with security issues including bid privacy, bidder anonymity and fairness problem. Privacy can be classified into bid privacy and bidder anonymity. Bid privacy involves making the winning bid public, while the losing bids must not be revealed. Bidder anonymity ensures that the identities of the bidders are protected. Secure MPC has been used to overcome the fairness problem of online auctions (Shi, 2013). Bidders are aware of other people's bids in open-bid auctions, whereas participant's bids are not revealed to the others in sealed-bid auctions. The two-attribute A+B auction (also called cost/time auctions) is a sealed bid procurement auction, where bidding occurs based on the cost which is the bidder's cost (A) and the time to deliver (B) (Pham, Teich, Wallenius & Wallenius, 2015).

Omote & Miyaji (2001) discuss the security requirements for auctions as follows:

1. Anonymity: nobody should be able to identify a bidder
2. Traceability: the winning bidder should be identifiable after the procedure
3. No framing: impersonation of a bidder must not be possible
4. Unforgeability: no one should be able to falsify a valid bid
5. Fairness: bids should be dealt with fairness

6. Verifiability: anyone can verify a signature and confirm whether bids are valid or not
7. Unlinkability among different actions: no one can link the same bidder's bids through different rounds of the auction

Auction setting for this research

Bogetoft et al. (2006) research a case of double auctions with multiple sellers and buyers, emulating the auctioneer via multi-party computation instead of trusted third parties to ensure the trustworthiness of the auctioneer. They establish the criteria for defining an ideal functionality, synonymous to an incorruptible computer as follows:

- Confidentially: obtain a set of integers from each input party
- Execution: The built-in program may use standard integer arithmetic comparisons and operations
- Output: Direct the outputs of the program to the parties

E-commerce eases supply chain management and inventory management, which directly influences the firm's performance, especially cost reduction. However, this electronic integration demands significant levels of trust between information systems and the participants of multiple organizations. It is important to pay attention to the pricing mechanism as long-term relationships between buyers and suppliers can otherwise be damaged. To overcome this, recent auction mechanisms suggest taking non-prices attributes into consideration, such as quality, delivery and payment terms. It is also important to incentivize losing bidders to sustain the business relationship (Pham et al., 2015).

Concepts of usability and user experience into the development of online auctions also play a vital role in its success (Tarazona-Bermudez et al., 2014). The benefits for buyers include transacting with a supplier directly for targeted products without any intermediaries, accessing thousands of products in an agile and dynamic way, relying on a transparent and dependable tool for transacting and connecting suppliers with the buyers offering the best price.

Teich, Wallenius, Wallenius, & Koppius (2004), present a classification of auction situations based on 18 criteria. The first four are about the nature and number of goods to be auctioned, 5-14 concern the auction rules and format and 15-18 relate to the nature and composition of bids:

1. Number of items of a good/service auctioned
2. Number of goods/services auctioned
3. Nature of goods/services (homogenous, heterogeneous)
4. Number of attributes
5. Type of auction (forward, reverse)
6. Nature of auction (one-round, progressive)
7. English vs. Dutch auction (ascending vs. descending price)
8. Who can participate (by invitation, open to anybody)
9. Are agents used or not
10. Price paid by winner (first price, second price)
11. Is price discrimination applied (yes, no)
12. Do constraints exist (explicitly, implicitly)
13. Is there a follow-up negotiation?
14. Is a value function elicited for the buyer?

15. What is the nature of bids (open cry, semi-sealed, sealed)
16. Dimensionality of the bid vector (1,2, n-dimensional)
17. Are bids divisible?
18. Are bundle bids allowed?

The auction setting we adopt is outlined in the Conclusions section of this chapter. We use this overview of auctions for the design requirements of the artefacts in Chapter 5.

4.4 Human-Computer Interaction and Security (HCISec)

Usability is perhaps one of the most significant social topics and challenges within the field of cybersecurity (Nurse, Creese, Goldsmith & Lamberts, 2011). It is vital to incorporate human and social elements of design, along with security. Essentially, the objective of security is to make undesirable actions more difficult and conversely, the objective of usability is to make desirable actions easier for the user. Following this concept, a *usable* system will reduce unintentional errors, whereas a *secure* system will guarantee that undesirable actions through the system are mitigated. There are limited studies that include usability and user interaction in security technologies, where both human-computer interaction (HCI) and security communities ignore this problem (Smith, 2003; Yee, 2002). Often, security and usability are seen as two clashing notions, where researchers believe that improving one of them affects the other negatively (Kainda et al., 2010). The underlying reason for this belief is that system implementers deal with security and usability as add-ons to a completed product. It is important that the security community incorporates key HCI thinking about people-centred design.

Gunson et al. (2011) have proven the imperative trade-off required between usability and security. At the same time, security and usability go hand-in-hand and it is crucial to consider both these factors while designing and evaluating a system. In order to improve the usability of secure systems, the need for human-computer interaction and security (HCISec) arises. This necessity encourages the research community to re-analyze the design and implementation of secure systems. Nevertheless, despite the efforts put into this knowledge gap, Kainda et al. (2010) elaborate on the fact that there are considerable examples of secure systems being designed while neglecting the importance of usability.

Firstly, a system is secure if users can depend on it and its software behaves as expected (Garfinkel, Spafford & Schwartz, 2003). Generally, security relates to a negative perception of users towards possible attackers, or agents with malicious intent instead of the legitimate use of a system (Kainda et al., 2010). Moreover, security remains a practical problem where users question whether the system in front of them is secure enough for what they want it to do (Dourish, 2004). On the other hand, usability research of secure systems centres on usability elements only. Kainda et al. (2010) elaborate that all the studies they reviewed, discussed “usability analysis” extensively, whereas, in reality, a thorough evaluation must also consider factors that may affect security. Principally, usability can be defined differently, varying with the context. At times, efficiency may be the priority, whereas learnability or flexibility may be equally important. In the context of secure systems, usability priorities must be the requirements such that the security can be used effectively (Whitten & Tygar, 1999). Eventually, the user requires a system that is both, usable and secure.

Additionally, Whitten & Tygar (1999) question the lack of good user interface design for security. User interfaces for secure systems seem to be confusing, clumsy or near-nonexistent. Although secure systems may have attractive graphical user interfaces, user interface design for effective security remains a challenge. It is a pressing need to make security understandable for novice users. Cryptographic implementations fail because users are unable to understand security-relevant user interfaces as the reality does not match the mental model that the system designers initially had (Smith, 2003). Moreover, the human factor is discussed to be the weakest part of a security system (Patrick, Long & Flinn, 2003). Consequently, the designers and developers of secure systems face a serious challenge, such that if a security system is not user-friendly, developers undergo failure in the marketplace or users who avoid or neglect the security features. Even though it frequently seems that security and usability are contradictory system attributes, it need not be that way. Following these issues, security poses a challenging domain for user interface design. Nonetheless, time and effort invested in designing and considerably enhancing the graphical user interface make the notion of complex cryptography manageable for novice computer users (Whitten & Tygar, 1999).

Primarily, security is seen as a secondary goal while designing a system (Whitten & Tygar, 1999). It is simple for users to neglect learning about security, or optimistically presume that their security is functioning correctly while they concentrate on their main objectives. Consequently, designers of user interfaces for security must not presume that users will be interested to read manuals or look for security controls that are designed to be unobtrusive. If security is too challenging or frustrating, users may give up on it completely. Secondly, the necessity of preventing hazardous errors makes it vital to provide adequate feedback to the users. However, providing such feedback for security management is challenging because the state of a security configuration is typically complex and efforts to condense it are not enough. Next, user interface design for security must give high importance to ensuring that users understand the security adequately, to prevent them from performing potentially expensive errors. This is crucial because once a secret is left unprotected by chance, there is no way of ensuring that it has not been accessed by an attacker.

Then, it is important to understand how users perceive and trust security systems. The best predictor of judging users' trustworthiness in an online secure environment is the quality of the website's visual presentation (Turner, 2002). Trust in such settings represents how much faith users have in the software, and implicitly, the owner of the software (Whitten & Tygar, 1999). Moreover, the identity of secure systems relates to whether a user is able to identify a system to be secure or otherwise. Hence, the security of a system is determined by the information conveyed through the user interface, among other things (Yee, 2002). Graphical representation of locks and keys are heavily used while depicting cryptographic technology. The graphical label of the lock signifies encryption, with an icon that looks like a closed padlock (Kainda et al., 2010; Whitten & Tygar, 1999). Even for untrained, novice users, such symbols are straightforward visual metaphors that facilitate in understanding security concepts intuitively. Users are on the lookout for indicators that grab their attention to the security of the system. However, tasks revolving around security must not require undivided attention from users because this is probable to cause frustration (Kainda et al., 2010).

Furthermore, the use of prompt messages is helpful to warn users about permanent actions. However, information regarding an action's result must be communicated neutrally, without

passing judgement about the action and without interrupting the user's workflow. The use of prompt warnings too often may decrease the users' trust in such admonitions, reducing their effectiveness in crucial situations when required. Therefore, such prompts should aim to inform the user, instead of interrupting (Yee, 2004). The goal of designing user interfaces for security is to ensure that inexperienced (with respect to cryptography) users can understand and use the basics while preventing any confusion and frustration that can lead them to use the system incorrectly or not at all. Some users also believe that the security and encryption element is supposed to be transparent (Whitten & Tygar, 1999). At the same time, Dourish (2004) argues that transparency can make the situation worse because users can find it difficult to see things that are transparent.

Comprehensively, security software is usable, provided that the people who are likely to use it:

- are reliably informed about the security tasks they must execute
- are able to comprehend how to successfully execute these tasks
- do not make hazardous errors
- are adequately comfortable with the interface to carry on using it

Frequently, usability factors are considered to trade-off against security and vice versa. Following this notion, designers assume that enhancing security, degrades usability. Therefore, the choice of favouring one or the other is seen as an unfortunate compromise. However, Yee (2002) discusses that usability and security goals seldom need to be at odds with each other. To summarize the importance of user interaction in security, Yee (2002) establishes design principles for such systems. In order to have confidence in using the system safely, users must have confidence in the following statements:

Table 1: Design principles that positively influence user feelings

Design Principles	User feelings
Explicit authority	Things do not become unsafe by themselves
Visibility	I can know whether things are safe
Revocability	I can make things safer
Path of least resistance	I do not choose to make things unsafe
Expected ability	I am aware of what the system can do for me
Appropriate boundaries	The system can safely do what I want
Expressiveness	I can tell the system what I want
Clarity	I am aware of what I am telling the system to do
Identifiability, trusted path	The system protects me from being fooled

Concisely, usability and security cannot simply be added-on to products, instead, they need to be incorporated throughout the entire design process (Yee, 2004). Once usability and security goals are not treated as add-ons, they can be designed together in order to prevent conflicts. For instance, if designers attempt to add-on security instead of designing it into a system from the first stage, among other things, usability suffers. Both of them contribute to the overall big picture of fulfilling user expectations. Good usability engineering demands understanding user requirements and incorporating the applicable features throughout the design process, instead of bolting on superficial features such as flashy widgets or skins at the end. Not only is it vital to identify these challenges early on, but it is equally important to

design the user interface and security measures together (Yee, 2004). Security and usability goals can be aligned by extracting and using as much accurate information as possible from a user's usual interaction with the interface.

Yee (2004) convinces designers that significant improvements can be reached by designing usability and security together. Hence, further research on evaluating usability in the context of security is valuable, as it is important to communicate a precise model of the security to users. Furthermore, it is idealistic and impractical to expect to attain maximum usability and security in secure systems. Generally, such systems require a trade-off between security and usability (Kainda et al., 2010).

4.5 Platforms and Consumer Acceptance

The application of big data, new algorithms and cloud computing are rapidly changing the nature of work and the structure of the economy. However, the exact nature of this change is determined by the social, political and business choices. While a digital platform economy is emerging, digital platforms are a complex research topic due to their distributed nature and their connection with markets, technologies and institutions. The deployment of algorithms to the cloud where they are easily accessible creates room for the infrastructure on which entire platform-based markets and ecosystems operate.

As MPC is still a very new technology yet to be practically developed and RM a new initiative in the semiconductor industry, it is vital to understand the technology's acceptance before implementing them. Predicting system use is an interest of many researchers to understand the reasons for the failure of adoption. While user acceptance of technology has been studied extensively, the Technology Acceptance Model (TAM) has been one which has captured the most attention of the Information Systems community. According to TAM, perceived usefulness and ease of use are posited as key drivers of consumers' intention to use (Davis, 1985). However, other vital intangible specifics such as trust in platform providers also play a role in the overall attractiveness of a digital platform (Reuver et al., 2017). Customers frequently hesitate in transacting with web-based vendors due to the uncertainty about vendor behaviour (Mcknight, Choudhury & Kacmar, 2002). Building trust allows customers to feel more comfortable with sharing personal data, placing orders, transacting and acting on the web.

Importance of trust and security between businesses and customers

Mayer, Davis & Schoorman (1995) propose a holistic definition of trust as "the willingness of a party (trustor) to be vulnerable to the actions of another party (trustee) based on the expectation that the other (trustee) will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party (trustee)". Trust is found to dynamically evolve with time and consists of multiple dimensions (competence, benevolence and integrity), rather than being unitary in nature. To facilitate building trust on both sides of an online platform, platforms could allow anonymous reciprocal reviewing (buyers and sellers review each other), let users share anonymous ratings and allow honesty from both ends without fearing retaliation (Luca, 2016). As gaining trust is important for web-based businesses, one way for sellers to do this is by depending on their website features to prove to customers their trustworthiness. The dynamics of trust would also keep changing with time as the customer becomes more experienced (Kim & Ahn, 2007).

While past studies consider trust to be three-dimensional as discussed above, in a transaction-relevant setting, trust is regarded as the perceived benevolence and integrity of a party taking part in the transaction (Kim & Ahn, 2007). Perceived benevolence is the degree to which one party is genuinely interested in the other party's welfare and its motivation to seek joint gain. On the other hand, integrity within an e-commerce setting pertains to the completion of online transactions, customer service policies that follow a transaction and the firm's use of customer's private data. Furthermore, the company's perceived reputation, willingness to customize products and services, perceived website usefulness, ease of use and security control can considerably influence trust (Kim & Ahn, 2007). Web usability involves the principles of website design comprising of the interface consistency, response time and interacting style. Aspects of web usability include ease of use, searching function and site navigational structure. A well-designed website becomes one of the company's competences, allowing customers to believe that the company has the capabilities to keep their promises. Therefore, a well-designed website which is user-friendly and useful needs particular capabilities and resources of the company (Kim & Ahn, 2007).

Trust in an online setting is built through (1) a belief that the vendor has nothing to gain by cheating, (2) a belief that there are safety mechanisms built in to the website, (3) by having a typical interface (4) one that is furthermore, easy to use (Gefen et al., 2003). Furthermore, trust in online settings represents how much faith users have in the system/software, and implicitly, the owner of the software (Whitten & Tygar, 1999). Therefore, we consider trust to compose of institutional trust as well as transactional trust. Institutional trust is explained as the choice of a party to depend on another party under conditions of risk (March and Shapira 1987; Sitkin and Pablo 1992). In this case, users allow their fate to be decided by the manufacturer and undertake the risk that they may experience unfavourable outcomes (such as loss) in case the manufacturer proves untrustworthy. On the other hand, transactional trust is built incrementally over time and consists of contractual trust, communication trust and competence trust. Contractual trust relates to the trust of character, communication trust is about the trust of disclosure and competence trust is the trust of capability. In an online setting, both, institutional and transactional trust come in to play, where users trusting a system also implicitly relates to them trusting the manufacturer (or the owner of the system) (Reina & Reina, 2008).

Simultaneously, customers are concerned about how secure their transactions are on the web. They expect for the company's website to provide the infrastructure required for secure exchanges of data. They perceive that security control positively plays a role in building trust as it lowers the customers' risk in transacting (Gefen, Karahanna, & Straub, 2003). Online, customers are affected by their trust in the seller and the features of the website interface. An e-vendor is more than a platform interface, it is indeed a business entity with whom customers economically engage. Trust is essential in such transactional, buyer-seller relationships, especially when there is an element of risk involved, including transacting with an e-vendor. For experienced consumers, the intention to transact with the previous seller from whom they purchased is subject to their trust, perceived usefulness and perceived ease of use. The authors elaborate that trust in an online setting depends on people's belief in the safety mechanisms built into the website as well as an easy-to-use interface. An increase in trust boosts the perceived usefulness of the website. Furthermore, the intention to use is greatly predicted by perceived usefulness. Gefen et al. (2003) demonstrate the importance of trust

along with the previously well-established factors that are perceived usefulness and perceived ease of use.

Extending this knowledge, Lapets et al. (2016) discuss the design and deployment of a secure multi-party computation protocol web-application without the need of organizations trusting third parties with their sensitive data. While emphasizing the importance of usability requirements, they explain that a secure multi-party computation is only valuable if multiple parties are able to trust it and use it. Additionally, attributes that such a protocol must have, are defined as follows:

1. Comprehensibility: The secure MPC protocol must be simple for users to comprehend in order to stimulate adoption.
2. Auditability: To build trust, the web service must be completely transparent, with an open-source code to allow external audits. Moreover, the protocol must never share sensitive data with the service, not even the aggregate final output of the computation.
3. Accessibility: To reduce the complexity that might hinder participation, the software must be rapidly and easily deployable, requiring no extra setup, specialized software and hardware.
4. Simplicity: The service must be usable within a relatively narrow time frame by non-expert parties, whose technical expertise might only comprise of basic knowledge of spreadsheet applications and web browsing clients.
5. Idempotence: parties should be able to resubmit (update) their data, should they find it to be corrupted.
6. Feedback: As incorrect or malformed data from parties ruin the aggregate value of the computation, the web interface should proactively warn users about spurious data.

Technology Acceptance Models

Understanding factors that influence the acceptance of a B2B platform is core to this research. Some research models from the literature are presented below, which will form the base for the research model of this research.

To begin with, behavioural intention to use is explained by subjective norms, perceived behavioural control and perceived usefulness, and actual use is directly predicted by behavioural intention to use (Fig 13) (Gumussoy & Calisir, 2009).

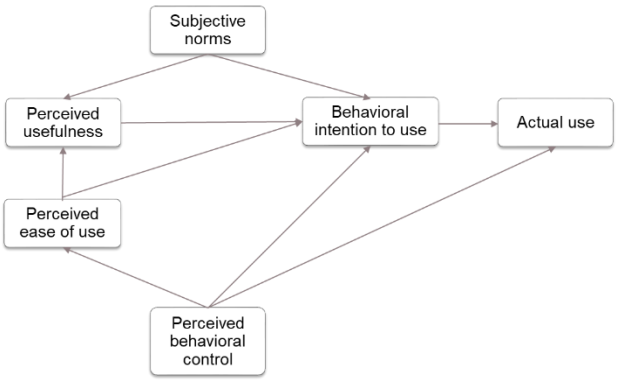


Fig 13: Research model (adapted from Gumussoy & Calisir, 2009)

Gefen et al. (2003) have further demonstrated the importance of trust along with perceived usefulness and perceived ease of use (Fig 14).

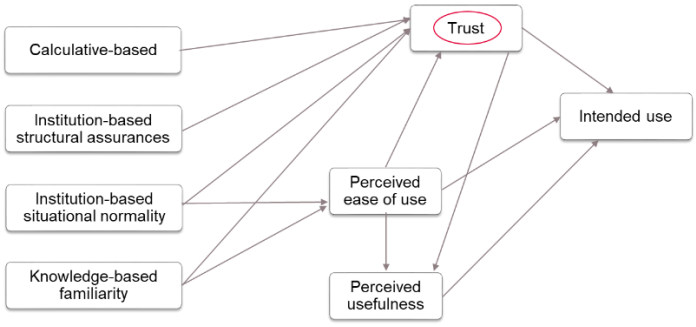


Fig 14: Research model (adapted from Gefen et al., 2003)

Lai (2016) extends the model to emphasize the significance of security and design on consumer's intention to use a platform and engage in payments (Fig 15).

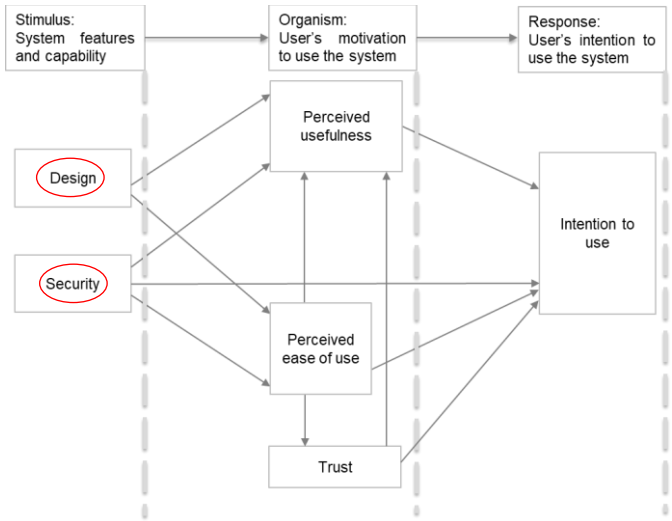


Fig 15: Research model (adapted from Lai, 2016)

Past studies have proven that online purchase intentions result from consumer assessments of the IT artefact itself, specifically its perceived usefulness and ease of use, as well as trust in the e-vendor (Gefen et al., 2003). Similarly, Lai (2016) explains that design and security are the stimuli that represent the system and feature capabilities, while the perceived usefulness and the perceived ease of use only represent the organism, signifying the motivation to use the system. Both of these are equally important to understanding customers' intention to use. However, these perspectives have so far been examined independently by IS researchers. Integrating these three perspectives (1. Perceived usefulness and perceived ease of use, 2. Trust, 3. Design and Security) and understanding the factors that can build online trust in a setting that lacks the classic human interaction that frequently builds trust in other environments, motivates us to develop an understanding of these concepts and their linkages to customer behaviour. Customer trust, design and security are an equally important part of understanding customer acceptance as the widely used TAM concepts - perceived usefulness and perceived ease of use (Gefen et al., 2003; Lai, 2016). Therefore, understanding these concepts will also greatly influence the acceptance of the RM platform:

Behavioural intention is a degree of likelihood that a person will get involved in a particular behaviour and it encompasses motivational factors that affect behaviour. Such factors are a measure of how much effort people intend to exert and how hard they intend to try to perform the behaviour. To begin with, users intend to use a new technology and only then actually use

it. Hence, behavioural intention to use becomes the direct predictor of actual use, as also proven by multiple studies (Gumussoy & Calisir, 2009).

Perceived usefulness is the extent to which a person presumes that using a specific system would improve his or her performance. Behavioural intention to use is largely influenced by perceived usefulness, more so for those who have high levels of internet experience (Gumussoy & Calisir, 2009).

Perceives ease of use is the extent to which a person presumes that using a specific system would be free of effort. Perceived ease of use is then a major secondary predictor of people's intention to use a system. People want to reduce the effort required in their behaviour. If using an auction technology demands high effort and is time-consuming, the buyer might not begin to use or give up using the system (Gumussoy & Calisir, 2009).

The relationship between perceived usefulness and perceived ease of use is described as follows: all things equal, the easier a system is to sue, the more useful it can be. Provided using the technology is easy, potential users would not have to spend a lot of time learning how to use it, this might affect the user's performance.

Security is defined as the state of feeling safe or protected from harm (Lai, 2016). It can be further divided into the dimensions of reliability, safety and privacy. It is seen that consumers associate trust with security, including positive word-of-mouth recommendations, reputation information, brand equity, consumers' experience-based knowledge of security aspects and risk management (Lai, 2016).

Design can be defined as the technical design and functionality (Lai, 2016) (of RM and MPC in this study) of novelty that is in line with the adaption to customers' capabilities of using such a platform for placing orders. It has been shown that consumers value the advantages of the design that provide ease of use and usefulness (Lin & Hsieh, 2006; Lai & Zainal, 2014). Sztmanski & Hise (2000) show that the easier the design of a site for online navigation that led to purchasing and e-payment, the higher the attraction of customers towards using the online site.

In this chapter, we have discussed the applicability of revenue management to the manufacturing industry in comparison to the service industry. Next, we considered the basic functionality of multi-party computation, explaining how it eliminates the need for a trusted third party and its applicability to real-life situations. Furthermore, we discussed auctions, which enable us to identify a suitable auction in order to implement revenue management. We then explain the challenges in the fields of human-computer interaction and security, while emphasizing the importance of considering usability and security, both, while designing, developing and evaluating security systems. Lastly, we discuss in detail the usability factors that play a vital role while assessing the acceptance of new technologies through well-established technology acceptance models. Incorporating fundamentals from the fields of revenue management, multi-party computation, auctions, human-computer interaction and security as well as technology acceptance, we discuss the artefacts that are designed in this research, in the next chapter. The above-discussed concepts present the foundation for designing and evaluating these artefacts.

4.6 Conclusions

Concisely, incorporating usability and security together remain a challenge in the field of human-computer interaction and security (HCISec). Bridging this conceptual and application gap is crucial while emphasizing the need to integrate these two concepts in order to design and develop usable security interfaces and systems. Incorporating usability and security in the development of systems is context-dependent. In this research, we apply these to the cryptography technology of multi-party computation, being applied to the use case of revenue management.

Neglecting usability of security systems leads to confusion, frustration and clumsiness on the users' side, that hampers instead of facilitating tasks. Furthermore, the rising complexity of security systems significantly hampers the usability of such systems. These challenges stem from the overuse of technical terminology, confusing or unclear functionality, the lack of visible system statuses and the lack of integration of security and usability (Nurse et al., 2011). Researchers emphasize the need for working towards improving the performance of online security systems through effective visualization. Communicating cryptographic technology precisely to users is important for their success (Smith, 2003). To facilitate the communication, symbols such as a padlock are often used to depict cryptographic technology (Dourish, 2004; Kainda et al., 2010; Whitten & Tygar, 1999; Yee, 2004). Furthermore, users value transparency in the security system, in addition to receiving prompts to warn them about permanent actions.

We integrate usability factors (trust, security, perceived ease of use, perceived usefulness and intention to use) for our research model based on the technology acceptance models established by Gumussoy & Calisir (2009); Gefen et al. (2003); Lai (2016). Subsequently, this research integrates trust, security and design along with perceived usefulness and perceived ease of use, as per the original TAM by Davis (1985). This is seen below in Fig 16. This model guides the generation of the parameters to evaluate the designed artefacts, namely, (1) Trust, (2) Perceived ease of use, (3) Perceived Usefulness, (4) Security and (5) Intention to use.

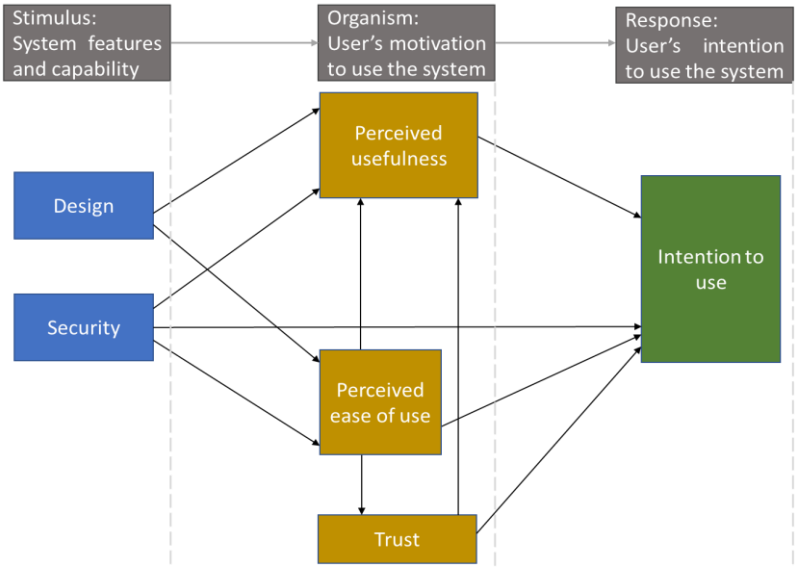


Fig 16: Research Model

With regards to MPC, we establish that privacy is crucial, where no party should be able to get information apart from their own (Zhao et al., 2019). Confidentiality is also important and the protocol must obtain a set of data from each input party (Bogetoft et al., 2006). Furthermore, anonymity is vital and nobody should be able to identify a bidder (Omote & Miyaji, 2001). Then, the MPC protocol executes computation via a built-in program that may use standard arithmetic comparisons and operations to generate an outcome. The output of the program can be configured and directed to the involved parties (Bogetoft et al., 2006). Comprehensibility is another facet of a well-designed MPC protocol, where it must be simple for new users to comprehend (Lapets et al., 2016). It should be simple so that the service is usable in a relatively narrow time frame by novice parties. The requirement of idempotence requires that parties can resubmit or update their data, should they find it to be corrupted. Moreover, in order to decrease the complexity that can hamper participation in the system, the protocol must be rapidly and easily deployable, requiring no extra set up.

We also identify the auction best suited to implement revenue management would be a single-sided, multi-attribute, forward, sealed-bid auction (Burmerister et al., 2002; Pla et al., 2014; Shi, 2013; Torrent-Fontbona et al., 2015). It must be single-sided as Infineon is the supplier and distributors the buyers. It would be multi-attribute because distributors bid through price, quantity and delivery dates, instead of price, individually. As Infineon as the manufacturer would sell to several potential distributors who compete for the products, this would be a forward auction. Lastly, it is sealed-bid because the bids are confidential for the distributors and it is crucial that these bids are not revealed to the others. We further identify the importance of usability and user experience in online auctions, where auctions are valuable for users as they allow users to transact directly with the manufacturer and are a transparent and dependable tool for transacting (Tarazona-Bermudez et al., 2014).

In addition to our literature review and the model in Fig 16, we use the existing buying platform and the processes, part of the Relevance cycle that was discussed in the previous chapter. The importance of the Rigour cycle is to inform the research project about past knowledge, so as to ensure its novelty and innovation. Hevner et al. (2004) describe that it is the researcher's accountability to thoroughly research the existing knowledge base in order to ensure that the designs produced and proposed are vital research contributions and not routine designs built upon the application of well-known processes. Therefore, it is the rigour of designing IT artefacts that differentiates Information Systems as design science from merely the practice of building IT artefacts. The rigour of our research is predicated on the skilled selection and application of the appropriate methods for developing and evaluating the artefacts. Moreover, additions to the knowledge base on the basis of DSR include any extensions to the original methods, theories or models made during the research, novel artefacts and the experience gained from applying the research to a field setting (Hevner, 2007). Consequently, through our research, we design, evaluate and proposes novel artefacts that offer a potential visual implementation of the integration of RM with MPC and establishes the unique applicability of MPC to the use case of RM. We evaluate the artefacts against users' trust and perceptions of security, perceived usefulness, perceived ease of use and intention to use.

5. Artefact Design (Design Cycle)

This section discusses the artefacts that are developed through this research. The requirements for designing and developing these, include identifying the functionality and the applicability of using MPC for RM, understanding the current buying platform, as well as the literature review.

The internal design cycle is certainly the core of any design science project. This stage involves the development of an artefact, its evaluation, and subsequent feedback to inform the design further. Moreover, it is vital to recognize the dependencies of the Design cycle on the Relevance and Rigour cycles while also valuing its relative independence during the actual execution of the research. Fundamentally, design is characteristically an incremental and iterative activity with no distinct stopping rules. A design artefact is effective and ready once it satisfies the necessities and limitations of the challenge it was meant to solve or simplify (Hevner et al., 2004). Due to the time limitations of this thesis, we are unable to perform multiple iterations of the design cycle.

With knowledge of the current buying platform, the order management processes, usability features, MPC, RM and the researcher's creativity, the four artefacts are designed. Before applying the above knowledge from the Relevance and Rigour cycles towards designing the artefacts, we establish the applicability of MPC to the real-life use case of RM. In such situations where there is insufficient literature in the field, the search is for satisfactory solutions, satisficing instead of explicitly specifying all the possible solutions. Hence, the design task includes the creation, utilization and assessment of heuristic search strategies implying the construction of an artefact that works well enough for the identified class of problems. In our case, the identified class of problem is the lack of understanding about how the implementation of MPC and RM would look, communicating this integration, as well as understanding customer's acceptance of such an interface.

In order to produce beautiful designs, analytical skills are required in combination with the talent of a creative artist. Besides a thorough grounding in mathematics, attributes of a good designer include taste, good judgement, brains, aesthetic gifts and sheer intellectual aggressiveness (Gelernter, 1989, p. 9). Simon (1996) has also emphasized the significance of style in the design process, expressing that the ability to creatively differ the design process within the bounds of satisfactory constraints, adds value and challenges designers participating in the process.

While paper-based prototyping would have been a simpler and faster way to design the mock-ups, we were motivated to maintain a high quality and keep the mock-ups as realistic as possible despite being a non-programmer. Therefore, we deemed it essential to learn and execute C# codes to design and develop all the artefacts. Additionally, though there are four artefacts in total, only three are used for evaluation because the first artefact demonstrates the functioning of the current buying platform. This artefact is only used to demonstrate to the participants how to run and work around the mock-ups.

5.1 Developing the functionality of MPC in the use case

Lead time-based pricing (LTBP) is highly relevant for manufacturing industries today, as earlier order delivery date requests present an added value for customers, which is already provided by several manufacturers today (including Infineon) at no additional costs for the customer. However, LTBP is dependent upon customers' willingness to pay (Garcia, 2018). Furthermore, it is challenging to fathom how the integration of RM and MPC looks like, due to the limited literature in terms of applicability in both these fields, as well as how customers perceive these. Consequently, the mock-ups in this research present the opportunity for visualizing pricing variations based on the order lead time. As customers value earlier delivery dates (than their contractually agreed delivery date), they are willing to pay a premium price for a shorter order lead time. Provided the supplier is able to deliver the orders earlier, according to the wish date of the customer (which happens often as depicted by real data in Fig 5), it presents the potential to apply lead time-based pricing. The LTBP algorithm behind such a platform is out of the scope of this research because it is still under development at the ideation stage as one of Infineon's project initiatives (Fig 2).

By extending our knowledge of the case's context and the literature review, as well as through initial discussions with Infineon and leaders of Work Package 5 from the SafeDEED consortium (SafeDEED, 2018) we establish the applicability of MPC to RM. Moreover, this development contributes to building the functionality of the MPC algorithm for this use case under the SafeDEED project. The applicability is explained as follows:

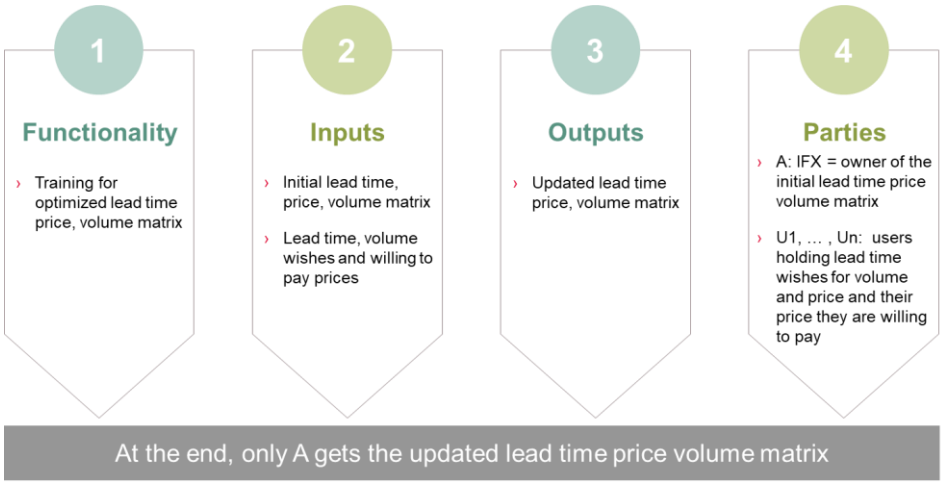


Fig 17: The functionality, inputs, outputs and parties involved in MPC with RM

The functionality to be attained by applying MPC as a tool for RM is to train the algorithm to optimize the lead time price and volume matrix. Through this, the computation will be able to identify the best bid for the manufacturer. Next, the inputs for the MPC algorithm are the initial lead time price and volume matrix from the manufacturer as well as the lead time, volume and price wishes from customers. Consequently, the output of the algorithm will provide an updated lead time price and volume. The parties involved in the computation are the manufacturer, who is the owner of the initial lead time price and volume matrix, as well as the customers who provide the lead time wishes regarding the volume and the price they are willing to pay. At the end of the computation, the manufacturer will obtain the updated lead time price and volume matrix.

To further explain how RM can be potentially implemented with, and without using MPC, we identify the following settings:

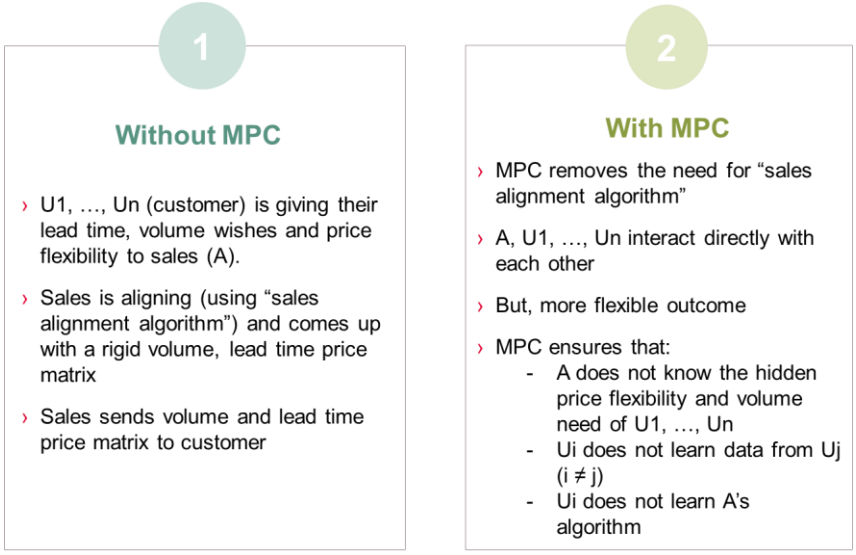


Fig 18: RM setting with and without using MPC

In the scenario where MPC is not used, the customers will provide their lead time, volume and price wishes to the Sales Department of the manufacturer. Sales will then align these requests using the sales alignment algorithm and produce a rigid volume, lead time and price matrix. As a final step, Sales will send the volume, lead time and price matrix back to the customers.

On the other hand, this process is simplified by using MPC. It removes the need for the sales alignment algorithm. Conversely, now, the customers would be interacting with each other to obtain a more flexible outcome via the computation. Not only will MPC ensure that the manufacturer does not obtain the confidential price flexibility and volume needs of all the customers, but also that customers do not learn each other's' data, while also promising to keep the manufacturer's LTBP algorithm confidential.

Identifying these scenarios (Fig 17and Fig 18) guide the main input interface of the mock-ups, where the users' inputs must include their wished lead time, price and volume. The MPC algorithm (which is not yet developed) will proceed with its computation based on these user inputs as well as the unallocated ATP information provided by the manufacturer. In this manner, everyone's data is kept confidentially without entrusting a third party service.

5.2 Design Requirements

A comprehensive summary of the requirements that guide the design of the artefacts can be seen in Table 2. The design requirements stem from the Rigour and Relevance cycles, by incorporating the attributes covering the fields of RM, MPC, auctions and user experience. The three artefacts are designed in a manner such that the individual effect of text, encrypted visuals and transparent visuals can be evaluated independently. They are designed with such variations so as to understand whether text, visuals, or a combination of both, are best communicated to the customers along with understanding the reasons behind these. The evaluation of the artefacts facilitates understanding the underlying usability factors (trust, security, perceived ease of use, perceived usefulness and intention to use) for their choices, which in turn would drive acceptance.

To begin with, after defining the applicability of multi-party computation to the use case of revenue management, we establish that the inputs required from customers for are their wished lead times, the prices they are willing to pay and the desired products' volume. We represent this by the customers' input grid on the left-hand side panel of the potential platform mock-ups and this remains constant for all three mock-ups. Furthermore, we identify the auction setting suitable for visualizing RM. This is the single-sided, multi-attribute, forward, sealed-bid auction. We apply this to the use case and recognize the characteristics of the auction:

- Single-sided: Infineon is the supplier and distributors are the buyers.
- Multi-attribute: Distributors bid through price, quantity and delivery dates, instead of price, individually.
- Forward auction: Infineon as a supplier sells to several potential distributors, who compete for the products.
- Sealed-bid auction: The bids are confidential to the distributors and it is vital that these bids are not revealed to the others.

According to past studies on usability and security technologies (Dourish, 2004; Kainda et al., 2010; Whitten & Tygar, 1999), we depict secure multi-party computation via symbolic representation through padlocks. Moreover, it is seen that transparency is a key criterion for users when using such a system. Therefore, we design the mock-ups in order to incorporate these features as follows:

- To communicate encryption we use text and the padlock symbol (Fig 20)
- To visually communicate the process of encrypting, we use the greyed out grid (Fig 22)
- To depict transparency, we use the transparent grid (Fig 23)

Table 2: Requirements to inform the design of the artefacts

Item	Requirement	Topic	References
A1	Privacy: no party should be able to get information apart from their own	MPC	Zhao et al., 2019
A2	Customer inputs: wished lead time, price and volume matrix	RM, MPC	Discussion with Infineon and Work Package 5 (SafeDEED) leaders (Fig 17)
A3	Single-sided, multi-attribute, forward, sealed-bid auction.	Auctions	Burmerister et al., 2002; Pla et al., 2014; Shi, 2013; Torrent-Fontbona et al., 2015
A4	Anonymity: nobody should be able to identify a bidder	Auction	Omote & Miyaji, 2001
A5	Confidentiality: obtain a set of numbers from each input party	MPC, Auctions	Bogetoft et al., 2006
A6	Execution: a built-in program may use standard arithmetic comparisons and operations	MPC, Auctions	Bogetoft et al., 2006

A7	Output: direct the outputs of the program to the parties	MPC, Auctions	Bogetoft et al., 2006
A8	Usability and user experience in online auctions (transacting directly with the supplier, transparent and dependable tool for transacting)	User experience, Auctions	Tarazona-Bermudez et al., 2014
A9	Trust (perceived benevolence and integrity) - The degree to which one party is genuinely interested in the other party's welfare - Its motivation to seek joint gain - People's belief in the safety mechanisms built into a website and an easy-to-use interface - Is built through (1) a belief that the vendor has nothing to gain by cheating, (2) a belief that there are safety mechanisms built into the website, (3) by having a typical interface (4) one that is furthermore, easy to use	User experience in secure online platforms	Gefen et al., 2003; Kim & Ahn, 2007
A10	Comprehensibility: the secure MPC protocol must be simple for users to comprehend	MPC, user experience	Lapets et al., 2016
A11	Simplicity: The service must be usable within a relatively narrow time frame by non-expert parties whose technical expertise might only comprise of basic knowledge such as navigating web browsing clients	MPC, user experience	Lapets et al., 2016
A12	Idempotence: parties should be able to resubmit (update) their data, should they find it to be corrupted	MPC, user experience	Lapets et al., 2016
A13	Accessibility: to reduce the complexity that might hinder participation, the software must be rapidly and easily deployable, requiring no extra setup	MPC, user experience	Lapets et al., 2016
A14	- Symbols such as a padlock to depict cryptographic technology - Transparency in the system - Prompts to warn users about permanent actions	Visualizing and communicating secure technologies	Dourish, 2004; Kainda et al., 2010; Whitten & Tygar, 1999; Yee, 2004

5.3 Description of the artefacts

The mock-ups are designed in a way to look similar to the current buying platform of Infineon while paying attention to the sequence of users' actions. As the input screen for RM is a radical change in comparison to the current buying platform, we keep in mind the progression of tasks that follow, should RM and MPC be introduced. Firstly, the customers are prompted to input their multi-attribute bids. Once this is complete and they confirm their inputs through the screens that follow, they are shown an intermediate screen (visible for five seconds) indicating that the computation is in process. The next screen provides them with the outcome of the computation, along with the choices of accepting or rejecting it. In addition to the sequence of actions, we are careful in designing the artefacts without unnecessary repetitions, yet with,

simplified operations, task clarity, the adaptability to customers' needs and wants, as well as providing clear and simplified information. Consequently, these design choices allow customers to smoothly experience the complete process of placing an order through the potential revenue management system using MPC as a tool.

The artefacts differ in the ways of how text and visuals are used in order to communicate the new system to the customers. In the first mock-up, there is only a text, briefly explaining the solution. It is coupled with the padlock symbol beneath the text, as such symbolic representations have been proven to prompt positive perceptions of security among users (Kainda et al., 2010; Whitten & Tygar, 1999). The second artefact presents the impression of encrypted data that implies that customers' inputs are protected. Whitten & Tygar (1999) discuss that users have more confidence in the system when the encryption element is transparent. Therefore, we design this mock-up in order to understand whether customers prefer to visually see proof of their data being encrypted. The last artefact incorporates transparency in a way to imply that the inputs are not being manipulated. The study by Whitten and Tygar (1999) discusses transparency positively. However, Garfinkel & Miller (2005) show that users can perceive systems as "a little too transparent" and consequently, a few users fail to read the instructions accompanying the visual indicators. Furthermore, Sheng, Broderick, Koranda & Hyland (2006) show that users are unsure whether encryption is in place, due to too much transparency. Therefore, by displaying users' inputs transparently, their trust in the system and supplier can be influenced.

All the platform mock-ups are developed using the programming language C#, on Visual Studio, in order for the mock-ups to be as realistic as possible as well as to have high quality, like that of a functional platform. While it was initially planned to use an online tool used for designing digital mock-ups (such as "Invision") or the use of paper-based prototyping, the mock-ups were revised in order to be designed and programmed with C#. The use of Invision was disregarded because Visual Studio provides the option of running the mock-ups as executable files, while Invision does not. Running the mock-ups as executable files during evaluation makes the process simple to follow as well as realistic for the participants. Since multiple screens were involved, for four mock-ups and due to the magnitude of the designing involved, Visual Studio was reasoned to be more manageable, robust and professional in creating and presenting the artefacts. The four artefacts developed are as follows:

1. Current buying platform (no RM and MPC)

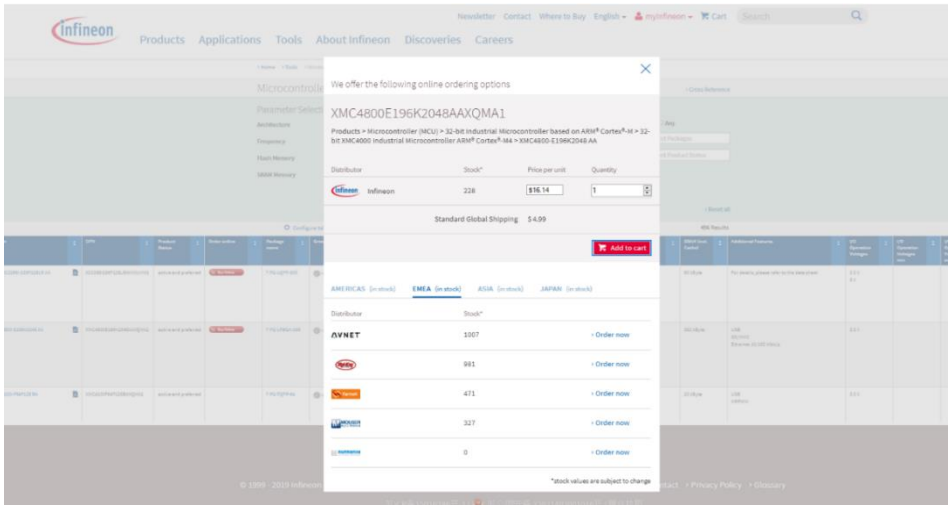


Fig 19: Current buying platform

This first mock-up is identical to the current buying platform of Infineon. There are no changes as the design and the functionality are directly taken from the fully functional website (as depicted in Chapter 3). The purpose of this interface is to build the foundation for the participants to understand the current ways of practice entailing the placement of an order. Additionally, demonstrating a video presentation of carrying out a buying process on this interface while walking through the main features and buttons, helps the participants to quickly grasp the setting of the experiment, understand the current ways of practice and equips them for the process they need to focus on during testing the potential future platform mock-ups. The two main reasons this artefact is shown to the participants in the experiment before they begin using the potential three future platform mock-ups are:

- To understand how the current buying platform (without RM and MPC) is, so as to be able to understand and compare how different the other three platforms are, which all include RM and MPC. This ensures that similar to real-life distributors, the participants are well-informed about the current ordering platform.
- To recognize which buttons are clickable on the interface. As they are all mock-ups, not all the available features are made to be interactive. Presenting a walkthrough of this interface helps the participants realize the task progression and the clickable features.

The next three interfaces that include different visualizations of RM and MPC have in common the left panel of the input screen, where customers fill in their bids. The right-hand side panel changes in each mock-up according to the text and visuals. This is because the focus is on the customers experiencing these different visualizations in order to understand the factors of importance to them, should RM and MPC be introduced to the market. While all the interfaces are programmed individually from the landing page until the order confirmation page, the main input screen for each mock-up is presented here to ease understanding. All other screens are common to all the three mock-ups and can be seen in Appendix 3.

2. Disclaimer

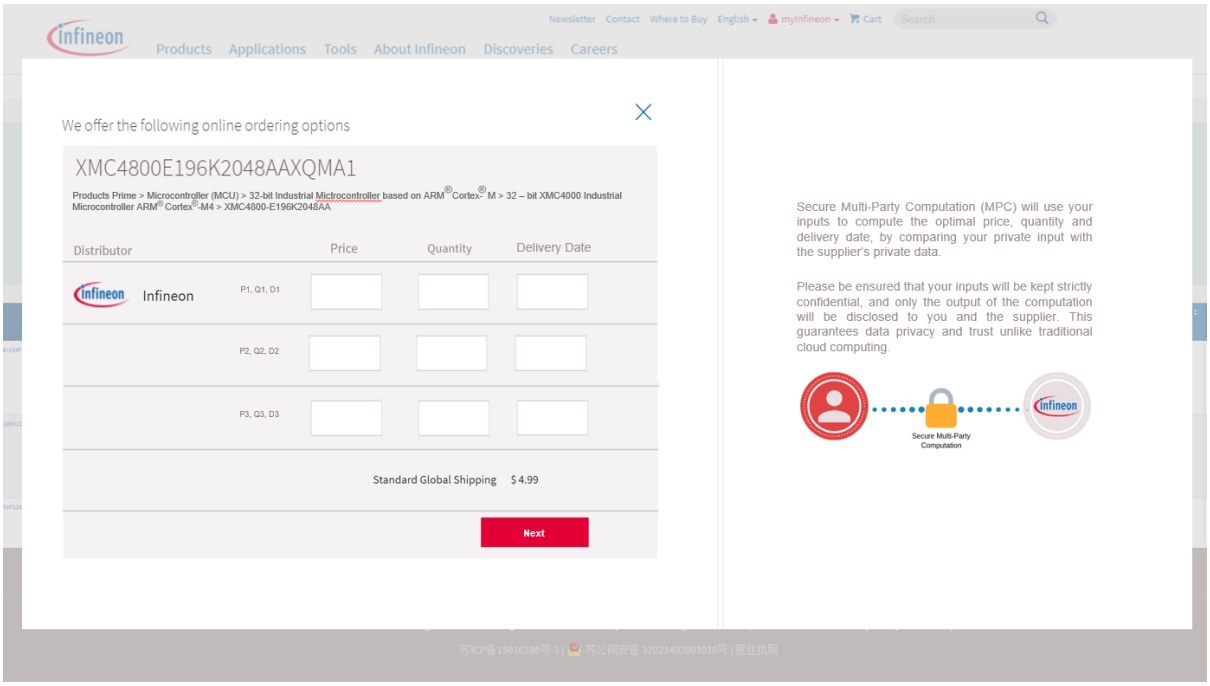


Fig 20: Potential platform mockup 1 - Disclaimer

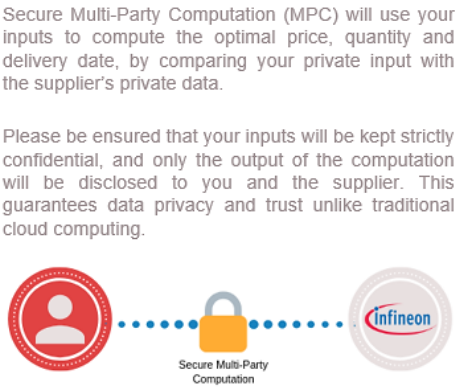


Fig 21: Disclaimer text and a padlock symbol

This mock-up presents a visual integration of RM with MPC, where customers can input a matrix of prices, product quantities and delivery dates. Furthermore, it includes a disclaimer about MPC. This platform is developed to give customers a clear idea of the new technology in the reformed platform and inform them about the process that will take place via a short descriptive text. The disclaimer makes it evident that there is a secure technology at play and that their inputs will be kept strictly confidential. Providing a disclaimer like here gives customers the chance of being aware of how their data may be used, allows them to learn more about it by themselves, as well as informs them of data security and privacy. Lastly, the padlock visual indicator under the text (Fig 21) further depicts the meaning of the text to reiterate the message and helps the customers to imagine this process (Kainda et al., 2010; Whitten & Tygar, 1999). We develop this mock-up based on the established auction scenario, literature review on MPC and the applicability of MPC to RM. We refer to this mock-up as 'Disclaimer'.

3. Blurry

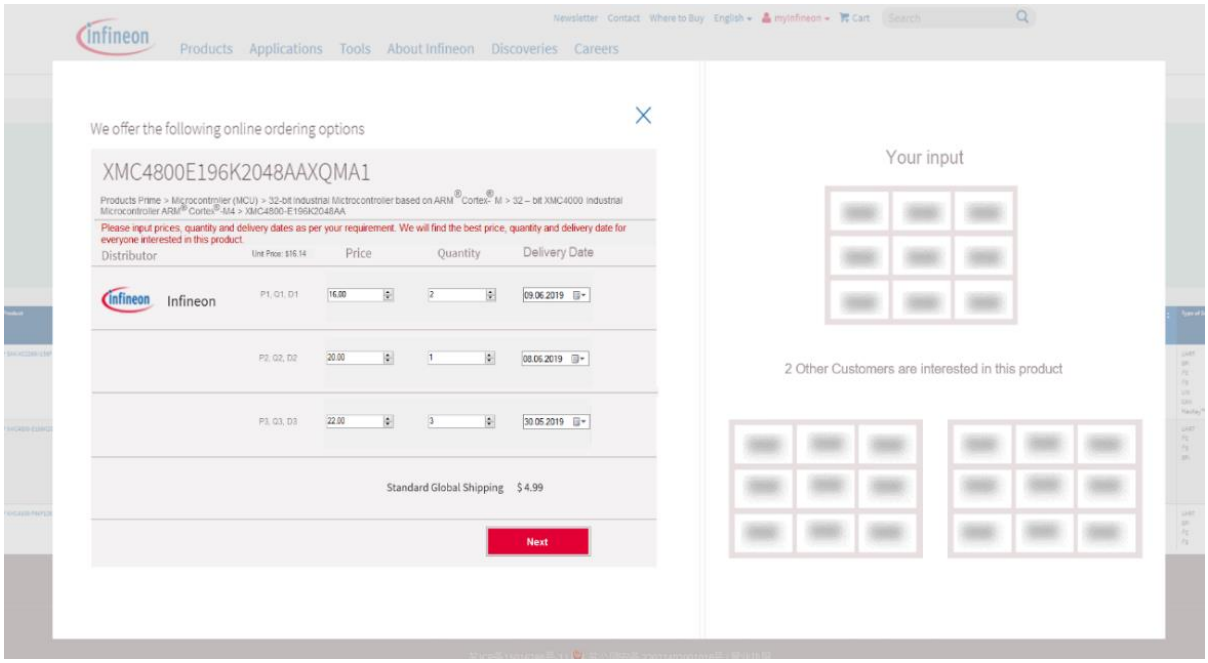


Fig 22: Potential platform mockup 2 - Blurry

This mock-up presents an alternate visual integration of the RM platform with MPC. This mock-up has no disclaimer about MPC, but instead, contains a blurred matrix visible against other customers' blurred matrices on the right-hand panel. This platform intends to make customers feel through the blurred visuals of their inputs that their data is encrypted and secure. As soon as they fill each field on the left-hand side panel, the grid on the right with "Your input" fills in and greys out. In addition to this, customers can see that other competitors are also interested in the product. Customers can notice other customers filling their grids, though they do not see the values of their inputs. This visual indicator shows that because their competitors' data is blurred and they cannot see it, similarly, their input too would be visible in this blurred format to other competitors, hence proving the encryption. This mock-up does not have any descriptive text to explain the situation to the customers, unlike the previous one. It relies on visuals and instant changes in the grid for inducing feelings in customers. We refer to this mock-up as 'Blurry'.

4. Clear

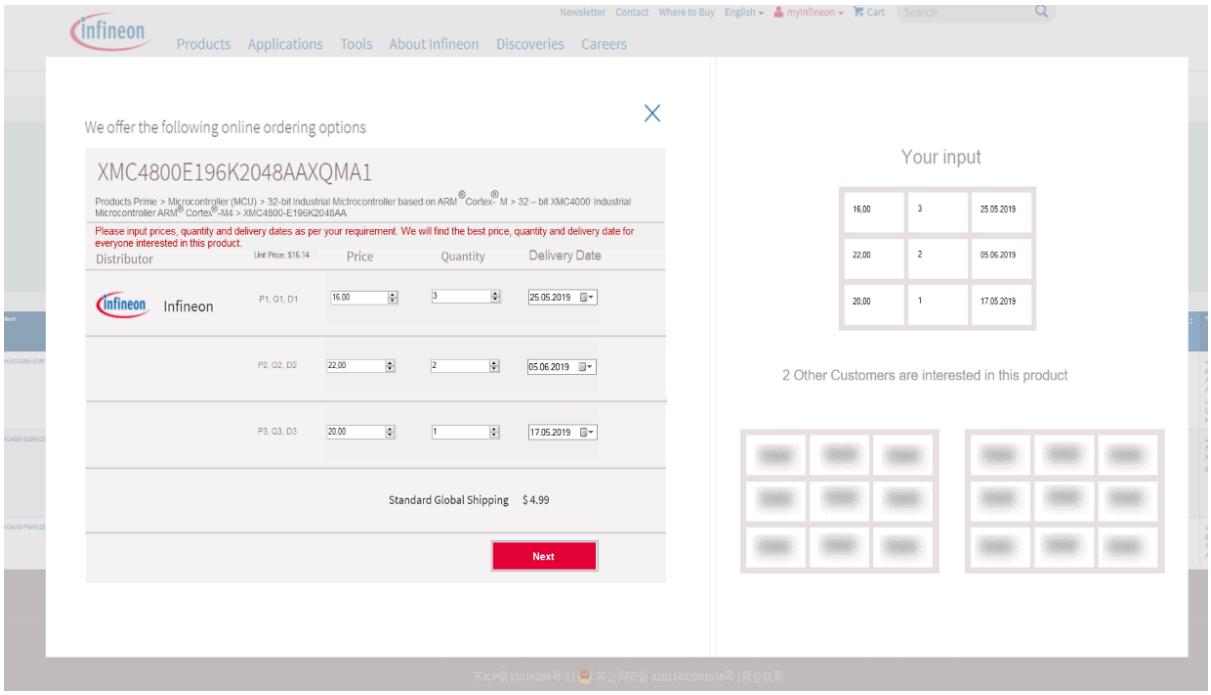


Fig 23: Potential platform mockup 3 - Clear

This final mock-up also presents a visual integration of the RM platform with MPC with no disclaimer about MPC. However, it provides a clear matrix visible against other customer's blurred matrices. This platform with the clear visuals of inputs shows customers the inputs that are being used for computation. It skips the blurred visual indicator of the previous mock-up that intends to make customers think that their inputs are encrypted and secure. In contrast, as soon as they fill in each field on the left-hand side panel on this mock-up, the grid on the right with "Your input", fills in identically, indicating transparency and no manipulation. In addition to this, customers can see that other competitors are also interested in the product. They are able to see that customers are filling in their grids, though they do not see the values of their inputs. This visual leaves the customers to imagine whether their data is encrypted, based on what they see from their competitors' grids. Like the previous mock-up, this design is also based on visual indicators, with no descriptive text to explain the process. However, this mock-up represents transparency, where customers can see their inputs being fed in real-time, for computation. We refer to this mock-up as 'Clear'.

6. Evaluation of the artefacts

In this chapter, we describe the evaluation approach we adopt for evaluating the artefacts and analyzing the data. We carry out user tests through experiments, followed by interviews to discuss the mock-ups. Then, we explain how we analysed the data collected from the interview sessions. After acknowledging the assumptions we make, we conclude the chapter by discussing the advantages and limitations of our approach.

6.1 Experimental approach

For effectively evaluating the design artefacts, a sound knowledge base of research methodologies is required. These are summarized by Hevner et al. (2004), where the authors elaborate that the choice of the evaluation method should suitably match the design artefact and the evaluation metrics so that the efficacy and goodness of an artefact can be rigorously demonstrated. The majority of the artefact's evaluation method is established by the business environment because the artefact is built within this environment. Therefore, the evaluation must consider the fit of the artefact within the technical infrastructure of the business setting.

One of the widely used and recommended methods for evaluating the usability of online security systems are user studies, where a sample participates in experiments in order to test a system's usability (Nurse et al., 2011). Particular instances of user studies include laboratory-based user testing, questionnaires, interviews, observing users and recording and assessing system use. In one of the first ever human-computer interaction and security studies, in order to study how users perceive the user interface of secure systems, Whitten & Tygar (1999) conduct user tests where participants are requested to use the secure software to perform a task. Moreover, the preferred evaluation method is semi-structured interviews, mainly because interviews are particularly suitable for examining events that happen irregularly and infrequently, such as user-tests (Nurse et al., 2011). Experiments are deemed to be the most suitable method to evaluate the artefacts developed in this research. This is because the artefacts we develop are at a fundamental stage and are not at the level of being directly used yet. Furthermore, the algorithm for LTBP is also not developed so far. In addition to this, access to real customers is not provided at this initial stage, according to the business setting. While discussing the experimental approach for evaluating artefacts, Cleven, Gubler & Hüner (2009) claim that the aim of the experimental approach is to isolate a certain effect as far as possible. All other factors that can have an effect on the dependent variables must be kept as steady as possible.

Following this, we have designed the artefacts such that the effects of text, suggested encryption and transparency through manipulating visual indicators can be tested independently through the experiments for evaluating the artefacts. The evaluation of the artefacts through a controlled experiment ensured that it is only the artefacts that are causing participants to feel a certain way about the usability factors (trust, security, perceived ease of use, perceived usefulness and intention to use). While it could be argued that the participants' varying previous knowledge about RM could affect their thought process, however, all the participants are provided with a basic explanation of RM beforehand, as well as are given enough room to ask questions. We ensure that everyone understands the relevant details to be able to think and perform like distributors while experiencing the three artefacts. We also ensure that every session has at least one participant from the LTBP team of the department.

Moreover, the evaluation is carried out within the resource constraints, such as access to limited participants, their availability and time constraints. Lastly, all the participants sign a consent form prior to taking part in the experiment.

The experiment includes nine participants as per the allocated resources of the company. We request the participation of five people who form the LTBP team of the Supply Chain and Innovation Department of Infineon. We also circulated a mass email to all the other students of the department, for those who would like to participate. As a result of five spots being filled by the members of the LTBP team, we chose the first four available participants who reached out to us. We requested the LTBP to participate because they have a better idea of how distributors think and act, which is valuable for generating close to realistic data in the controlled experiment and interview process. Three groups are made where there is at least one participant with sound knowledge of LTBP and RM. Session 1 has one such participant and Sessions 2 and 3 have two such participants.

All the students assume the role of one of Infineon's customer type, the distributor. There are three customers types of Infineon, namely, distributor representatives, electronics manufacturing services and direct accounts/OEMs. We use the scenario of distributors for this research, as they are a significant customer segment of Infineon, representing approximately 40% of Infineon's total revenue (Infineon, 2018). Distributors are wholesalers who purchase products from Infineon and sell them to their end customers and Infineon has no possibility to affect the prices between the distributor and customer. Therefore, distributors mostly sell products at a mark-up price for profit. They are a lucrative channel for Infineon to market with, as they have suitable infrastructure and a relevant customer reach. Infineon views distributors as partners who are vital to their success. They also provide support for a large and heterogeneous group. Furthermore, trainings are held for distributors to be well-trained on Infineon's products (Infineon, 2016). As their business is based on buying from Infineon and selling products at higher prices, distributors are willing to pay a lot extra as they are able to sell at even higher prices. All information regarding prices is confidential and they do not want to disclose this, as it could prove detrimental for their business. They do not want customers to know their margins, or other competing distributors to know the price you buy at, hence, signifying the sensitivity of the prices. These are key reasons why the distributors are a justified customer group taken for this research in terms of their need for confidentiality and revenue management. Overall with revenue management, distributors can depend more on short-term deliveries and serving their end customers, with a reduced bullwhip effect. It will enable them to expand their reach, as they can deliver on short notices. By choosing distributors, there is a smaller risk of harming a long-term relationship (such as that with a direct customer) and there is also no binding price for a certain period (for instance, the volume purchasing agreement).

Therefore, the distributors' profile is briefly described to the participants at the start of the experiment (Appendix 2). We then carried out the experiment, where the three platform mock-ups are used in turns by the participants and are evaluated based on usability criteria (trust, security, perceived usefulness, perceived ease of use and intention to use). The evaluation of artefacts includes defining appropriate metrics, gathering as well as analyzing appropriate data. Hevner et al. (2004), recognize that artefacts can be evaluated with regards to functionality, completeness, accuracy, consistency, performance, usability, fit with the organization and other relevant quality characteristics, also including the style of an artefact.

In this research, we evaluate the usability of the artefacts based on the research model in Fig 16, because the factors play a major role in understanding customer acceptance of RM and MPC, which is a proven barrier to the acceptance of RM (Garcia, 2018).

In addition to the evaluation parameters (trust, security, perceived usefulness, perceived ease of use and intention to use), there exist certain goals for designing the evaluation. According to Venable et al. (2012), there are three such possibly competing goals while designing the evaluation phase of design science research. These are as follows:

1. Rigour: All research, including design science, must be rigorous. There are two facets of rigour in design science. Firstly, it is in establishing that it is the artefact and only the artefact without other confounding independent variable causing an observed improvement, leading to the efficacy of the artefact. Secondly, it is in establishing that the artefact functions in a real situation, which is its effectiveness. We ensure the efficacy and effectiveness of our evaluation method respectively, by providing everyone with the same foundational knowledge prior to the start of the experiment, as well as by testing the artefacts with students employed in the manufacturing industry, to get a realistic environment for the evaluation without directly harming the crucial manufacturer-supplier relationship.
2. Efficiency: The evaluation must be able to be carried out within resource constraints such as money, equipment and people's time.
3. Ethics: Research should not needlessly put people, organizations, or the public at risk, during or after the evaluation.

During the experiment, firstly, we walk the participants through the first mock-up which is the current buying platform of Infineon. Through this, they grasp the current process and consequently, they can more easily compare the differences in the mock-ups they use that incorporate RM and MPC. The demo of the current buying platform also instructs them about which buttons are interactive, as these are mock-ups instead of fully functioning prototypes with an algorithm deployed at the backend. Next, they use the three potential future RM with MPC platform mock-ups, which was followed by semi-structured interviews (further discussed in the next section). We conduct three experiment and interview sessions which consist of three participants each. In each session, the three participants use the mock-ups in different orders (consistent within participants in one session) to account for order bias. This ensures that participants experience different orders of the mock-up and are not influenced by the order of any particular mock-up. The order that the participants use the mock-ups are:

- Session 1 uses Disclaimer -> Blurry -> Clear
- Session 2 uses Clear -> Disclaimer -> Blurry
- Session 3 uses Blurry -> Clear -> Disclaimer.

The introduction and explanation of the experiment took approximately fifteen minutes and the demo of the current buying platform took another five minutes. Participants on average took thirty to thirty-five minutes to get familiarized with and experience the three mock-ups as well as fill in a template that required them to rank and reason the platforms in terms of the usability parameters. This template is provided instead of directly interviewing the participants at the end, or, merely prompting the participants to write down their feelings after using each mock-up. Direct interviews at the end would lead to participants forgetting and mixing their

experiences with each of the mock-ups. Similarly, prompting the participants to write down their feelings on a blank sheet, would lead to us missing some important points due to the participants being inexpressive. We develop the template based on the interview questions (section 6.2). The same questions are presented to the participants in a tabular format, where they can rank and reason their choice of mock-ups. The template is valuable because it streamlines the participants' thinking process, so as to be relevant to the study. The template further helps in discovering factors in great detail which may not be possible without it, in contrast to if the participants were prompted to write down their feelings on a blank sheet of paper. Discussing and expressing feelings is challenging during interviews, however, using this method greatly eased the otherwise challenging process.

6.2 Interviews

The objective of the interview following the experiment is to explore specific topics of interest which lead us to infer how the usability factors (trust, security, perceived ease of use, perceived usefulness and intention to use) vary among customers, with the three different platform mock-ups. While this exploration can be targeted and specific, or open and general, this study adopts a method of providing the interviewees with the opportunity to express themselves openly while guiding the interview with structured questions. Thus, we adopt semi-structured interviews to allow room for understanding the challenges pertaining to customer acceptance of RM and MPC, as well as for guiding the interviews.

We considered adopting the research method of interviewing participants prior to designing the artefacts in order to understand the features that they think are vital for such a platform to be accepted. However, by testing this with a few available students, this was confirmed to generate not very useful and relevant data, because participants were made to imagine a future platform with no prior knowledge of it. Additionally, as the participants are students and not real customers, this process would have been extremely cumbersome for them to firstly, imagine such an interface and secondly, express themselves. Hence, this approach was ruled out. Our method of conducting post-interviews is more rigorous, where the participants experience the artefacts first and only then are questioned about their choices. Having a foundation beforehand and then experiencing the mock-ups allows them to understand how they would feel in place of the distributor. This approach enabled us to gather clear, detailed and relevant data.

Interviews rely on developing a good level of rapport with the participants while aiming to facilitate a natural interaction and flow of conversation. Therefore, as good practice, we structure the interviews to begin with an introduction (of the interviewer as well as the session). Next, we explicitly state the confidentiality, anonymity and the voluntary nature of the research, followed by requesting the participants to sign a consent form to proceed with the session. Following this, we provide the basic concepts of RM and the distributor's role to the participants (Appendix 2) to ensure that everyone is on the same page, as not everyone understands RM at the same level. Consequently, it is necessary to establish a common level of knowledge before proceeding further. The information that we present to the participants can be found in Appendix 2. We conducted the experiment and interview session with three participants common to each experiment and interview. The participants use the mock-ups independently in the experiment (in the same order within a session but different order across the sessions). However, the interview involves all the participants answering the questions of

the interview protocol turn-by-turn, while also giving them the opportunity to discuss with each other throughout the interview session.

In order to develop the interview protocol for evaluating customer's perception of the integration of RM and MPC, we build on items for evaluating user experience from literature (Alsaad, Mohamad & Ismail, 2017; Gumussoy & Calisir, 2009; Kim & Ahn, 2007). Based on the literature of technology acceptance models and the constructed research model (Fig 16**Error! Reference source not found.**), pre-structured post-experimental interviews are conducted. We ensured that there were no (mis)wording issues that could lead to unfocused answers.

We choose to conduct group interviews because participants can more easily provide more valuable inputs than isolated interviews. It also saves on time constraints (available time of participants), company and researcher resources (conducting nine different sessions during the limited time of this thesis) by grouping three participants in each session. Discussions with each other led to novel insights and changing perspectives which would not have been possible had the interviewees expressed their feelings one-on-one, isolated with the interviewer. Another reason to have group interviews is that it mimics the reality of the practical world where distributors will discuss among each other and share their thoughts on the new ordering system as well as the supplier's way of conducting business, through word-of-mouth. It further facilitates carrying on the discussions relevantly, as it helped and encouraged the participants to not only think individually but also provided them with the opportunity to discuss reasons for and against the other participants' view. This method facilitated in raising several viewpoints through discussion, despite the participants being nine in number. There is a high chance that the data would not have been as rich, had isolated interviews been conducted. Typically, it is particularly difficult to get participants to describe their feelings in interviews. We overcome this through the group interview, leading to a variety of thoughts surfacing.

On the other hand, it is important to acknowledge the downsides of group interviews. Firstly, group interviews can be perceived as a loss of privacy for interviewees. However, as we are not dealing with a relatively sensitive topic, this is not a major concern. Secondly, participants may respond in part to their peers, which may reduce the interviewer's control over the interview process. Therefore, it may inhibit the exchange of views, causing the loss of minority or opposing points of view (Ruyter, 1996). In order to mitigate this, all the participants were constantly prompted for their opinions and were reminded of the freedom to express their own individual ideas. Lastly, the results of group interviews are relatively unstructured in comparison to individual interviews.

The qualitative data from the interviews allow us to understand behaviour from the individuals' perspective. It adopts a more dynamic state of reality, offering a depth of information which quantitative data generally misses. Whether the research involves interviewing people or asking questions on paper, the researcher has the power to potentially influence participants' responses. Therefore, it is important to consider the reliability and validity (internal and external) of the study. In order to acquire qualitative data from the interviews that is of good quality, reliable and valid, it is important to consider some common pitfalls of qualitative data collection. In order to avoid any biases and maintain the reliability and validity of the data, our questioning style was:

- Neutral
- Open-ended (“why” questions)
- Jargon-free and clear
- Individual unbundled questions

The questions posed to the participants are as follows:

1. If any, which of the three platforms would you use? Why?
2. In descending order, could you please rank which interface promises to keep your best interests? Why?
3. Which interface felt the most secure to you? Why?
4. Which interface did you find the easiest to use? Why?
5. What do you think about revenue management? In terms of accepting the new pricing model?
6. Do you have any further comments or notes to share?

The questions above focus on getting the data on the following themes respectively: (1) intention to use, (2) trust, (3) security, (4) perceived ease of use, (5) perceived usefulness.

In order to be able to compare the participants’ responses with each other, it is vital to ask the same questions in the same order. Standardization of the interview’s structure ensures that the participants will have a similar experience through the process and that the results are not unevenly influenced by order bias. We also guarantee that the participants understand the questions by explaining words that are unclear as well as allowing them to ask any questions through the process. To further avoid biasing responses, we act neutrally with regards to expressions, body language, tone and demeanour, e.g., no opinions were provided by the interviewer. At the end of the sessions, we provided a brief to the participants in order to ensure what is learnt, is accurate. Furthermore, there was room for questions and further discussion at the end of each session.

Since Infineon is cautious at this initial stage to directly access their customers in the real world in order to study about acceptance, thus, only accessible resources are used in order to simulate the reality using students employed at Infineon. The Head of the Supply Chain and Innovation Department also participated in the interview, in order to provide valuable inputs based on experience in the industry, as well as to audit the quality of the interview sessions. The participants undergo the experiment, using the different artefacts and then expressing their feelings through the group interview sessions. Of the nine participants that we interviewed, five worked on projects directly related to LTBP and RM. This is useful because they have knowledge of the current order management process. Therefore, since they are instructed to assume the role of the distributor, they are more easily able to understand the constraints and feelings of the distributor. While the other four participants do not directly work with RM, they were part of the Supply Chain and Innovation department of Infineon and have a basic idea about the LTBP and RM initiative. The table below shows the list of interviewees:

Table 3: List of interviewees

No.	Job description	Date
1	Head of Supply Chain and Innovation	29.05.2019
2	Supply Chain Modelling & Simulation	29.05.2019
3	Digital Work Life & Human-Machine Interaction	29.05.2019
4	Semantic Web & Blockchain	03.06.2019
5	Lead time-Based Pricing	03.06.2019
6	Lead time-Based Pricing	03.06.2019
7	Lead time-Based Pricing	05.06.2019
8	Lead time-Based Pricing	05.06.2019
9	Knowledge Management, Education & Supply Chain Audits	05.06.2019

Lastly, we took notes during and soon after every interview session, in addition to the audio recordings so as to not miss out on any details mentioned by the participants. Essentially, the researcher themselves are a tool for conducting qualitative research because the way they express and communicate can influence the interview.

6.3 Data Analysis

A common approach to analyzing qualitative data is thematic analysis (seen in Fig 24). Thematic analysis is used to realistically and accurately present experiences, meanings and the reality of the involved participants. Moreover, Braun & Clarke (2006) describe thematic analysis as a means to identify, analyze and report patterns within data. This method concisely organizes and describes data in rich detail. Additionally, it is flexible, accessible and more widely used in comparison to other more complex forms of qualitative analysis. It works towards identifying patterns across participants' datasets, rather than analyzing within an individual dataset. Fig 25 explains how the themes were developed for analysis.

Once the interviews are conducted, the audio recordings are transcribed in text format. Then, the participants' names are substituted by pseudonyms. Additionally, we double-checked the transcripts to ensure their correctness. We begin the analysis process by performing an open-coding on the transcripts on paper. "Codes" are a concept that most accurately label what is being described. Codes are used to organize data into meaningful groups, extracting and segregating aspects of the data that are interesting, relevant and meaningful to the research. We continued to highlight words, phrases and sentences that describe a particular phenomenon and gave these a name, i.e., a code. We ensured that the code remains as close to the original language of the participants. A lot of codes were generated in the first run, where some codes were not related to the research questions. While we already have the five pre-determined themes based on usability criteria from the literature research (perceived usefulness, perceived ease of use, trust, security and intention to use), instead of preliminarily establishing codes only relevant to these themes, a second round of coding was performed. This helped to get rid of the codes that were not related to the study and fine-tune the already identified codes to represent meanings as closely as possible to original quotes. For this, apt code names were selected, which were slightly different from the code names identified in the first round of coding.

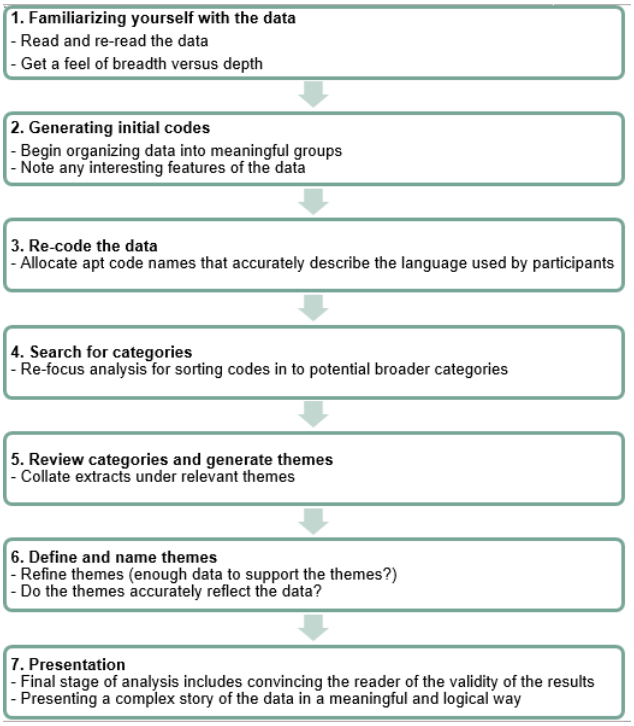


Fig 24: Stages of thematic analysis

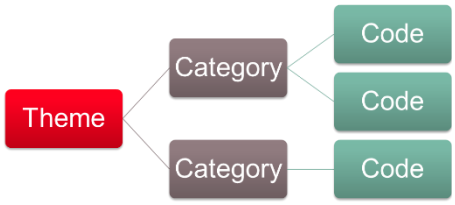


Fig 25: Development of themes

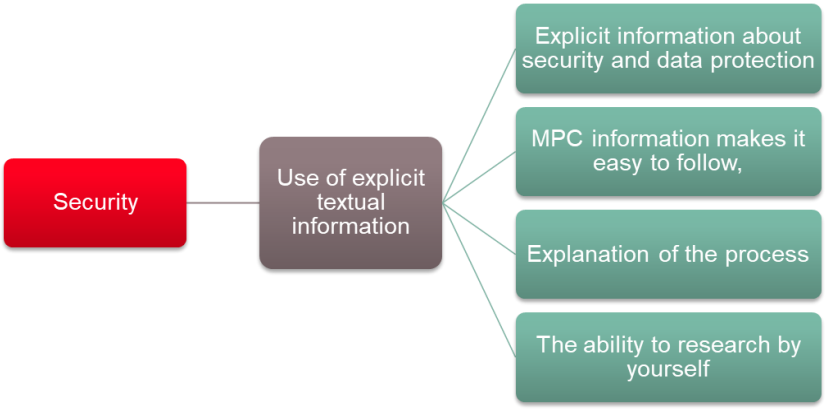


Fig 26: Example of codes, categories and theme

Once the codes are identified, the transcripts are coded on ATLAS.ti 8.0, a computer-assisted software for analysis of qualitative research. ATLAS.ti facilitates the analysis for unstructured and semi-structured data, as in this research. It allows codes to be assigned to certain parts of the texts and the codes can be grouped together under one defined group. For instance, codes that all relate to the feelings expressed specifically due to the presence of the text in the Disclaimer mock-up were grouped together. These codes are “explicit information about security and data protection, MPC information makes it easy to follow, MPC information feels safe, explanation of the process and the ability to research by yourself”. All these codes contain viewpoints strictly related to the presence of the information in text through the Disclaimer mock-up.

Subsequently, the codes were put together in different “categories” (Fig 26). Codes with similar meanings can be grouped together under a category. Using the example codes above, the codes were grouped into a category called “use of explicit textual information”, as all the codes within this umbrella term relate to the presence of the specific text. As the majority of these discussions occurred while discussing the security element of the interfaces, we group the category under the theme of security. Once again, the category names were kept so as to closely resemble the original language and meaning of the participants. Through this grouping and the need for categories to be more inclusive of the codes under it, the category names become more general and abstract than the code names. The guideline followed here was to stick to the language that would still be understandable to the participants. Additionally, it is a tendency for researchers to identify and use data that confirm our own predisposing assumptions and to neglect the data that contradict them. Hence, the transcripts were read and reread multiple times without bias in order to ensure all findings are taken into account.

As the interviews were semi-structured, the pre-determined themes (perceived usefulness, perceived ease of use, trust, security and intention to use) helped in structuring the categories. Broad themes were identified under which codes that are linked within categories, were collated. This is the stage where the data was being interpreted in order to make sense of it in relation to the research question. Different categories were combined to fit an overarching theme. All the extract linked to a particular theme must fit a coherent story within a theme and be meaningful in the big picture in relation to the entire dataset. This implies that it should be meaningful not only within themes but also between them. In addition to the five pre-determined themes, one new and relevant theme was also discovered during the process of open-coding and by keeping an open mind towards any new discovery or development. This was guided by the principles of grounded theory, for being open to what is grounded in data. This theme is the ‘perceived extent of control’, which is a key usability concept that multiple participants strongly related to. There were contrasting points made in favour of and against how the presence of information induced certain feelings. These will be discussed in detail in Chapters 7 and 8. Lastly, the researcher is responsible for collecting, sorting and analyzing the information and reaching conclusions. Chapter 7 details the results of the study.

6.4 Assumptions

In this section, we discuss the assumptions we have made in conducting this research. We initially planned to design the mock-ups via a basic design web tool (Invision). This would not be as interactive and would only rely on visual depiction. Paper-based prototyping was also

considered as it might have been cumbersome to design four artefacts via a tool. However, to ensure a realistic artefact within a realistic business setting, the mock-ups were programmed via Visual Studio, in C#, despite it taking much more resources in terms of effort and time. This involved learning a new skill and programming language, as it was deemed to be essential for experimentation when participants interacted with a realistic interface, ensuring the rigour of the research. The following assumptions were made with regards to the artefact and experimental design:

1. While the mock-ups were programmed in C#, they were not built upon an MPC and LTBP algorithm, as these are unavailable at the moment and are still under development. Hence, the data handling is not entirely robust. During experimentation, participants were instructed to input realistic data entries only, as not all possible anomalous scenarios can be tested. The fact that participants were instructed to input realistic data commonly through all the mock-ups, along with an example bid that was explained at the beginning (Fig_of_Appendix 10), ensured that the lack of algorithms does not affect the study. It is worth noting that when customers will use the future platform as well, the participants will not be interacting with the algorithm and their feelings would be affected by the visuals that they experience and interact with.

2. While Infineon has multiple customer types as seen in (Fig_of_Appendix 3), this research studies the varying acceptance of the mock-ups with one customer segment (distributors). Distributors make up a large share of Infineon's customer base and will be most impacted by the RM with MPC platform. A single customer segment is chosen in order to ease the cognitive burden on the participants due to the complexity of the experiment, as it involves assessing three mock-ups and then an interview. Another reason why one customer segment is selected is due to the resource constraints. As nine participants were included in the experiment and interviews, it is more valuable for the research to have one significant customer segment commonly represented by all nine participants instead of sparsely distributing three customer types over the nine participants, resulting in adding no significant value to any single customer segment. Hence, the scope of this study is limited to distributors. Furthermore, students are used instead of real customers, due to real customers being inaccessible at this stage.

3. Infineon conducts its business through SAP, which is usually used by its customers to place orders. The current buying platform depicted (Fig 19) and used for this study is the online order placing website, which is also used an additional selling channel by Infineon. Since access to SAP is restricted, this functional website is used in its place.

6.5 Advantages and limitations

Multiple design science research frameworks have emerged with time. However, they are all similar in the sense of dividing the design process into multiple phases by establishing milestones to guide the design process (Koppenhagen et al., 2012). This aids in smooth transitions between guidelines while having a clear vision of the big picture. Another advantage of this approach is that it endorses an iterative approach, going through multiple cycles of the design process by incorporating the feedback from each cycle, proving rigour in the methodology (Takeda, Veerkamp, Tomiyama & Yoshikawa, 1990; Peffers, Tuunanen, Rothenberger & Chatterjee, 2008; Sein, Henfridsson, Purao, Rossi & Lindgren, 2011).

Furthermore, the approach allows for testing and evaluating the designed artefacts against the chosen case setting for validation. This provides the foundation for reaching an optimal solution which is accepted by consumers and semiconductor firms.

Furthermore, collecting qualitative data through interviews enables us to access rich and detailed information about selected participants in their specific context (Mohajan, 2018). Adopting semi-structured interviews also provides the flexibility to follow unexpected ideas during the research, due to the room for discussion. This ensures that all the ideas are explored effectively. This led to the unexpected generation of the additional theme while coding the interview transcripts. This was possible because the interviews were not limited to the questions and could be redirected by the researched in real-time when required. This also permits participants to open up and can provide evidence that was not initially considered. Furthermore, as our approach uses a small sample size, costs and resources are minimized. This is because since we involve students, they are willing to participate at no cost. Additionally, because there is one researcher to conduct the experiment and interview sessions, resources had to be matched accordingly.

On the other hand, a limitation due to the short history of design science is that it is case sensitive. The sub-processes within frameworks differ depending on the case setting. For instance, a design science framework for digital platforms for start-ups is different from that of a mobility-as-a-service platform (Nederstigt, 2016; Tura et al. (2018). Little is discussed about validating and publishing scientific contributions of design science research, while importance is given to the evaluation criteria and valuation in terms of the artefact's utility (Hevner et al., 2004). Another issue to note is that the experimentation is not done with real customers but it is a simulation of the real world using students as participants. However, Chen & Hirschheim (2004) explain that most of the experiments as part of a design science research are in fact carried out in an artificial setting.

Subsequently, designers must rely on intuition, experience and trial-and-error due to the inadequate existing knowledge base. Hence, a constructed artefact represents the designer's understanding of the problem and solution, which is essentially the contribution of the research, and this can further be built upon. Through the developed artefact, it is possible to learn about the nature of the problem, the environment and the possible solutions. This is the reason why it is significant to develop and implement prototype artefacts (Hevner et al., 2004).

With rapid advancements in technology, design science research is prone to perishability. These rapid advancements can invalidate the results of design science research before they can be effectively implemented in businesses, or before sufficient payback can be realized once organizational resources are committed to implementing the results (Hevner et al., 2004). Design results can be overtaken by technology even before they make a presence in the research literature. Hence, design science researchers should continue to advocate the capabilities and impacts of new technologies and artefacts, to businesses. Design science facilitates the creation of technological artefacts that greatly impact people and organizations. It focusses on problem-solving and often takes a simplistic view of the business setting in which the designed artefacts would function. The potential of advancements through design science lies in the design of an artefact, its formal specification and an assessment of its utility, which is often through comparison with competing artefacts, as is the case in this study.

7. Results

This chapter outlines the findings of the experiment and the interviews. We detail the factors and participants' feelings related to acceptance of the artefacts that are discussed in the interviews. To begin with, as it was ascertained through the literature review and the field study, everything that is discussed through the interviews is initially categorized under the five pre-determined themes (trust, perceived ease of use, perceived usefulness, security and intention to use). As a result of semi-structured interviews and room for open discussion, a new theme is discovered because we are open to new ideas. This suggests that relevant and important ideas from the interviews are not missed and everything that is discussed is reported and analysed.

The results (further elaborated in the next sections) show that **trust** and **security** (pre-determined themes from the literature review), and the **perceived extent of control** (newly discovered theme) are the factors that involve the participants in choosing a particular mock-up over another. The other three themes (**perceived usefulness, perceived ease of use and the intention to use**) caused participants to feel indifferent about the visual representation of the integration of revenue management and multi-party computation. Reflecting back, one of the reasons for this result for perceived usefulness may have been due to the way our question was phrased, which was directed to gauge perceived usefulness (what do you think about revenue management? In terms of accepting the new pricing model?). However, this question may have been general instead of being directed specifically to the interfaces.

Of the three sessions (S1, S2 and S3), S2 was shorter and the discussions less elaborate. The participants were comparatively less talkative in this session. On the other hand, S3 was the longest and along with S1, participants had elaborate and relevant discussions.

Table 4 summarizes the points that were raised during discussions in the three interview sessions. The first three columns consist of the themes, the categories within the respective themes and the codes within those categories.

The next column of "Code Frequency" (four sub-columns: Session 1, Session 2, Session 3 and Totals) presents the number of times a particular code was discussed.

Moreover, the "Participant Mentions" column shows how many people (out of 9 participants) discussed a particular code. The colours of these columns represent the extent of discussion of a particular topic/code (from red, yellow to green, increasingly signify the extent of discussion).

Finally, the last three columns break down for each code, how many times the participants chose each mock-up (Disclaimer, Blurry and Clear). We count each time a participant negatively or positively, explicitly links a particular code with a mock-up. Consequently, each cross signifies how many times the participants chose why they did not like a particular mock-up respective to the code, whereas, the tick signifies the participants preferring a particular mock-up, corresponding to a particular code. For instance, for the first code (unfair treatment against competitors) the Disclaimer mock-up was negatively discussed as an example once

and the Blurry and Clear mock-ups were negatively discussed examples twice. Similarly, for the code “visuals induced confidence in encryption”, the Disclaimer mock-up was not discussed at all, the Blurry mock-up was preferred nine times, and the Clear mock-up was preferred once.

The table concludes that in the theme of trust, the Clear mock-up was preferred (Disclaimer: -14, Blurry: +1, Clear: +14). In terms of security, the Disclaimer mock-up was favoured over the other two interfaces (Disclaimer: +24, Blurry: -7, Clear: -12). Lastly the Blurry and Clear mock-ups were both chosen favourably in the theme for control (Disclaimer: -1, Blurry: +4, Clear: +4).

The three relevant themes (trust, security and control) will now be discussed with their categories including the feelings of the participants and their quotations.

Table 4: The themes, categories and respective codes, with the number of times each code was mentioned by session and participants, along with a breakdown of the number of times each mock-up was positively and negatively chosen for each code

Theme	Category	Codes	Code Frequency				Participant mentions (9)	Platform mock-ups		
			Session 1 Gr=30	Session 2 Gr=30	Session 3 Gr=40	Totals		Disclaimer	Blurry	Clear
Trust	Malicious intent of supplier	○ 8. Unfair treatment (against competitors)	1	0	4	5	4	✗ -1	✗ -2	✗ -2
		○ 9. Dubious/malicious intent working behind Gr=7	0	1	6	7	4	✗ -4	✗ -3	✗ -1
		○ 12. Lack of trust in disclaimer by supplier	0	1	4	5	3	✗ -5		
		○ 27. Suspicious Gr=5	1	0	4	5	3	✗ -3	✗ -2	
	Transparency	○ 14. Visuals induced confidence (in encryption) Gr=10	3	4	3	10	6		✓ 9	✓ 1
		○ 18. Transparency Gr=9	0	4	5	9	5	✗ -1		✓ 8
		○ 20. Honest Gr=3	0	1	2	3	3			✓ 3
		○ 24. Assurance of inputs Gr=7	0	1	6	7	4		✗ -1	✓ 3
									Totals:	
								-14	1	12
Security	Use of explicit textual information	○ 1. Explicit information about security and data protection Gr=13	2	5	6	13	7	✓ 12	✗ -1	✗ -1
		○ 21. MPC information made it easy to follow Gr=1	0	1	0	1	1	✓ 1		
		○ 22. MPC information felt safe Gr=1	0	1	0	1	1	✓ 1		
		○ 25. Explanation of process Gr=9	1	2	6	9	4	✓ 8	✗ -1	✗ -1
		○ 29. Ability to research by yourself Gr=2	2	0	0	2	1	✓ 2		
	Insecurity in repetition	○ 6. Unnecessary repetition reducing security Gr=5	4	1	0	5	4		✗ -1	✗ -5
		○ 11. Increased hacking possibility due to multiple data paths Gr=1	1	0	0	1	1		✗ -1	✗ -1
		○ 13. Disturbing Gr=1	1	0	0	1	1			✗ -1
		○ 19. Tricky visuals without information Gr=3	0	1	2	3	3		✗ -3	✗ -2
		○ 5. Industrial espionage Gr=1	1	0	0	1	1			✗ -1
									Totals:	
								24	-7	-12
Extent of control	Competition induced stress	○ 2. Competitors push bids Gr=3	2	1	0	3	2		✗ -3	✗ -3
	Feeling of being in control	○ 3. Feeling of being in control Gr=3	2	1	0	3	3		✓ 2	✓ 2
		○ 4. Competitor advancement Gr=7	2	4	1	7	5	✗ -1	✓ 4	✓ 4
		○ 26. Assurance in market demand Gr=1	0	0	1	1	1		✓ 1	✓ 1
									Totals:	
								-1	4	4
		Totals	23	29	50	102	67			

7.1 Perceived usefulness, perceived ease of use and intention to use

The participants were indifferent between the artefacts when asked about the perceived usefulness, perceived ease of use and intention to use. One main reason for this result for perceived usefulness may have been due to the way our question was phrased. It did not target perceived usefulness specifically at the interfaces but rather the perceived usefulness of the entire system. Discussions around these three themes did not include any of the mock-ups directly. Instead, these themes entailed a general discussion about RM as well as its usefulness and barriers. Consequently, the participants did not choose, discuss, or justify any single mock-up with respect to these themes. As the participants are not experts in the field of RM, these general discussions are not relevant to understanding how customers visually perceive a potential platform implementation of RM and MPC. Furthermore, these discussions are not helpful in understanding the barriers of implementing RM as these remarks are not supported with any evidence or reasoning based on the mock-ups. Concisely, because the logic and functionality of all the three mock-ups were the same and they differed only visually, participants expressed that all the mock-ups were equally useful (or not), equally easy to use and participants had the same intention to use (or not) across any of the three mock-ups as all of them hosted the same system.

7.2 Trust (consideration of customer's best interests)

When participants discussed trust, they expressed concerns about their trust in the system and implicitly, also the supplier. Similar to the current website, they perceive that the supplier is the owner of the new system. Hence, the theme of trust entails two categories as per the discussions. This includes perceiving a malicious intent of the supplier (trust in supplier) and transparency of the mock-ups (trust in system). These two categories complement each other such that the more transparent the mock-up was, the less the participants felt that the supplier had a malicious intent. The Disclaimer mock-up, which only presented the new RM and MPC system via text and a padlock symbol, generated negative feelings among the participants regarding trust in the supplier (the owner of the platform). The reasons involved feelings of being unfairly treated against competitors, the supplier having ulterior motives to use their data, the lack of trust in the text disclaimer posted by the supplier as well as being suspicious overall about the supplier.

On the other hand, the Clear mock-up performed well with respect to transparency, which people associated with trust in the mock-up. This is a positive category for trust which prompted the participants to choose the Clear mock-up, while they expressed their dislike towards the Disclaimer mock-up in the previous category. This holistically shows why people would trust a potential RM with MPC platform, and distrust the supplier. We count each time a participant negatively or positively, explicitly associates a particular code with a mock-up. While the Disclaimer mock-up scored -14 due to participants' negative mentions, the Clear platform scored +12 owing to its positive mentions, proving that for trust in the system, transparency is key and the clear mock-up provides that. The Blurry mock-up scored highly on one code only, wherein visuals of greying out their inputs gave them the confidence to trust the mock-up with their confidential data. While this mock-up was picked nine times for this code, due to being discussed negatively in the other codes it only scored +1 overall.

Every code under the theme of trust was elaborately discussed, as seen by the green colours of the total code frequency and the participant mentions columns of Table 4. This implies the importance that the participants gave to trust, wherein S3 discussed the most about this.

7.2.1 Malicious intent of supplier

This category contains four codes. These are “unfair treatment (against competitors)”, “dubious/malicious intent working behind”, “lack of trust in disclaimer by supplier” and “suspicious” feelings. This is a negative category influencing trust. The reason these codes fall under the same category is that they relate to users’ distrust in the supplier and doubting the suppliers’ intent. Concisely, some participants felt that the supplier may have ulterior motives, of which treating them unfairly against competitors is a result, while also not believing the disclaimer presented on behalf of the supplier.

7.2.1.1 Unfair treatment against competitors

Participants often brought up the topic of feeling that their data might be treated differently to their competitors and used unfairly against them. Four of the nine participants discussed this issue. While the Blurry and Clear mock-ups were chosen twice each to negatively generate feelings of being treated unfairly against competitors, one participant mentioned this about the Disclaimer mock-up. The reason for the latter was explained in the manner that the manufacturer’s employees may use the customer’s inputs and compute a different algorithm with it leading to unfairness.

S3-P2: “Any employee regardless of input that I make, they might compute another algorithm with my input which is unfair. So I wasn't sure that my interest will be kept.”

S3-P3: “Maybe there is a chance that the data can be shared with other people, with other distributors.”

The mock-ups Blurry and Clear both provided visuals of competitors’ data in a grid format. In S3 there was an elaborate discussion on the possibility of the manufacturer using customer’s inputs against competitors’ grids and using negotiation tactics based on competitors’ data to influence another customer’s price. The reason for this feeling was because these two mock-ups do not explicitly mention that their data will be dealt with securely. For these two mock-ups, a participant from S1 stated that it was rather useless to have the grids on the right-hand side panel, both their own grid as well as competitors’ grids. They felt their data was re-opened after already entering it on the left-hand side and this induced feelings of being treated unfairly against others.

S1-P2: “They provided my information twice, I didn't see any point of it. I rather felt treated less fair because my data is opened again so maybe it's treated in a different way than the data of my competitors.”

S3-P1: “What if the manufacturer in the platforms with the grids shares your inputs, all of your input with each other or he negotiates with me based on your prices? Because he or she does not mention there that they will not use your data in those two interfaces.”

7.2.1.2 Dubious/malicious intent working behind

Four participants discussed the issue of negatively feeling that the manufacturer has ulterior motives to misuse customers' data. The Disclaimer mock-up was negatively picked four times, the Blurry mock-up was negatively picked three times, and the Clear mock-up only once. For the Disclaimer mock-up, participants felt negatively about it because they could not visually see what happened to their data and perceive that the manufacturer tries hard to make them believe via a text that they need not worry. Ironically, this created distrust among participants.

Similarly, for the Blurry mock-up, participants believed that greying out their inputs did not give them a chance to see what data exactly has been used for computation. They know that it is some data but they had no chance of seeing that it is exactly the inputs they have entered. This led them to believe that the manufacturer may have malicious intent and could alter their data for its own benefits without customers really knowing.

While the Clear mock-up was not preferred explicitly, the lack of negative mentions for it relatively suggests that the participants did not see a reason to doubt the intent of the supplier in this mock-up. Conversely, it was the text which was not supported by visual indicators in the Disclaimer mock-up, and the blurred cells suggesting encryption in the Blurry mock-up that led to participants doubting the intent of the supplier.

Like the previous code, S3 had an elaborate discussion on this while S1 did not mention this and it was mentioned once in S2.

S2-P2: "The one with the blurred cells almost seemed a bit dubious to me."

S3-P1: "Yeah, so my data might be used under the hood somehow."

S3-P2: "I felt that in the one with text, I had a feeling that something is working against me behind."

S3-P3: "The platform showed this sign and that it's going to be trustable but then instead it just created untrusted parts of it. We don't know actually if my input is going to be taken seriously or not."

7.2.1.3 Lack of trust in disclaimer by the supplier

This code particularly pertains to the negative feelings generated by the Disclaimer mock-up. Three participants of S2 and S3 mentioned five times that the text without any visuals was rather incomplete by itself and did not elicit feelings of trust, but rather distrust. The text raised questions on how accurate the information in the text was and whether it was truly believable. As a result, the Disclaimer platform was mentioned as negatively prompting feelings of trust five times.

S2-P1: "It only says that your data is safe. It's just a text by the supplier. It's not visual but just a text that says your data is secure. I would go for the image actually, like the blurred image. Not for the text."

S3-P3: "I got the feeling that I might be cheated now, you never know what's actually going on. That's why I was very insecure about this platform whereas the other one was completely showing everything. I personally wouldn't trust the text because anything can be done by a company even though it says something. But you don't actually know."

S3-P3: "As a company, if I want to use your data, you wouldn't know unless you really investigate it. So this is the feeling that you get directly when they say all your data is protected. Do you think a hundred percent that it's actually protected?"

7.2.1.4 Suspicious

Three participants in S1 and S3 discussed that they found the Disclaimer and Blurry mock-ups to be suspicious, linking it to the intent and thus, the trust in the supplier. For the Blurry mock-up, they mentioned that the greying out of their inputs in the grid on the right-hand side seemed suspicious. They were unsure of whether their data was only visually shadowed for them to see, or whether it was actually protected. For the Disclaimer mock-up, a participant of S3 mentioned that they were unsure whether their input is going to be taken seriously and used for the right reasons in their best interest. For this mock-up, another participant mentioned that showing the computing image below the text ironically raised suspicion in the platform.

S1-P2: "Even though it was shadowed on the screen, maybe it's actually not. There is no information provided whether this data is really protected or if it's just visually shadowed by the supplier."

S3-P2: "For the first platform, I thought that just blurring the face seems all suspicious to me."

S3-P3: "We don't know actually whether my input is going to be taken seriously or not"

7.2.2 Transparency

This category also consists of four codes. These are "visuals induced confidence (in encryption)", "transparency", "honest" and "assurance of inputs". This is a positive category influencing trust in the system, while the previous category focussed on the 'trust in supplier' aspect of trust. Participants believed that visual indicators in the Blurry interface prompted confidence in the system. Furthermore, they expressed that they considered the system to be transparent and represent all the necessary information in an honest way through the Clear mock-up. Additionally, the grid that replicated their bids in real-time gave them assurance and the opportunity to double-check their data. As all the discussions were targeted towards the users' trust in the system, this category under the theme of trust discusses the 'trust in system' aspect of trust.

7.2.2.1 Visuals induced confidence (in encryption)

Participants in all sessions discussed that the visuals of the Blurry mock-up induced confidence and a good feeling with regard to trusting the mock-up. Six of nine participants discussed this idea and it was mentioned a total of ten times, thrice in S1, four times in S2 and thrice in S3. The participants found it assuring to see that because their inputs are blurred and

they see others' grids blurred out as well, other competitors would be unable to see their inputs too. They also discussed that it brings them value to see other competitors' grids greyed out. They mentioned that they trust that their confidential inputs are encrypted immediately and directly, making them feel safe and confident.

S1-P3: "Showing that the others are greyed out, gives me confidence that the others also see me as only greyed out. So it's value addition in seeing that the others are greyed out."

S2-P1: "I think that the blurred view displays that your view is not visible for the other competitors as well. So I got more the feeling that the data is more confidential in that way, I would say. So that both the supplier and the other competing customers can't really see your offer."

S2-P1: "Because my offer is blurred. So you really see that the offer is encrypted directly. The other one only says that your data is safe. It's just a text by the supplier. It's not visual but just a text that says your data is secure. I would go for the image actually, like the blurred image."

7.2.2.2 Transparency

Transparency in the Clear mock-up in S2 and S3 was a key point of discussion by five of nine participants. A participant also particularly compared the transparency of the Clear mock-up to the Disclaimer mock-up, scoring the latter negatively on transparency. Participants of both these sessions related to the transparency from the supplier's side where everything is clear, including the data they enter. A participant explained that security is not the main focus but transparency and knowing that the system is fair, is important. This led to the Clear mock-up scoring highly on this code.

S2-P2: "For me, it would be the most transparent one. So I literally see what I typed in.

S2-P2: "It's not about data security but on the competition. And if you approach it from this direction then it would be the most transparent one."

S3-P1: "Because of the visibility of my own inputs, I could track my own input".

S3-P2: "The original idea was that I was sure that my input is correctly given."

7.2.2.3 Honesty

This code relates to transparency. Three participants of S2 and S3 felt that the Clear mock-up presented all the desired information in an honest way, giving them a good image. This was due to the transparency in the Clear mock-up, which made them feel that they are not tricked. In an honest manner, the Clear mock-up provided them with all the information for making their choice. In this regard, the Clear mock-up was said to be a well-balanced platform, including an auction scenario, the information about their competitors and honesty and transparency of the system. This led to the participant feeling confident and scoring the Clear mock-up positively.

S2-P2: "Plus it shows the information that you typed again, so it seemed like you're not getting tricked. It would be the most honest one and I also see that in an honest way that some other customers are interested in the products.*"*

S3-P2: "It was well-balanced because I had the atmosphere of an auction, such that other customers are also interested in my product. So I had some feeling that I should take them also into my consideration and I was certain about which input I am making. I had the feeling that I was confident that my input is correctly put into the system."

7.2.2.4 Assurance of inputs

Four participants discussed the surety they felt in the Clear mock-up due to the visual indicator of their inputs on the right-hand side panel, giving them the reassurance of the data they entered. They also liked the fact that the Clear mock-up provided them with the opportunity of double-checking their inputs and being reminded of what they had already entered. One participant in S2 mentioned that they were unsure what data from them is actually being used because they were unable to see it in the Blurry mock-up. This enabled the Clear mock-up to score positively and the Blurry mock-up negatively, with respect to this code.

S3-P2: "I felt that I was not a hundred percent sure if my input is correctly reflected because it was blurred."

S3-P3: "It was more effective because it displayed the numbers that I had entered. I know it might not be the most secure one but it was the best because when I reached the third offer that I'm going to place, I was remembering what I entered before. Having the ability to see it gave me a reminder so I could actually make a correct input. So this was like a double-check and I think it was very beneficial."

7.3 Security

From the results of the interviews, two categories formed the theme of security. These were the use of explicit textual information and insecurity in data repetition. While the Clear mock-up was the winner in the trust theme, the Disclaimer mock-up took the lead in terms of security. Certain aspects were considered important by participants which generated feelings of being secure and the Disclaimer mock-up generated high positive feelings among the participants with regards to security aspects. The reasons involved having explicit information about security and data protection, having this information made it easy to follow, feeling of being safe, being well-informed about the process and the ability to research about the system by themselves. While this category rated the Disclaimer mock-up positively, complementarily the next category (insecurity in data repetition) rated the Blurry and Clear mock-ups negatively.

The Blurry and Clear mock-ups made participants feel insecure due to the repetition of their data. This is a negative category for security which prompted the participants to express their dislike towards the Blurry and Clear mock-ups. This involved people finding the data repetition to be unnecessary, the increased possibility of their data being hacked, feeling disturbed, being unable to understand the visuals of the Blurry and Clear mock-ups without any supporting text and the possibility of industrial espionage. These two categories together also

holistically explain why people felt secure and at the same time, insecure about a potential platform. While the Disclaimer mock-up scored a high +24 due to participants' positive mentions, the Blurry and Clear mock-ups scored -7 and -12 respectively, owing to their negative mentions. This proved that having all the information about the process is vital for finding a mock-up secure, such as the Disclaimer. For security, the Blurry and Clear mock-ups did not score positively even once.

7.3.1 Use of explicit textual information

This category consists of five codes. These are "explicit information about security and data protection", "MPC information made it easy to follow", "MPC information felt safe", "explanation of the process" and "ability to research by yourself". This is a positive category influencing security. All the codes in this category are related to the presence of the information in the Disclaimer mock-up.

7.3.1.1 Explicit information about security and data protection

This was the most discussed code overall, discussed by seven of nine participants. It was mentioned a total of thirteen times wherein the Disclaimer mock-up was preferred twelve times and the Blurry and Clear mock-ups were negatively picked once each. The participants mentioned that they felt unworried and well-informed through the Disclaimer mock-up as it clearly talked about security through text. This allowed them to have an understanding before-hand about the security and data protection of the new platform. Participants liked that they could explicitly read what the security of the new system is, especially when their inputs are confidential. It was also mentioned that the Blurry and Clear mock-ups are more implicit in this sense, leaving the participants to perceive the security and data protection information visually by themselves.

Interestingly, while the disclaimer text prompted doubts about the intent of the supplier, conversely, in terms of security, the text prompted positive feelings. This trade-off between trust and security is further discussed in the next chapter. Concisely, while trust is enhanced by displaying transparency through the interface, users feel more secure when they are informed via text about the security and data protection. A combination of transparency in encryption and information via text is required in order for users to trust the platform and thus, the supplier, as well as feel secure while using the platform.

S1-P2: "I would use it because it explains the security and technology behind it so that I get an understanding of what is happening with my data afterwards."

S1-P3: "I like one the most because it told me how security is being done."

S2-P1:"It clearly states that the data is safe and that you don't have to worry about security."

S2-P3: "I like the information and instructions about security issues."

7.3.1.2 MPC information made it easy to follow

Linking back to the previous code, the presence of explicit information of the security and data protection led to one participant feeling that it was easier to use the Disclaimer mock-up over the other two. They described it as a good feeling as a consequence of having this information explicitly presented to them before-hand. The use of the symbolic lock also helped in understanding the encryption process. This concept was only discussed once, in S2.

S2-P3: "It was mostly just a feeling because when I looked at the other two interfaces, I first looked at the numbers and I thought okay, I have to do something with it. Whereas on this interface, I first looked at the instructions and the symbol. Only then I looked at the numbers and it was fine for me and it was easier to then fill in the data."

7.3.1.3 MPC information felt safe

As a consequence of the explicit information via text, a participant of S2 mentioned that they felt safe and confident. They were confident of the security of the platform and believed this aspect because of the disclaimer and the lock. Hence, this participant chose the Disclaimer mock-up.

S2-P3: "The instructions gave me a good feeling. I felt confident and safe"

7.3.1.4 Explanation of process

This code is different from the first one in this category because it talks about the explanation of the new process, while the first code discusses the information about the security aspects. On the other hand, this factor was mentioned by four participants, nine times. They chose the Disclaimer mock-up eight times here and negatively picked the Blurry and Clear mock-ups as they provided not enough information about the process of the new system. Conversely, the Disclaimer mock-up provided clarity on the process, one step ahead of the security details. It gave information regarding the outcome which helped the participants to know what is happening with their data, process-wise.

S2-P3: "I chose it because of the clarity and security issues."

S3-P1: "I put more weight on security and data protection. Another advantage is that it tells you how the outcome is calculated."

S3-P1: "In the other two interfaces, it's implicit how the outcome is calculated. That's why I didn't believe it. Here, it's explicit. I believe something explicit more than something implicit which is how it describes how the output is calculated."

7.3.1.5 Ability to research by yourself

Participants felt that having explicit information about the technology allowed them the freedom and the possibility of doing some research about it by themselves, to make an informed decision about whether they really believe it is secure or not. They also got an insight

into the new platform through this text. This factor was discussed twice in S1 by one participant, leading to +2 points for the Disclaimer mock-up.

S1-P2: "I get some insight and maybe I can check on my own when I know which technology is behind it. I can research again if I really believe this."

S1-P2: "If I know what it is, I will definitely research what the technology behind it is."

7.3.2 Insecurity in data repetition

This category also consists of five codes. These are "unnecessary repetition reducing security", "increased hacking possibility due to multiple data paths", "disturbing", "tricky visuals without information" and "industrial espionage". This is a negative category influencing security. All the codes in this category relate to negative feelings, all prompted due to the repetition of their data on the interface.

7.3.2.1 Unnecessary repetition reducing security

This issue was discussed five times by four participants. In this, the Blurry and Clear mock-ups were negatively discussed one and five times respectively. Participants believed that it was useless and unnecessary to have their inputs reflected one more time on the right-hand side panel. They did not see the point of this and would rather have it only once on the left-hand side like in the Disclaimer mock-up.

S1-P1: "I didn't really like it because it shows exactly the same thing on the two panels. So on the security level, I could not see the point of having the same information twice on the screen. It even felt less secure."

S1-P3: "There is no benefit at all to show on the right-hand side what they already keyed in on the left. It is about this information which is useless because I already have it on the left-hand side."

7.3.2.2 Increased hacking possibility due to multiple data paths

A participant from S2 elaborately discussed the insecurity related to the multiple streams of data. They explained that transferring the data from the input screen for computation is already one stream of data. However, if before computation these inputs are transferred to be reflected on the right-hand side panel, it gives hackers or security breaches another possible data stream to act upon. This was expressed as a disadvantage through data repetition for the Blurry and Clear mock-ups once each.

S1-P2: "It would take some process or processes to get the data from my inputs to the right panel screen and that's an additional path of my data which can be hacked. So if my data is just placed from my input to the storage place, it's one path of the data which can be potentially insecure but then if it's transferred from the storage place to the screen, it's a second stream of the data. So two streams of the data are obviously less secure than one stream."

7.3.2.3 Disturbing

One participant of S1 expressed their feelings of being disturbed because of excess information in the Clear mock-up. They discussed that it did not help them but rather was excess information and repetition of their data, causing them to feel disturbed in this scenario. They scored the Clear mock-up negatively due to this reason.

S1-P3: "I think I see additional information here and it is more disturbing for me."

7.3.2.4 Tricky visuals without information

Three participants mentioned thrice totally that the visuals of the Blurry and Clear mock-ups were confusing and tricky to figure out as they were mere repetitions, not supported by any text. They expressed that the image of the computation which appears on the "computing" screen (Fig_of_Appendix 16) was confusing here because they were unsure whether their inputs have been accounted for and the computation is in process, or if it was just another sign for security. Another participant mentioned that they had an instinctive feeling due to the greyed out cells that their data is protected in the Blurry mock-up, however, they were not sure whether to believe it or not because it is not reinforced through text that explicitly states the security element.

This same participant also expressed another interesting notion where they thought that the grid on the right-hand side panel in the Blurry and Clear mock-ups was how the manufacturer (instead of fellow customers) was able to view their inputs. They mentioned it would be easier to understand if it is explicitly stated that the manufacturer cannot see your inputs and that they are confidential, instead of only replicating their inputs. For these reasons, the Blurry and Clear mock-ups scored negatively, -3 and -2 respectively.

S2-P3: "There was this sign that was a bit misleading for me because I didn't know if the auction options are fixed now due to the sign, or if it's a sign for security. It was a bit tricky for me."

S3-P1: "I had a gut feeling that the data is protected but this is not explicit. So it is a good feeling because it is blurred even though it's repeated, but there is no statement that says my data is not going to be shared."

S3-P1: "I thought that these blurred inputs are from the perspective of the supplier. That you could see my input. That I could see the input that you could also see."

7.3.2.5 Industrial espionage

One participant in S1 discussed the issue of industrial espionage that can occur due to the repetition of the input data on the right-hand side panel of the Clear mock-up. They explained that in case someone is using the new platform in a busy environment, it is very easy to peek over and see the repeated data. This is confidential information for the distributors and they would not want this data to be leaked under any circumstances. Hence, they argued that it was unnecessary to have the data repeated on the right-hand side panel and scored the Clear mock-up negatively for this.

S1-P1: "I guess people would use (the platform) inside the company but imagine you are on a train and you are bidding. You don't want people next to you to see the numbers. You don't want to show it again. A lot of industrial espionage is of these kinds."

7.4 Extent of control

The extent of control theme was newly formed based on the interview results. We thought it to be best to not include it under one of the pre-determined themes of trust, security, perceived usefulness, perceived ease of use and the intention to use. This is because the participant's feelings regarding this theme and its categories did not affect their trust or security in the platform/manufacturer. These discussions were more about how they felt about the amount of information presented to them in each of the mock-ups and thus, how much they felt in control of the situation with each of these varying mock-ups. Consequently, certain mock-ups performed better than the others for justified reasons. This topic was elaborately discussed when the last interview question was asked, in order to allow room for adding any additional comments and discussing feelings that were not previously addressed. One participant in the first session also linked this to the intention to use, where they mentioned that the presence of competitors has a negative effect on their intent to use the Blurry and Clear mock-ups as it pushes their bids. However, this was only a secondary reason where the primary choice was indifference between the mock-ups.

Two categories formed this theme. These were competition induced stress and the feeling of being in control. Unlike the previous two themes, the categories of this theme do not complement each other directly. Instead, they discuss the same idea but from two different perspectives. For one, the information about competitors is perceived negatively, and in the other category, this is seen as a positive.

In this theme, the Blurry and Clear mock-ups were scored similarly, with the Blurry and Clear mock-ups finishing at +4. This was because these mock-ups made the participants feel like they were in control, they could monitor their competitors' advancement and they were assured about their products' market demand. The Disclaimer mock-up was negatively picked once for not showing competitors' advancement, ending at -1.

7.4.1 Competition induced stress

This category discusses the negative effect that showing competitors' information has on the participants. It consists of one code about competition induced stress. This category negatively influences the theme of control.

7.4.1.1 Competitors push bids

Two participants mentioned a total of three times that they disliked the extra information about their competitors in the Blurry and Clear mock-ups. This refers to the grids on the right-hand side panel where they saw information about their competitors. Having this information pressurized and pushed them to increase their bid prices further. The participants expressed that they knew in the back of their minds that competition exists in the Disclaimer mock-up as well, but it was too direct in the Blurry and Clear mock-ups, making them feel stressed. It was

also mentioned that showing such information of competitors looked like a marketing gimmick by the manufacturer where they are trying to promote their products through such tactics. This was perceived as a disadvantage and the Blurry and Clear mock-ups were negatively scored -3 each.

S1-P2: "I did not really like the number of competitors that was provided on the two interfaces because it made me increase my prices. I know that there are some competitors in the other interface too but here it's obviously shown to me. It makes me feel like oh, maybe you should raise your price a little bit more otherwise you won't get what you need."

S1-P2: "The process is a little bit easier in the other interface when I don't have information about the competitors. If I see competitors then I start thinking if it is a marketing strategy to make people think about how many competitors they have. Like booking.com when they write the last two rooms available on our website."

S2-P3: "If I see that there are other customers too I have the feeling of being pushed."

7.4.2 Feeling of being in control by the presence of information

This category consists of three codes, "feeling of being in control", "competitor advancement" and "assurance in market demand". This category positively influences the theme. The codes are grouped together on the basis of the effects that the presence of information has on the users' feelings about their control of the new system.

7.4.2.1 Feeling of being in control

This code relates to the positive feeling of being in control of the new scenario of revenue management and the auction, due to additional visual information about what the other customer are doing. It relates to users being well-informed about the new system holistically, by being presented extra information in addition to their own inputs.

Three participants discussed that the extra information on the right-hand side panels of the Blurry and Clear mock-ups allowed them to feel in control of the whole process. Having this visual information of the setting made them feel that the more information they see, they more in control they feel. It was a value addition for these participants, and they scored both the Blurry and Clear mock-ups +2.

S1-P1: "The more information I have, the more I feel in control, like knowing the number of competitors."

S1-P3: "It was the best one because I could concentrate on my doing and I got some light information on the right-hand side."

7.4.2.2 Competitor advancement

This was another elaborately discussed code by five of the nine participants. They expressed this issue seven times in total. The notion revolved around the positive feeling knowing their

competitors' advancement. They thought it was an honest way to show the holistic view of the setting where you know how many customers are competing with you. One participant particularly pointed this out as a negative point for the Disclaimer mock-up, where they expressed that they were unable to see how many customers they were competing with. They missed this information and considered it necessary to know so that they could estimate the chance they stand of winning their bid (or not). As the Blurry and Clear mock-ups provided this visual information, the participants scored those +4 and +3 respectively.

S1-P1: "*Knowing how advanced competitors are can be interesting."*

S2-P2: "I see in an honest way that some other customers are interested in the products."

S2-P1: "I like to see how many customers are competing with you."

S2-P1: "You don't really see how many competitors you are competing with. So it's tricky to guess how big your chances are and with how many people you're competing."

7.4.2.3 Assurance in market demand

This idea was mentioned by one participant in S3 and it positively influences the feeling of being in control. The participant discussed that they liked the information about their competitors because they could infer that there is a good enough market demand for the product if there are others competing for it as well. Had they not had the information about their competitors and were to bid in isolation as in the Disclaimer mock-up, they would bid very low prices knowing that they are the only buyer for the product. In relation to the issue of competitors pushing bids higher, they mentioned that they do not mind paying extra knowing that they definitely would get the product. They would be accessing this new platform in the first place knowing well that they need a product on short notice, and they would go the extra mile to acquire the product. Hence, they would like to be well informed about the information on how many others are competing for the same product so they can estimate their bids accordingly and realize the market demand of the product they are interested in.

S3-P2: "Because other suppliers are also interested in this product, I could be sure that there is enough market demand for it. If it's only me, I would write down a very low price because I know that I am the only buyer."

We present a summary of our findings below, segregated by the three concepts that were involved when participants evaluated the three artefacts. Positive numbers suggest the number of times participants mentioned the indicated mock-up positively with regards to the factor associated with it. On the other hand, negative numbers indicate the number of times that the participants expressed their dislike towards the indicated mock-up with regards to the factor.

To sum up our findings, the Clear mock-up performed the best in terms of trust and the Disclaimer mock-up performed the best in terms of security. In terms of perceived extent of control, the Blurry and Clear mock-ups had a similar performance, however, since the Blurry mock-up performs comparatively poorly in all the other categories, the Clear mock-up is the

winner in the Control theme. These findings are summarised with respect to the three factors (trust, security and the extent of control) as well as the choice of mock-up accordingly, below:

Table 5: Comparison of mock-ups with respect to trust

	Factors	Platform mock-ups		
		Disclaimer	Blurry	Clear
Trust	Unfair treatment (against competitors)	-1	-2	-2
	Dubious/malicious intent of the supplier	-4	-3	-1
	Lack of trust in the disclaimer by the supplier	-5	x	x
	Suspicious	-3	-2	x
	Visuals induce confidence (in encryption)	x	+9	+1
	Transparency	-1	x	+8
	Honesty	x	x	+3
	Assurance of inputs	x	-1	+3
		-14	+1	**+12**

Table 6: Comparison of mock-ups with respect to security

	Factors	Platform mock-ups		
		Disclaimer	Blurry	Clear
Security	Explicit information about security and data protection	+12	-1	-1
	MPC information makes the process easy to follow	+1	x	x
	MPC information feels safe	+1	x	x
	Explanation of the process	+8	-1	-1
	Ability and freedom to search	+2	0	0
	Unnecessary repetition reducing security	x	-1	-5
	Increased hacking possibility due to multiple data paths	x	-1	-1
	Disturbing effect	x	x	-1
	Tricky visuals without information	x	-3	-2
	Industrial espionage	x	x	-1
		24	-7	-12

Table 7: Comparison of mock-ups with respect to control

	Factors	Platform mock-ups		
		Disclaimer	Blurry	Clear
Extent of control	Competitors push the bids	x	-3	-3
	Feeling of being in control	x	+2	+2
	Competitor advancement	-1	+4	+4
	Assurance in market demand	x	+1	+1
		-1	4	**4**

Lastly, as discussed earlier, the participants were indifferent between the artefacts when questioned about the perceived usefulness, perceived ease of use and intention to use. Feelings about perceived usefulness, perceived ease of use and intention to use were not discussed elaborately as the participants were not real customers. The answers were rather superficial as the participants did not have enough expertise to compare the perceived usefulness, perceived ease of use and to comment on the intention to use these mock-ups. Instead, discussions about these concepts entailed a general dialogue about RM as well as its usefulness and barriers. Therefore, no choices were made with regard to a particular mock-up while discussing these concepts. These general discussions do not help in answering our research question of how users perceive the visual integration of RM and MPC with regards to trust and acceptance. Real customers in the business are more likely to scrutinize the perceived usefulness, perceived ease of use and the intention to use. Furthermore, the barriers to the implementation of RM have previously already been researched by Garcia (2018). Concisely, because the logic and functionality of all the three mock-ups were the same and they differed only visually, participants expressed that all the mock-ups were equally useful in terms of the introduction of revenue management (or not), equally easy to use with the integration of RM and MPC, and participants had the same intention to use such an integration of the two paradigms (or not) across any of the three mock-ups.

8. Discussion

In this chapter, we discuss and summarize the results from Chapter 7, propose a visual integration of RM and MPC and discuss the foundation of LTBP, which is required to implement RM.

Through this research, we develop and evaluate three platform mock-ups that visualize RM and MPC for the first time. Essentially, it is important to understand how the platform can enhance or hamper feelings of trust, security and control in order to facilitate acceptance. The evaluation of the artefacts reveals that the nine participants are able to choose and discuss for and against factors related to acceptance of the artefacts designed in this research. Through the semi-structured interviews related to acceptance, participants discuss their diverse views pertaining to both positive and negative feelings. In fact, most of these feelings are expressed independently in more than one session, signifying the validity of the evaluation.

Revenue management and multi-party computation both have great potential should they be adopted. RM allows manufacturers to capitalize on missed revenues by selling unallocated ATP and also allows customers to get faster deliveries. Similarly, MPC enables getting rid of a trusted third party, thus, enhancing the security aspects of the platform. In a competitive industry such as the semiconductor industry, it is vital to maintain a long-lasting supplier-customer relationship. Therefore, the potential future platform must facilitate customer acceptance. In this respect, it is necessary to understand how a possible implementation of these two technologies (RM and MPC) could look like and how customers perceive the integration of RM and MPC technology on a platform. Visualizing a potential implementation of this platform and understanding the effect that usability design principles have on customers, is the first step. The following table lists our findings of the key attributes that enhance and hamper stimulating the feelings of trust, security and control:

Table 8: Positive and negative attributes that influence trust, security and control

Finding	Positive attributes	Negative attributes
Trust	Visuals guiding customers through the process	Feelings of being unfairly treated against other customers
	Transparency	The malicious intent of the manufacturer
	Honesty	Information through text without being supported by visuals
	The reassurance of customers' inputs	Being suspicious of the system
Security	Explicit information about security and data protection	The unnecessary repetition of data
	Having the information presented in an easy to follow manner	The increased possibility of hacking
	Feeling safe due to the text	A disturbing effect
	Explanation of the process	Information through visuals without being supported by a text

	The freedom and ability to research about the technology	The possibilities of industrial espionage
Extent of Control	The feeling of being in control	Competition induced stress
	Knowledge about their competitors' advancement	
	The assurance in market demand	

To summarize our findings, we discover that positive feelings regarding **trust** in the system and implicitly, also the supplier (being the owner of the system) come from transparency through visuals in the platform. This is also seen in past studies, where Whitten & Tygar (1999) discuss that users have more confidence in security when the encryption element is transparent. Additionally, Turner (2002) discusses that the quality of a website's visual presentation is the best predictor of gauging users' trustworthiness in an online secure environment. Then, trust in such an environment characterizes how much faith users have not only in the software but also in the owner of the software (Whitten & Tygar, 1999). Correspondingly, our results show that trust is composed of positive and negative attributes related to the system and the intent of the supplier, who is assumed to be the owner of the platform, similar to the ownership of the current buying platform.

On the other hand, positive feelings pertaining to the **security** of the artefact come from clarity of the security aspects via text. The security aspects were best described by the Disclaimer mock-up. Typically, the identity of secure systems depends on whether users are able to recognize a system to be secure or otherwise. Hence, information communicated via the user interface is of prime importance in order for users to determine the security of a system (Yee, 2002). As discussed by Kainda et al. (2010) and Whitten & Tygar (1999), the graphical representation of locks is heavily used while illustrating cryptographic technology. The symbol of the lock is a straightforward visual metaphor that indicates encryption even for inexperienced, new users. Similarly, the use of this symbol in the Disclaimer mock-up facilitated users in understanding the security concepts intuitively. As users constantly search for indicators that signify the security of the system (Kainda et al., 2010), the lock and explicit text in the Disclaimer mock-up enabled users to understand the security aspect more thoroughly than the other mock-ups. However, the unnecessary repetition of data and the increased possibility of hacking due to this, may not be an accurate representation of the real world, as customers' real data would already be transmitted through multiple paths, as explained due to the concept of "reserved ATP" in Chapter 8. This means that customers bids would be under consideration for a certain timeframe, until either a better bid comes along, or the time expires. Showcasing encrypted (blurry) data on the interface hence, does not have a significant effect on the possibility of hacking in comparison to the multiple transmission of this data at the backend as it is.

It is worth discussing that the use of explicit text (as in the Disclaimer mock-up) on the one hand, increases users' perception of security of the system, however, at the same time, users' trust decreased in the supplier due to the explicit text. Participants believe the system to be more secure if they are well-informed about the security element of the system and are briefly informed about the process. However, they believe that this could be a gimmick by the supplier and not everything that is written should be trusted on the interface. This trade-off between trust and security implies that users prefer to visibly see what happens to their data in order

to trust the system and supplier (transparency), but they would also like to be informed in text what the new system entails, prior to the process. In the real world, as distributors already have a well-established relationship with the supplier, it is possible that the “trust in supplier” aspect is not as crucial as the “trust in system” aspect, as the distributors already maintain a healthy relationship with the supplier, implying their trust in them. As distributors are well aware of the business practices of the supplier, presenting a text via the Disclaimer mock-up to them, for instance, would enhance their perceptions of security (as shown in our study), but may not negatively affect the “trust in supplier” aspect as much, even though it is found in our study.

Transparency of the platform is key and this is the reason the Clear mock-up was the winner in **trust and control** both. People feel most in **control** of the platform with the support of visuals through the process, informing them of the setting and their competitors. This situation is realistic with regards to multi-party computation where it is crucial that the inputs themselves remain protected. Having this feature does not violate other users’ confidentiality because the grid merely shows the progress of the competitors, without any specific names or values. This is the foundation of multi-party computation, where the data itself is not revealed despite knowing the basic information of how many other parties are participating in the protocol.

Furthermore, it is realistic while considering products in high demand. This is because users will be able to see how many fellow customers are interested in, or are placing bids for a certain product, they can be assured of the market demand for this product and can raise their prices according to how urgently they need this product. Without this information about competitors, there are higher chances that distributors would not place high bids, leading to not winning the offer. In that case, receiving the default offer could cause frustration in this scenario. On the other hand, users may not like to bid against other customers and may expect to be served with priority based on their individual healthy relationship with their supplier. Therefore, when the information about competitors is implicit (like in the Disclaimer mock-up), it may lead to a more positive experience with the bidding process for customers, in comparison to when they explicitly see that others are also interested in the same product. Moreover, the grid for competitor advancement can be perceived by customers as a mere marketing gimmick which may seem to be unsuitable for the business-to-business sector.

The three artefacts that we use in this research are designed in a manner such that the individual effect of text, encrypted visuals and transparent visuals can be evaluated independently. It is necessary to not compromise on one attribute and focus on the others because this could reduce the acceptance of the platform. Studies have shown that evaluation of usability and security, both need to be considered while designing such systems (Kainda et al., 2010). As implementers consider security and usability as add-on features of a completed product, security and usability are subject to be seen as two clashing notions with the belief that improving one of them affects the other negatively. However, it is crucial that the security community integrates key HCI thinking about people-centred design.

Nevertheless, as per the results of our study, a trade-off is required between usability and security features, as previously also proven by Gunson et al. (2011). While text and symbolic representation (Disclaimer mock-up) increase users’ perception of security, transparency is equally important in fostering feelings of trust and control. Essentially, security and usability go together, and it is crucial to consider them both while designing and evaluating a system. It then follows that to foster feelings of trust, security and control altogether, text and visuals

need to be appropriately combined. Furthermore, we see that it is idealistic and impractical to expect a system to attain maximum usability and security, as also elaborated by Kainda et al. (2010). While transparency facilitates trust and control, it also induces stress due to competitors. Similarly, while the explicit text and padlock representation facilitates perception of security, it lacks the transparency in visualizing encryption. Therefore, such systems involve a trade-off between security and usability. Manufacturers would need to assess the weight they would like to give to each of the three themes. While trust requires visual indicators and the ability for customers to follow the process in order to trust the system and the supplier, security requires a brief explanation of the security and the process. This trade-off needs to be further studied to establish the relationship between them.

It is a compelling need to make security comprehensible for new users. Several cryptographic implementations are unsuccessful because users are unable to comprehend security-relevant user interfaces (Smith, 2003). Therefore, we pay attention to the human factor of a security system, as discussed by Patrick et al., (2003). At the same time, security should not be perceived as a secondary goal while designing a new system (Whitten & Tygar, 1999) as it is easy for users to ignore the security aspects of the system, or assume that their security is working accurately while they focus on their main goal, which is placing bids in the case of revenue management. Consequently, we represent the security aspects of multi-party computation in various ways, so as to communicate the security elements of the technology while assessing users' trust in the system and supplier and its acceptance.

Following our results from Chapter 7, a potential RM with MPC platform is proposed below. This includes the positive elements for trust (transparency), security (clarity and explanation) and control (competitors' advancement):

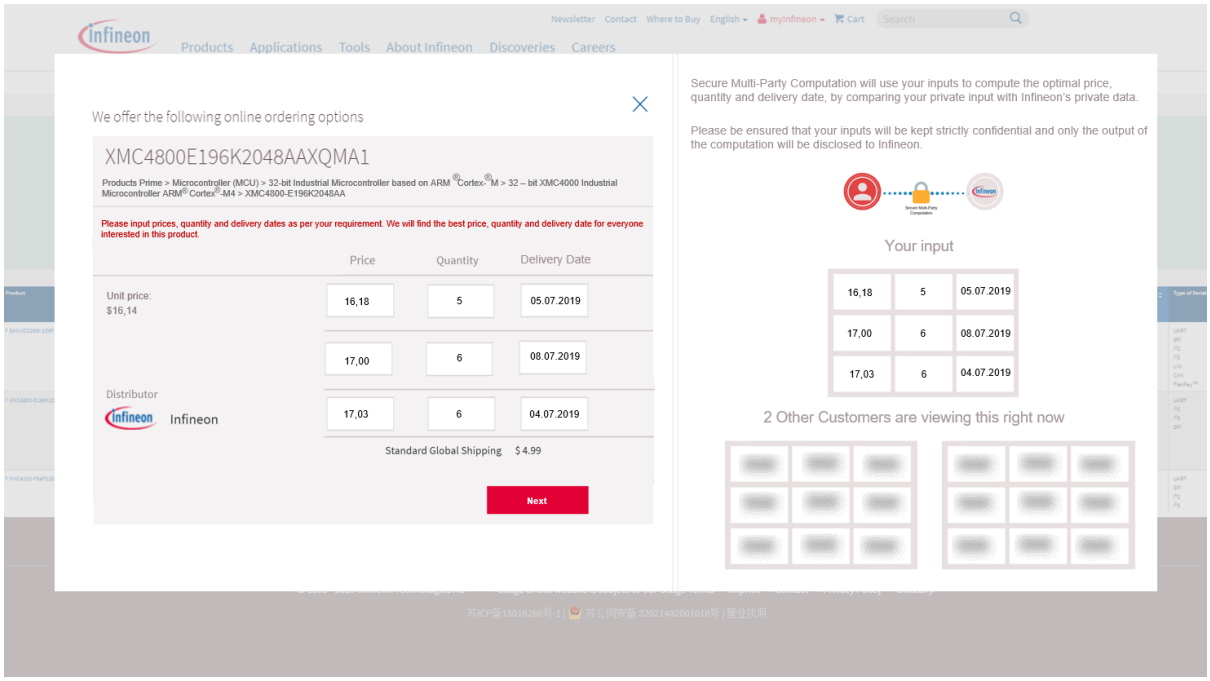


Fig 27: Proposed platform design for RM with MPC to facilitate trust, security and control

The above-proposed platform is a combination of the Disclaimer and Clear mock-ups developed in this research as they evidently prompted positive feelings of trust, security and control altogether. This can be seen in Table 4, wherein the Clear mock-up was highly

preferred with regards to trust due to the transparent visuals, the Disclaimer mock-up was highly preferred with regards to security due to the explicit text, and the Clear mock-up tied with the Blurry mock-up with respect to the extent of control due to the complete knowledge of the auction setting. We disregard the Blurry mock-up because it was fared poorly by the participants in the other two important themes of trust and security because the cells greying out with their inputs was perceived to be suspicious. The concept of combining these two mock-ups was interestingly also raised by one of the participants in Session 1. They discussed that the security aspects of the Disclaimer mock-up were precise while the competitors' information is equally important. Comprehensively, the Disclaimer mock-up prompted positive feelings related to security, the Clear mock-up prompted positive feelings in trust and control. Therefore, the proposed potential platform that is most likely to be positively perceived by customers with regards to trust, security and control, is a combination of the two.

Through the research, it is also established that the LTBP and MPC algorithms need to be developed further for understanding the acceptance of these and incorporating them in the platform. The initiative of LTBP is only at a very initial stage and MPC is yet to be practically implemented. To assess the realistic acceptance of such a platform, both these technologies must be advanced. On the basis of the developed mock-ups through this research, we initiated a preliminary discussion session to get the conceptualization of the LTBP started.

After initial discussions with the leaders of Work Package 5 who directly deal with MPC (SafeDEED, 2018), a potential framework for the LTBP algorithm is proposed with the establishment of a "dynamic price adder range" (Fig 28**Error! Reference source not found.**). This would include a minimum and maximum price set by the manufacturer depending on their daily free ATP. If a customer bids with a price lower than that of the minimum price, the order is rejected and a default option is provided by the manufacturer. In case the customer bids with a price higher than that of the maximum price set by the manufacturer, this order is immediately confirmed. For orders that are in the range of the minimum and maximum prices, the concept of response time would be taken into account. This means that the manufacturer can confirm the customer's order at any time between the time the order is placed, until 48 hours. The closer the bid is to the maximum price, the faster the order can be confirmed. Once a customer places an order between the price range, the volume they ordered is theoretically taken away from the free ATP and held in the reserved ATP until a higher bid comes along (Fig 29**Error! Reference source not found.**). If a higher bid comes along within the defined time frame (48 hours), the original bidder is contacted with the rejected receipt along with a default option for purchase. If a higher bidder does not come along, the original bidder is contacted with the successful order after the time frame expires (dependent on how close the price is to the maximum desired price from the manufacturer).

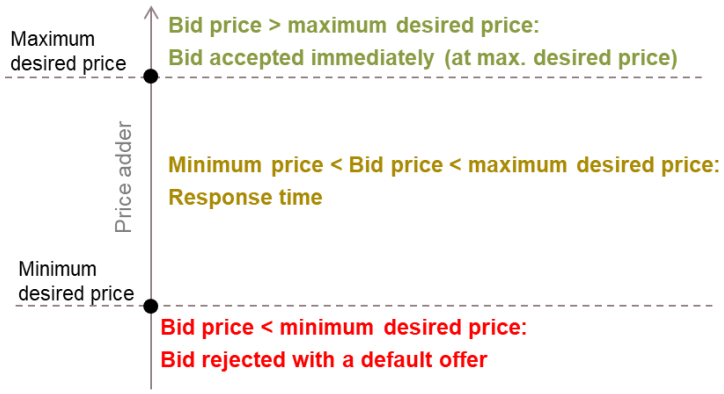


Fig 28: Dynamic price adder set by the manufacturer

The idea behind this concept of the LTBP algorithm is that if a customer urgently requires a certain product, they would bid with a high price in an effort to have their order confirmed immediately. The new system would be communicated to the customers before-hand so that they can assess the importance of having certain products immediately. If they can afford to wait and accept the risk of losing the bid, they can bid with a lower price accordingly. In the case when the bid price is greater than the maximum desired price of the manufacturer, the offer is capped at the maximum price set by the manufacturer. This is to keep the system stable and prevent exceptional rises. This overall functionality of LTBP is aligned with MPC because the maximum price that customers would be willing to pay is confidential for them. Similarly, information about the free ATP is confidential for manufacturers. Using both these data to compute an outcome while keeping them confidential would be of great interest to manufacturers and customers both.

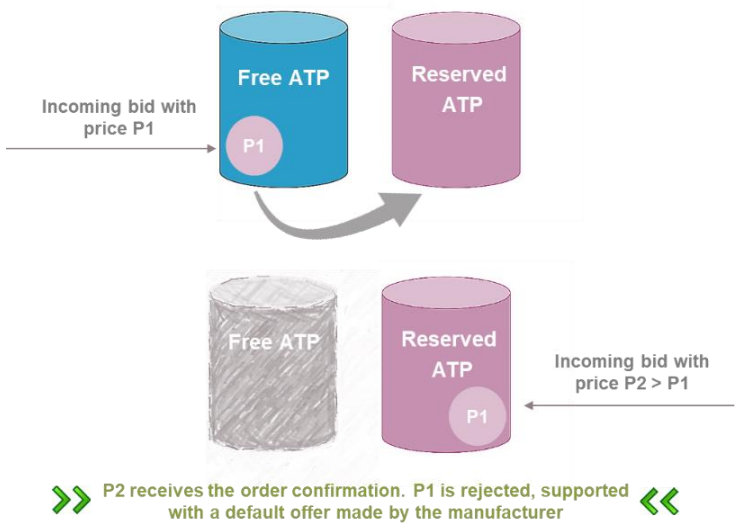


Fig 29: Concept of reserved ATP

9. Limitations

In this chapter, we reflect on our study from a holistic perspective. We discuss the limitations of our study concerning the sample, the simplifications made and the methodology.

Firstly, students who work in the Supply Chain and Innovations Department at Infineon were involved as participants for the evaluation of the artefacts instead of distributor customers from the real world. While access to distributors is important, manufacturers find maintaining a healthy supplier-manufacturer relationship more important for the business. A healthy relationship is vital to survive in this industry and any mistakes could cost manufacturers their reputation in an already tough market with small margins. Consequently, we were not given access to real customers for our research. Furthermore, there is a general misconception regarding a small sample size, where it is thought that the smaller the sample size, the less is the research depth. However, our sample size of nine participants is considered sufficient for usability research. Hwang & Salvendy (2010) show that the general rule for an optimal sample size for usability research is 10 ± 2 participants. After analyzing several research papers to devise a general rule for sample size, they discuss that with these many evaluators, research can reach 80% overall discovery rate. While our sample size of nine participants is aligned with this rule, the majority overlap in the results of the three sessions during evaluation further shows reasonable validity of the results.

Next, this research uses the developed platform mock-ups for evaluation. Since these are mock-ups and not functional platforms, the systems are not connected. While each session consisted of three participants each, their systems were not connected in any way. Connected systems will allow for more realistically gauging users' trust in the system and supplier as well as acceptance of the platform through the varying visual interfaces. This is because users would be able to see changes in the number of fellow interested customers and their advancement in real time in the mock-ups Blurry and Clear. Therefore, having them connected in reality to perform MPC may bring several other factors into play. For instance, when the auction scenario for RM is represented more realistically with connected systems, principles of game theory will surface. Coalitions of small customers could be formed to model one big customer. This will allow them to get an overall lower price. MPC will be valuable in this case, wherein there are several parties involved and every small customer's data is confidential and also decides the outcome of the computation. This can be further researched once the algorithm for MPC for the RM use case is more developed, beyond the conceptual stage that it is at currently.

Similar to the MPC algorithm for RM, the lead time-based pricing algorithm is also not yet developed and it is the foundation of RM. Once this pricing algorithm is developed, customer acceptance of the platform could be more realistically studied regarding the prices that manufacturers are expecting in return for their products, and the maximum price that customers are willing to pay for these. While this research provides the first step into understanding how a potential platform may look like, and what effect this has on customers with regards to acceptance, research can build on this to further evaluate these factors with respect to the LTBP and MPC algorithms.

Another point of discussion is that while participants evaluate the mock-ups and choose their preferred ones supported with reasons and justification, this research does not measure the extent they like or dislike a particular mock-up or the extent that a particular mock-up scores on each of the themes (trust, security and control). Additionally, other predictors that may explain customer acceptance of such a platform are not all taken into account due to the relatively short time period of this study. In general, a quantitative approach is constructed utilizing pre-explorative data for the research interest. However, such data was so far, unavailable and is first provided by this research. Due to the limited time and resource constraints of this Master thesis, a quantitative approach could not be further taken to build on the data concluded by the design science research approach. However, our approach aims at providing explorative and qualitative data as a foundation for further generalizing quantitative research. The experimental design for such a research to build on ours, could include a survey that follows once the participants use all the mock-ups. The contents of the survey can be based on the factors that influence trust, security and control (established through our research) in order to determine their causality empirically. Furthermore, the sample size can be increased while conducting such a research, in order to reach precise and representative conclusions.

10. Conclusion and Further Research

10.1 Conclusion

It is vital that customers perceive the new technology positively so that they can trust the system to ensure their best interests, and are able to provide their confidential data. The research question of this study was "*How can multi-party computation be applied to and visualized with revenue management as a platform interface in order to enhance users' trust in the system and supplier, as well as enhance perceptions of security, perceived usefulness, perceived ease of use and intention to use?*" Through the literature review, we first identified the parameters that influence customer acceptance. These include trust, security, perceived usefulness, perceived ease of use and the intention to use the platform. These factors have been previously studied independently and this study reflects on these existing technology acceptance models to study the mentioned concepts together. We designed four artefacts based on requirements through literature review (Table 2) to test for the parameters listed above. In addition to the first artefact which was identical to the current buying platform, we designed three mock-ups, namely, Disclaimer, Blurry and Clear. The Disclaimer mock-up included a description of the new system via text and the representation of cryptographic technology via a padlock, while the Blurry mock-up presented encryption of customers' inputs via visual indicators. Lastly, the Clear mock-up leveraged transparency, by presenting the customers' inputs once again, before they can confirm their inputs.

Through evaluation of the artefacts, we identify positive and negative feelings related to trust, security and the extent of control. Following our findings, we discuss how these feelings foster (for the positive ones) or hamper (for the negative ones) trust, security and control of the platform. Discussions about perceived usefulness, perceived ease of use and intention to use did not generate findings relevant to our research question. Regarding perceived usefulness, one reason may have been due to the misworded interview question.

To answer the main research question, we establish that multi-party computation can be applied to the use case of revenue management after identifying its inputs, outputs and functionality. In order for such an integration (RM and MPC) to be successful in terms of building trust and perceptions of security and control, we find that *using symbols to suggest cryptography, text to explain the technology and transparency in encryption* are key factors. The above-mentioned factors enhance security, trust in the system and supplier as well as enable users to feel like they are in control of the new system, respectively. For the themes of perceived usefulness, perceived ease of use and intention to use, as of yet, we are unable to establish key findings relevant to any specific interface. Taking the above-mentioned factors in to account, we propose a potential RM with MPC platform in Chapter 8.

Furthermore, the sub-questions of our research were:

1. What is MPC and what is its functionality in RM and the use case?
2. What data is required to simulate the result of MPC and what data involved is confidential?

3. What are the different customer types of Infineon and what is the targeted customer segment for participating in RM?
4. What attributes can enhance trust and acceptance?
5. How can the mock-up artefacts be evaluated?

We answer the sub-questions wherein we identified the functionality of MPC for the use case of RM, which in turn provided information about the data that is required from Infineon and the customers for RM and MPC (Fig 17). Through evaluating these artefacts, we find that trust, security and another newly developed theme, the extent of control, influence customers' perception and choice of a certain platform. Our proposed platform design fosters trust, security and control amongst customers (details are presented in Fig 27). Concisely, we conclude our proposed interface to be trustworthy because of the *transparency* that customers' perceive while entering their inputs and confirming that they are recognized accurately through the grid on the right-hand side panel. Moreover, it is secure due to the text *explanation and the pictorial representation of the process below it (padlock)*. Lastly, customers feel they have control over the platform by being well-informed of *their competitors' advancement* and by having knowledge of the setting. To the best of our knowledge, we are the first to provide data to understand what a possible implementation of RM and MPC would look like and how this would be perceived by customers.

It is worth mentioning that this research does not evaluate users' feelings in the technology (multi-party computation) and its functionality itself, but rather in how the cryptographic technology can be visually communicated to users. In order to analyze users' reactions to multi-party computation in action, working interfaces would need to be used for experimentation. On the other hand, our research is another step forward in the field of human-computer interaction and security (HCISec) where it is still a challenge to communicate security technologies to users, and further enable them to trust, use and accept such a system. By defining the application of an upcoming cryptographic technology (MPC) to a real-life use case (RM), we establish how this integration can be communicated to users via mock-up interfaces in order to increase trust in the system and supplier, perceptions of security and control.

10.2 Further Research

In this section, we discuss possible research directions for the future. We suggest approaches for building on our research and empirically understanding the effect of the features on customer acceptance, along with suggesting the ultimate objective of the RM with MPC platform.

Prior to this research, there was little understanding as to how a RM platform with MPC could look like. Our main contribution is to set the foundation related to understanding how this platform could look like, how it is perceived by customers and the concepts underlying the platform's acceptance. While it would be valuable to provide clear-cut advice to practitioners as to how this platform should be designed, the findings of this thesis do not allow this because it requires that the extent that trust, security and control influence customers' acceptance be measured. Quantitative research can be undertaken to statistically validate the extent that trust, security and control influence customer acceptance. Having this research establish the

influence of trust, security and control on evaluating the artefact can help take research to the next stage where the effects of these can be measured.

Further research can be conducted to understand the inter-relationship between these three factors (trust, security and control). While this study has focused on the visual representation of a potential platform, attention could be given to other platform features that could also enhance trust, security and control. Other attributes for platform design such as platform openness, restrictions for participation, ownership, leadership and management practices of running the platform affect the lifecycle of a platform and must be considered when establishing a platform (Tura et al., 2018). Moreover, other several predictors that may explain customer acceptance of such a platform can be studied. The effect of these design principles and other predictors of acceptance with respect to a RM with MPC platform can be further studied to understand how to get the best of these in one platform.

Furthermore, while the platform mock-ups designed and proposed in this research took a single-sided auction scenario, the long-term goal would be to have a marketplace with multiple manufacturers and buyers on either side of the platform. E-marketplaces are online platforms where the owner allows third-party sellers to sell on the platform, the e-marketplace's owner does not own all the inventory, and the platform is for sellers and buyers both (Patel, Qi & Wills, 2010). This would prove more valuable to customers as they can holistically compare the deals offered by different suppliers and consolidate products in the industry that can be delivered on a short notice. It can be further investigated whether this is a suitable step for Infineon to take. Due to the increasing popularity and success of online auction marketplaces, the interest in practical and academic fields of e-marketplaces continues to rise. Thus, the value of customer's trust is key to the success of e-marketplaces, as e-commerce most often involves the sharing of personal, sensitive, corporate and financial data between transacting parties. Fostering this trust remains a significant research issue and a challenge for online businesses (Kim & Ahn, 2007).

The design science research approach usually simplifies a complex challenge by explicitly depicting a subset of the relevant means, ends, and laws or by dividing a challenge into simpler sub-challenges. With time, as means, ends, and laws are refined and made more realistic, the design artefact becomes more relevant and valuable. An effective design science research is a significant step forward towards integrating design science and behavioural science research (Hevner et al., 2004). For this research, the future implementation of a RM platform with MPC was sub-divided into evaluating customer acceptance through designed platform mock-ups by identifying five parameters (trust, security, perceived usefulness, perceived ease of use and intention to use). While such simplifications and divisions may not be realistic enough to significantly and directly impact practice, they serve as a starting point. Using this, progress can be made iteratively as the scope of the design problem is gradually expanded. Once MPC is more developed practically, it will help in applying it realistically to the RM use case. Additionally, this could be combined with behavioural and organizational theories so as to develop an even greater understanding of business challenges, contexts, solutions, and relevant evaluation approaches.

11. Reflection

11.1 Contribution to literature

In order to enhance the usability of secure systems, there is an imperative need for human-computer interaction and security (HCISec) in the field of implementing cryptographic technologies, as also expressed by multiple researchers (Gunson et al., 2011; Kainda et al., 2010). Incorporating usability and security together has remained a challenge in the field of HCISec, and bridging this conceptual and practical gap is critical by integrating these two concepts in order to design and develop usable security interfaces and systems. Consequently, this requirement should motivate the research community to re-examine the design and implementation of secure systems. However, despite the efforts put into this knowledge gap, Kainda et al. (2010) discuss that there are still a significant number of examples of secure systems that are designed while ignoring the value of usability. As Yee (2004) establishes that remarkable improvements can be attained by designing usability and security together, we bridge this knowledge gap by evaluating usability in the context of security as it is crucial to communicate a precise model of the security to users while incorporating factors that facilitate in enhancing trust and acceptance of the system.

Essentially, we contribute to the field of human-computer interaction and security (HCISec) by studying the application of the MPC to the use case of RM in order to identify interface features that enhance users' perceptions of trust, security and control of the security system. We incorporate features of both, security and usability while designing and evaluating this new system (integration of RM and MPC). Firstly, we prove that users perceive security positively through symbolic representation (the padlock) to depict cryptography technology. At the same time, users' trust in the system and implicitly the supplier, is influenced by the transparency of the system. The role of transparency in facilitating and hampering users' perception of the system and supplier has been argued for and against by Whitten & Tygar (1999) and Dourish (2004) respectively. We establish through our study that transparency positively influences users' trust in the system and the supplier. Moreover, users feel in control of the situation when they are presented with information about their competitors. Our findings recognize that the factors that influence customers' acceptance of this technology include the trust (transparency), security (text and symbolic representation) and control (competitor knowledge) of the platform.

Multi-party computation has so far not been visualized to be implemented practically, though it has been extensively studied theoretically. Similarly, the concept of revenue management along with the benefits of implementing it in the manufacturing industry have been well researched, however, the form how revenue management can be potentially implemented has not yet been studied. Through this research, we show that revenue management and multi-party computation can both be implemented in the manufacturing industry through an auction scenario. We further identified the auction setting that would be best suited to both, revenue management as well as multi-party computation. This is the single-sided, multi-attribute, forward, sealed-bid auction. This scenario is single-sided because initially, there is one supplier and multiple customers as buyers. It is multi-attribute because customers bid through price, quantity and delivery dates, instead of only price. It is a forward auction as the supplier

would be selling to several potential buyers who would be competing for the products. Lastly, it is a sealed-bid setting because the customers' bids are confidential, consequently, it is vital that these bids are not revealed to the others.

Additionally, while there is substantial literature on the security aspects and the basic general functionality of multi-party computation, there is a knowledge gap when it comes to its practical applicability to real-life use cases. We apply multi-party computation to a real-life use case, which is revenue management in the manufacturing industry, by identifying the overall functionality, the inputs, outputs of the computation protocol, and the parties involved in the computation. This sets the ground for practically applying MPC in the future for such cases, as this had not been identified so far.

For the next part of our contribution, we are able to design various platform mock-ups using the above functionality (applying MPC to the RM use case). Our design consists of combinations of text and visual representation of the two technologies in an auction setting. We apply visually the theoretical security requirements of the MPC protocol as discussed by Zhao et al. (2019). Thus, we identify the factors that influence the perception of customers with regards to potentially introducing revenue management using multi-party computation. This thesis proposes a potential platform visual implementation of revenue management using multi-party computation for the manufacturing industry. This contributes to the field of HCISec, where multiple researchers have argued (Kainda et al., 2010; Patrick et al., 2003; Whitten & Tygar, 1999) that the knowledge gap between usability and security needs to be bridged. This is an important step in the direction of understanding how customers potentially react to this visual integration of MPC and RM. Based on visual perception, we establish that the platform's acceptance is influenced by people's trust, the notion of security and control in the platform.

Lastly, this research is an important milestone contributing towards the SafeDEED project, where it was yet to be understood how multi-party computation can be applied and visualized for the use case of revenue management. It builds on knowledge and data from three Work Package leaders (Delft University of Technology, the Netherlands, Infineon Technologies AG, Germany and KNOW-Center, Austria). Based on our research, the development of the algorithm for applying MPC to RM can be initiated as we have explicitly identified the inputs, outputs, functionality of the algorithm, the need and use of the pricing algorithm, response time from the manufacturer as well as the use of reserved ATP. In addition to this, we provide the foundation for visualizing and communicating the integration of multi-party computation and revenue management.

However, it is worth questioning whether this research can be used to establish the trust in multi-party computation as a technology in isolation via the design and evaluation of the mock-up artefacts. As the research proposes an integration of RM and MPC, through a platform offered by the manufacturer firm, the factors of trust, security and control can be attributed to the system as a whole, in addition to the trust in the manufacturer. This assumes that the manufacturer owns the new platform, similar to the governance structure of the current buying platform. In reality, independently establishing users' trust in MPC alone is rather challenging because MPC is a tool that enhances the security of computations in use cases where multiple parties are involved, who own confidential data. Essentially, MPC is not a system in itself, but rather it needs to be practically implemented to a use case in order to be used to its potential.

We hope that this first step leads to further research in understanding the practical application of multi-party computation to revenue management as well as in establishing the extent that trust, security and control influence customer acceptance of such a platform. The design and evaluation of the artefacts serve to come one step closer to seeing the implementation of RM using MPC in manufacturing firms.

11.2 Recommendations to Practice

In this section, we elaborate on the recommendations to practitioners who aim to implement revenue management using multi-party computation as a platform technology.

This research builds upon the challenges revolving around customer acceptance of revenue management and multi-party computation. To facilitate acceptance of the technology, practitioners must understand that the value of multi-party computation is at the back-end of the system, which is not visible by the customers. Therefore, to allow customers to understand the technology and its secure aspects, effective visualization of multi-party computation is essential. Similarly, the practical implementation of revenue management is complex and this needs to be simplified at the front-end to facilitate its acceptance.

While the end goal of such a platform would be to have a marketplace with multiple buyers and sellers on either side of the platform, this platform could also be provided by a single manufacturer, where they offer other manufacturers' products as well. It would be worthwhile to investigate whether such a platform would be suitable to introduce and sustain by a single company for the industry.

In addition to this, it would make sense for the manufacturer to own the new platform, similar to the governance of the current buying platform. Since the manufacturer already has an established relationship with its customers, it may be detrimental for the relationship to include a trusted third party or a different owner of the new platform. Furthermore, due to the established healthy manufacturer-customer relationship, it is likely that customers trust the manufacturer's practice of conducting business, proving the foundation in the "trust in supplier" aspect of trust. Leveraging this relationship would further help build trust in the system. Conversely, involving a trusted third party to govern the new platform would dissolve the purpose of multi-party computation. With multi-party computation, manufacturers and customers can be assured that no trusted third party has access to their confidential data. Therefore, for customers to trust the manufacturer's platform with their data, it may be necessary for the manufacturer to have such a disclaimer or include this in the form of terms and conditions.

Moreover, it is worthwhile to discuss the power asymmetry between the client and the supplier. Cool and Henderson (1998) discuss supplier/buyer power as that, what is gained through a favourable position on the market. Their definition of power in the supply chain consists of structural power (the supplier/buyer concentration), attribution power (ability of suppliers/buyers to bargain and the cost of switching suppliers/buyers), dependence power (impact on seller's cost and differentiation), and integration power (incidence of forward integration from suppliers/buyers). Subsequently, Cool and Henderson's (1998) findings showed that buyer power had a much larger effect than supplier power on seller profitability in the supply chain. Additionally, when customers have an advantage on the bargaining power against manufacturers, it gives them a higher power to dictate the conditions of trade or

whether the trade occurs at all (Hui, Klasa & Yeung, 2011). Furthermore, when customers have greater bargaining power, the business bears losses more rapidly. Therefore, in order to enable a more equal collaboration method with the implementation of revenue management, as well as due to the confidentiality involved, a secure technology that involves inputs from multiple parties is required in order to facilitate the implementation of revenue management in the manufacturing industry. Subsequently, multi-party computation is a fair way to compute on the confidential data from the manufacturer as well as the customer. However, it should be made explicit to the customer that the manufacturer is not directly computing on the customers' data themselves. Instead, multi-party computation is an alternative that bypasses giving access to confidential inputs to the manufacturer as well as a trusted third party. Moreover, in order to allow customers to feel like they also get something in return from using multi-party computation, the algorithm can be designed in order to present competitors' advancement to customers, as we have discussed through our research. Undoubtedly, this does not have to include information about fellow customers' names, inputs or any other details. Encrypted data can be previewed in order to communicate to customers that others' are using the platform too, while also simultaneously indicating the market demand of the particular product.

Furthermore, we recommend focusing on facilitating trust, security and control features of the platform so as to foster acceptance. Other platform usability features such as sound, colours or video (Shneiderman, 2018) can also be tested to evaluate their effect on trust, security and control perceptions. As we find that transparent visual indicators enhance trust and control perception of the platform, as well as written text and symbolic (padlock) presentation facilitates the security perception of the platform, it is recommended to keep them both into consideration. The platform mock-up that we propose in Chapter 8, is the integration of the positive attributes from all the mock-up artefacts designed and evaluated in this study. This can be used for further studies once the MPC and LTBP algorithms are developed. Moreover, we suggest that weights are assigned to the importance of trust, security and control by manufacturers, as we have proven the different factors that potentially enhance and hamper these concepts. This would best be understood by experts in the field so that they can effectively combine, or possibly perform a trade-off in order to establish the importance of each of these factors. Through this, factors that foster positive feelings among customers can be emphasized and factors that prompt negative perceptions can be mitigated through the visuals of the platform.

Additionally, it is essential for manufacturers to internally develop the lead time-based pricing algorithm in order to get a more realistic idea about customer perception. Once this is established, the MPC algorithm must be developed in order to be integrated with the LTBP algorithm accordingly. We have proposed the basic functionality of these two algorithms in Chapter 8. Then, a complete working prototype can be tested, based on the results of this study.

Lastly, before manufacturers can implement such a platform, it is important that an equivalent study is performed with real distributor customers. Understanding how distributors think and perceive this platform is vital to evaluate a potential platform. However, this is recommended once the platform is fully developed, namely via including the algorithms at the back-end.

Bibliography

Alsaad, A., Mohamad, R., & Ismail, N. A. (2017). The moderating role of trust in business to business electronic commerce (B2B EC) adoption. *Computers in Human Behavior, 68*, 157-169. doi:10.1016/j.chb.2016.11.040

Bitran, G., & Caldentey, R. (2003). An Overview of Pricing Models for Revenue Management. *Manufacturing & Service Operations Management, 5*(3), 203-229. doi:10.1287/msom.5.3.203.16031

Bogetoft, P., Damgård, I., Jakobsen, T., Nielsen, K., Pagter, J., & Toft, T. (2006). A Practical Implementation of Secure Auctions Based on Multiparty Integer Computation. *Financial Cryptography and Data Security Lecture Notes in Computer Science,* 142-147. doi:10.1007/11889663_10

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2), 77-101. doi:10.1191/1478088706qp063oa

Burmeister, B., Ihde, T., Kittsteiner, T., Moldovanu, B., & Nikutta, J. (2002). A practical approach to multi-attribute auctions. *Proceedings. 13th International Workshop on Database and Expert Systems Applications*. doi:10.1109/dexa.2002.1045975

Chakravarty, A., Kumar, A., & Grewal, R. (2014). Customer Orientation Structure for Internet-Based Business-to-Business Platform Firms. *Journal of Marketing, 78*(5), 1-23. doi:10.1509/jm.12.0442

Chen, W., & Hirschheim, R. (2004). A paradigmatic and methodological examination of information systems research from 1991 to 2001. *Information Systems Journal*, *14*(3), 197-235. doi:10.1111/j.1365-2575.2004.00173.x

Chiang, W. C., Chen, J. C., & Xu, X. (2006). An overview of research on revenue management: current issues and future research. *International journal of revenue management, 1(1),* 97-128

Cleven, A., Gubler, P., & Hüner, K. M. (2009). Design alternatives for the evaluation of design science research artifacts. *Proceedings of the 4th International Conference on Design Science Research in Information Systems and Technology - DESRIST 09*. doi:10.1145/1555619.1555645

Cool, K., & Henderson, J. (1998). Power and firm profitability in supply chains: French manufacturing industry in 1993. *Strategic Management Journal,19*(10), 909-926. doi:10.1002/(sici)1097-0266(199810)19:103.0.co;2-k

Davis, F. (1985). A technology acceptance model for empirically testing new end-user information systems: theory and results. Unpublished Doctoral dissertation, MOT Sloan School of Management, Cambridge, MA.

Dourish, P. (2004). *Where the action is: The foundations of embodied interaction*. Cambridge: MIT Press.

Ehm, H., & Ponsignon, T. (2012). Future research directions for mastering end-to-end semiconductor supply chains. *2012 IEEE International Conference on Automation Science and Engineering (CASE)*. doi:10.1109/coase.2012.6386323

Garcia, D. J. (2018). BM roadmapping approach: overcoming barriers for the implementation of Lead Time Based Pricing (Master's Thesis). Delft University of Technology, Delft, The Netherlands.

Garfinkel, S. L., & Miller, R. C. (2005). Johnny 2. *Proceedings of the 2005 Symposium on Usable Privacy and Security - SOUPS 05*. doi:10.1145/1073001.1073003

Garfinkel, S., Spafford, G., & Schwartz, A. (2003). *Practical UNIX and Internet security*. Beijing: OReilly.

Gefen, D., Karahanna, E., & Straub, D.W. (2003). Trust and TAM in Online Shopping: An Integrated Model. *MIS Quarterly, 27*(1), 51. doi:10.2307/30036519

Gelernter, D. (1989). *Machine Beauty: Elegance and the Heart of Technology*. New York, NY: Basic Books.

Gumussoy, C. A., & Calisir, F. (2009). Understanding factors affecting e-reverse auction use: An integrative approach. *Computers in Human Behavior, 25*(4), 975-988. doi:10.1016/j.chb.2009.04.006

Hevner, A.R., March, S.T., Park, J., & Ram, S. (2004). Design Science in Information Systems Research. *MIS Quarterly, 28*(1), 75. doi:10.2307/25148625

Hevner, A. R. (2007). A Three Cycle View of Design Science Research. *Scandinavian Journal of Information Systems, 19*(2), 87-92.

Hui, K. W., Klasa, S., & Yeung, E. (2011). Corporate Suppliers and Customers and Accounting Conservatism. *SSRN Electronic Journal*. doi:10.2139/ssrn.1426839

Hwang, W., & Salvendy, G. (2010). Number of people required for usability evaluation. *Communications of the ACM,53*(5), 130. doi:10.1145/1735223.1735255

Infineon. (2016). *Distribution for COMM*. Retrieved from Infineon internal database.

Infineon. (2018). *Revenue with Distributors*. Retrieved from Infineon internal database.

Infineon. (2019a). *Application of Revenue Management in the Semiconductor Industry with a focus on a Lead time-Based Pricing Strategy*. Retrieved from Infineon internal database.

Infineon. (2019b). *Progress of Lead Time Based Pricing in collaboration with Safe-DEED.* Retreived from Infineon internal database.

Kainda, R., Fléchais, I., & Roscoe, A. (2010). Security and Usability: Analysis and Evaluation. *2010 International Conference on Availability, Reliability and Security*. doi:10.1109/ares.2010.77

Kenton, W. (2018). Reverse Auction. Retrieved from https://www.investopedia.com/terms/r/reverse-auction.asp

Kim, M., & Ahn, J. (2007). Management of Trust in the E-Marketplace: The Role of the Buyers Experience in Building Trust. *Journal of Information Technology, 22*(2), 119-132. doi:10.1057/palgrave.jit.2000095

Kimes, S. E., & Wirtz, J. (2015). Revenue Management: Advanced Strategies and Tools to Enhance Firm Profitability. *Foundations and Trends® in Marketing, 8*(1), 1-68. doi:10.1561/1700000037

Koppenhagen, N., Gass, O., & Müller, B. (2012). *Design Science Research in Action - Anatomy of Success Critical Activities for Rigor and Relevance*. Barcelona, Spain: 20th European Conference on Information Systems.

Krishna, V. (2002). *Auction theory*. Elsevier.

Lai, P. C. (2016). Design and Security impact on consumers intention to use single platform E-payment. *Interdisciplinary Information Sciences, 22*(1), 111-122. doi:10.4036/iis.2016.r.05

Lai, P.C., & Zainal, A. A. (2015). Consumers' Intention to Use a Single Platform E-Payment System: A Study among Malaysian Internet and Mobile Banking Users. *Journal of Internet Banking and Commerce, 20*(1)m 1-13.

Lapets, A., Volgushev, N., Bestavros, A., Jansen, F., & Varia, M. (2016). Secure multi-party computation for analytics deployed as a lightweight web application. Technical report, Computer Science Department, Boston University

Lin, J. C., & Hsieh, P. (2006). The role of technology readiness in customers perception and adoption of self-service technologies. *International Journal of Service Industry Management, 17*(5), 497-517. doi:10.1108/09564230610689795

Luca, M. (2016). Designing Online Marketplaces: Trust and Reputation Mechanisms. doi:10.3386/w22616

Ma, T. (2008). Pricing Initiatives and their Supply Chain Coordination in Semiconductor Industry (Master's Thesis). Hamburg University of Technology, Hamburg, Germany.

March, J. G., & Shapira, Z. (1987). Managerial Perspectives on Risk and Risk Taking. *Management Science,33*(11), 1404-1418. doi:10.1287/mnsc.33.11.1404

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An Integrative Model of Organizational Trust. *The Academy of Management Review, 20*(3), 709. doi:10.2307/258792

Mcknight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and Validating Trust Measures for e-Commerce: An Integrative Typology. *Information Systems Research,13*(3), 334-359. doi:10.1287/isre.13.3.334.81.

Mohajan, H. K. (2018). Qualitative Research Methodology In Social Sciences And Related Subjects. *Journal of Economic Development, Environment and People, 7*(1), 23. doi:10.26458/jedep.v7i1.571

Nederstigt, B.G. (2016). Empowering retailers to compete offline with online insights (Master's Thesis). Delft University of Technology, Delft, The Netherlands.

Omote, K., & Miyaji, A. (2001). A Practical English Auction with One-Time Registration. *Information Security and Privacy Lecture Notes in Computer Science,*221-234. doi:10.1007/3-540-47719-5_19

Patel, A., Qi, W., & Wills, C. (2010). A review and future research directions of secure and trustworthy mobile agent-based e-marketplace systems. *Information Management & Computer Security, 18*(3), 144-161. doi:10.1108/09685221011064681

Patrick, A. S., Long, A. C., & Flinn, S. (2003). HCI and security systems. *CHI 03 Extended Abstracts on Human Factors in Computing Systems - CHI 03*. doi:10.1145/765891.766146

Peffers, K., Tuunanen, T., Rothenberger, M.A., & Chatterjee, S. (2008). A Design Science Research Methodology for Information Systems Research, *Journal of Management Information Systems, 24*(3), 45-78.

Pham, L., Teich, J., Wallenius, H., & Wallenius, J. (2015). Multi-attribute online reverse auctions: Recent research trends. *European Journal of Operational Research, 242*(1), 1-9. doi:10.1016/j.ejor.2014.08.043

Pla, A., López, B., Murillo, J., & Maudet, N. (2014). Multi-attribute auctions with different types of attributes: Enacting properties in multi-attribute auctions. *Expert Systems with Applications, 41*(10), 4829-4843. doi:10.1016/j.eswa.2014.02.023

Reina, D. S., & Reina, M. L. (2008). *Trust & Betrayal in the Workplace: Building Effective Relationships in Your Organization* (2nd ed.). San Fransisco: Berrett-Koehler.

Reuver, M. D., Sørensen, C., & Basole, R. C. (2017). The digital platform: A research agenda. *Journal of Information Technology, 33*(2), 124-135. doi:10.1057/s41265-016-0033-3

Roman, D., & Vu, K. (2019). Enabling Data Markets Using Smart Contracts and Multi-party Computation. *Business Information Systems Workshops Lecture Notes in Business Information Processing,* 258-263. doi:10.1007/978-3-030-04849-5_23

Ruyter, K. D. (1996). Focus versus nominal group interviews: A comparative analysis. *Marketing Intelligence & Planning,14*(6), 44-50. doi:10.1108/02634509610131153

SafeDEED. (2018). Safe Data Enabled Economic Development, Grant proposal to the H2020 program.

Sein, M. K., Henfridsson, O., Purao, S., Rossi, M., & Lindgren, R., (2011). Action Design Research. *MIS Quarterly, 35*(1), 37-56.

Sheng, S., Broderick L., Koranda, C. A., & Hyland, J. J., (2006). Why Johnny Still Can't Encrypt: Evaluating the Usability of Email Encryption Software. In Proceedings of the Second Symposium On Usable Privacy and Security – Poster Session.

Shneiderman, B. (2018). *Designing the user interface: Strategies for effective human-computer interaction*. Boston: Pearson.

Simon, H. A. (1996). The Science of Design: Creating the Artificial. Cambridge, Mass.: *MIT Press*, 111-138.

Sitkin, S. B., & Pablo, A. L. (1992). Reconceptualizing the Determinants of Risk Behavior. *Academy of Management Review,17*(1), 9-38. doi:10.5465/amr.1992.4279564

Smith, S.W. (2003), "Humans in the loop: human-computer interaction and security – group of 3", IEEE Security & Privacy Magazine, Vol. 1 No. 3, pp. 75-9

Sousa, P. R., Antunes, L., & Martins, R. (2017). The Present and Future of Privacy-Preserving Computation in Fog Computing. *Fog Computing in the Internet of Things,* 51-69. doi:10.1007/978-3-319-57639-8_4

Takeda, H., Veerkamp, P., Tomiyama, T., & Yoshikawa, H. (1990). Modeling Design Processes. *AI Magazine*, *11*(4), 37-48.

Talluri, K. T., & Van Ryzin, G.J. (2005). *The theory and practice of revenue management*. Springer Science & Business Media.

Tarazona-Bermudez, G. M., G-Bustelo, B. C. P., Martínez, O. S., Alvarez, B. T., & Rojas, L. A. R. (2014). Reverse electronic auction web tool for B2B. *Computers in Industry, 65*(5), 841-849. doi:10.1016/j.compind.2013.12.008

Teich, J. E., Wallenius, H., Wallenius, J., & Koppius, O. R. (2004). Emerging multiple issue e-auctions. *European Journal of Operational Research,159*(1), 1-16. doi:10.1016/j.ejor.2003.05.001

Torrent-Fontbona, F., Pla, A., & López, B. (2015). In *AAAI Workshops*. Retrieved from https://www.aaai.org/ocs/index.php/WS/AAAIW15/paper/view/10084/10202

Tura, N., Kutvonen, A., & Ritala, P. (2018). Platform design framework: Conceptualisation and application. *Technology Analysis & Strategic Management,30*(8), 881-894. doi:10.1080/09537325.2017.1390220

Turner, C. W. (2002). The Online Experience and Consumers' Perceptions of E-Commerce Security. Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 46(14), 1246–1250. doi:10.1177/154193120204601402

Venable, J., Pries-Heje, J., & Baskerville, R. (2012). A Comprehensive Framework for Evaluation in Design Science Research. *Lecture Notes in Computer Science Design*

Science Research in Information Systems. Advances in Theory and Practice, 423-438. doi:10.1007/978-3-642-29863-9_31
Whitten, A. & Tygar, J.D. (1999), “Why Johnny can’t encrypt: A usability evaluation of PGP 5.0”, Proceedings of the 8th USENIX security composium, August 1999, Washington.

Yao, A. C. (1982). Protocols for secure computations. *23rd Annual Symposium on Foundations of Computer Science (sfcs 1982)*. doi:10.1109/sfcs.1982.38

Yee, K. (2002). User Interaction Design for Secure Systems. *Information and Communications Security Lecture Notes in Computer Science,*278-290. doi:10.1007/3-540-36159-6_24

Yee, K.P. (2004). Aligning Security and Usability. Security & Privacy, IEEE, 2(5), 48-55. doi: 10.1109/msp.2004.64

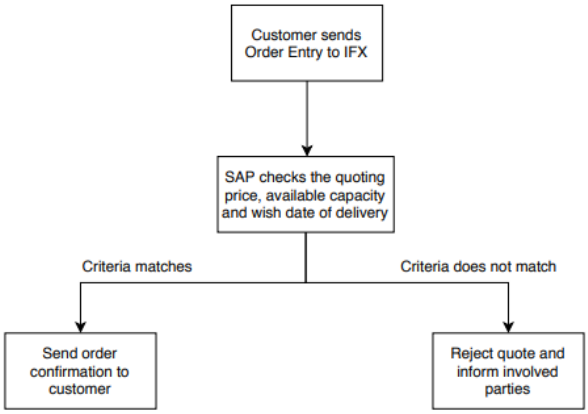
Zatta, D. (2016). *Revenue Management in Manufacturing: State of the art, application and profit impact in the process industry*. Springer.

Zhao, C., Zhao, S., Zhao, M., Chen, Z., Gao, C., Li, H., & Tan, Y. (2019). Secure Multi-Party Computation: Theory, practice and applications. *Information Sciences, 476*, 357-372. doi:10.1016/j.ins.2018.10.024

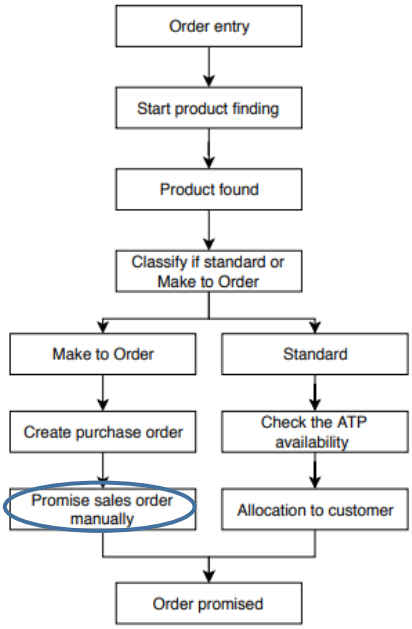
Appendix

Appendix 1. Current Processes at Infineon

Fig_of_Appendix 1 explains the order management process in simplified terms which are further elaborated in the next few figures. Sales is currently involved with taking and confirming orders. Once a customer's quote is received by Sales, they check the price and volume availability in the current system. Fig_of_Appendix 12 shows the different actions required in different cases, either when an ordered product is 'make to order', or a standard product.

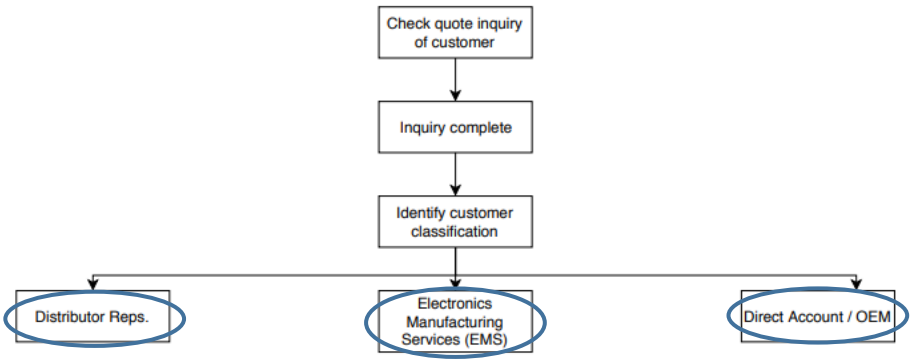


Fig_of_Appendix 1: Simplified order management process



Fig_of_Appendix 2: From order entry until order promised (Manual activity from Sales)

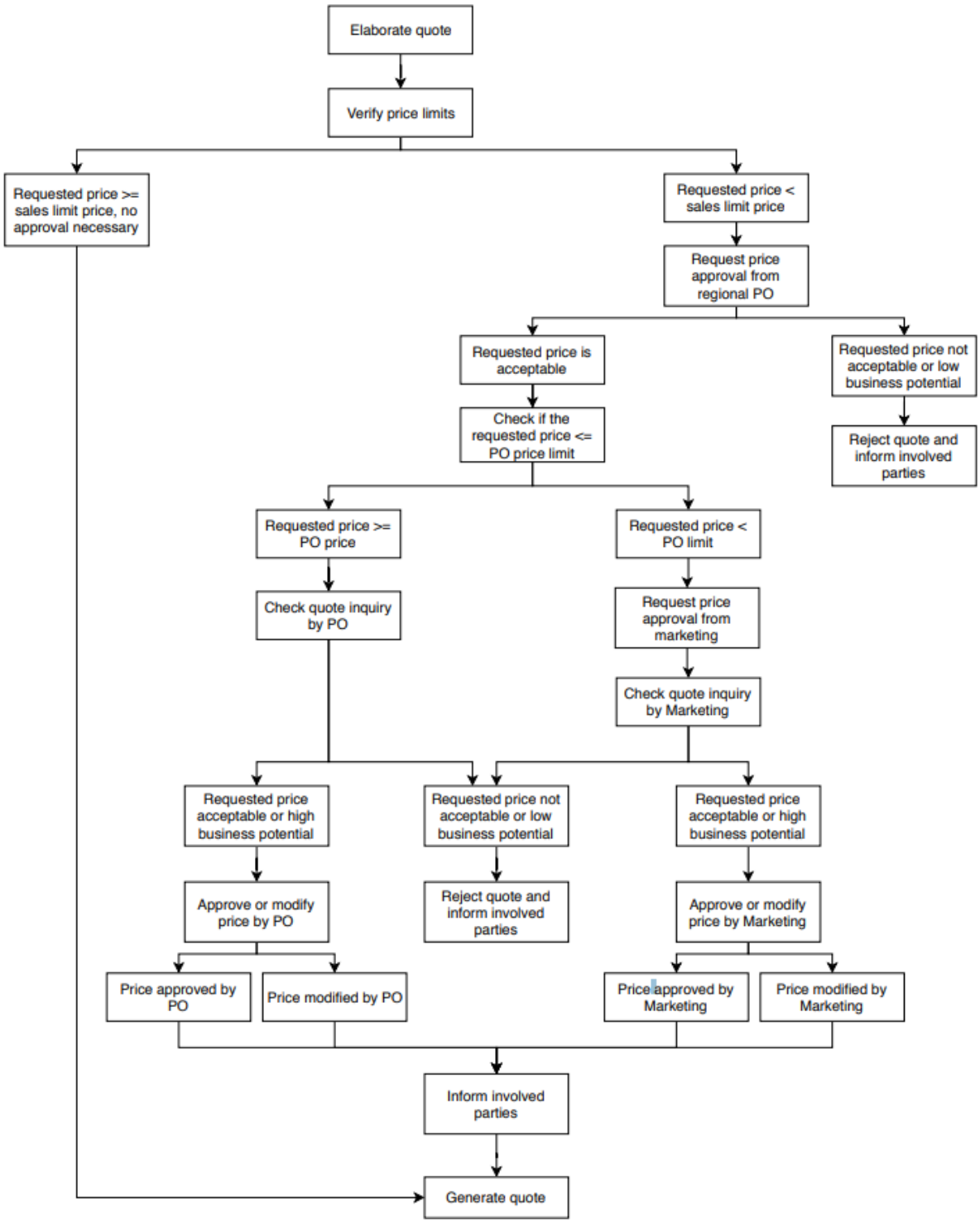
In addition to this, the order process also involves checking for the customer classification for every order. Fig_of_Appendix 13 depicts the three customer types at Infineon, which is checked for, once the received inquiry is complete (from the previous figure).



Fig_of_Appendix 3: Customer types

Fig_of_Appendix 14 explains the process of generating a quote in detail, which helps in comprehending the price comparison that leads to accepting or rejecting a quote in the current system. It then provides an understanding of how the introduction of RM and MPC will change the price comparison algorithm. Consequently, this introduces the need for lead time-based pricing.

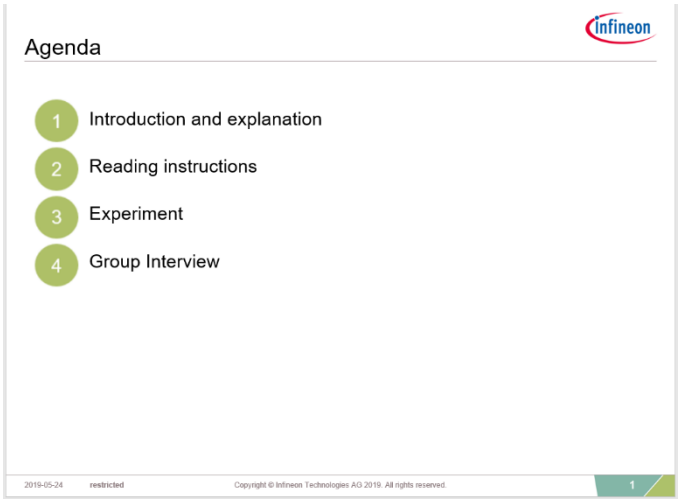
Firstly, it is checked if the requested price (by the customer) is greater than, equal to or less than the sales limit price. If it is greater than or equal to, the process is quite simple and a quote is generated. On the other hand, if the requested price is less than the sales limit price, the requested price needs approval from the regional purchase officer. This further requires inquiry with Marketing, in case the requested price is less than the PO limit. If the price is eventually approved, a quote is generated. With RM, all quoted prices would typically already be higher than the quoted unit price, as customers would like earlier deliveries, and would be willing to pay higher prices for this. MPC will further ease the process, as it will automatically compute the outcome based on the input of customer's willing to pay prices.



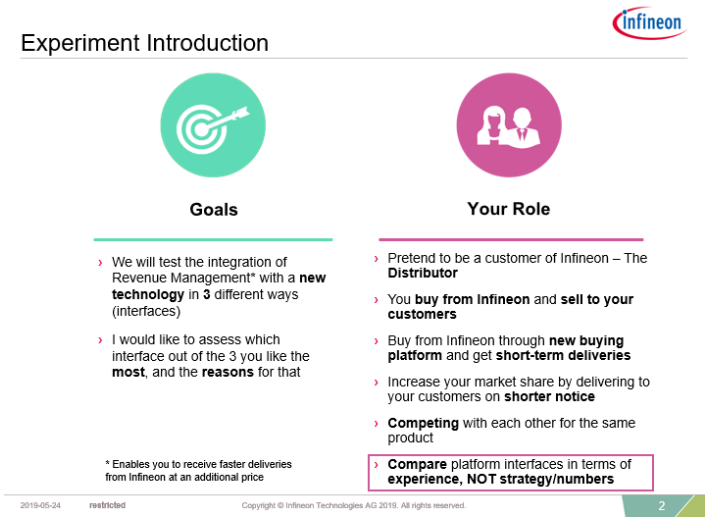
Fig_of_Appendix 4: Quote verification and generation

Appendix 2. The preparatory material for the experiment and interview

The following documents were shown to the participants before they used the three mock-ups and the interview session.



Fig_of_Appendix 5: Agenda for the session



Fig_of_Appendix 6: Introduction of goals and participant role

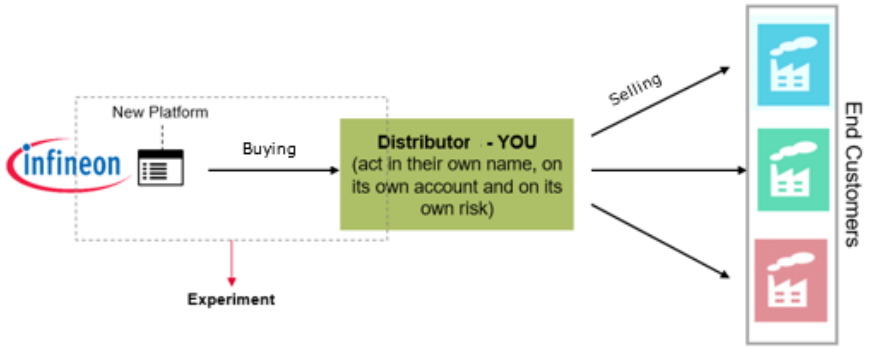
EXPLANATION (Experiencing the design of 3 platforms)

Revenue Management (RM):

- RM is used in the service industry such as airlines. This means that sooner flights are higher priced.
- RM in our context is when customers get products sooner than stated in the contract.
- Its acceptance depends on you.

Distributors Profile:

Please imagine that you are a distributor (a customer type) who buys from Infineon. You then sell to your customers at a price that you are free to set yourself. You usually sell at a markup price (selling price > buying price), to be profitable. Because the price you pay to Infineon is sensitive for your business (you don't want customers to know your margin, or other competing distributors to know the price you buy), you want to keep it confidential and private. Your customers will be willing to pay higher prices for earlier product deliveries. Hence, you would be buying at a higher price from IFX to get your products faster.



EXPERIMENT PROCEDURE

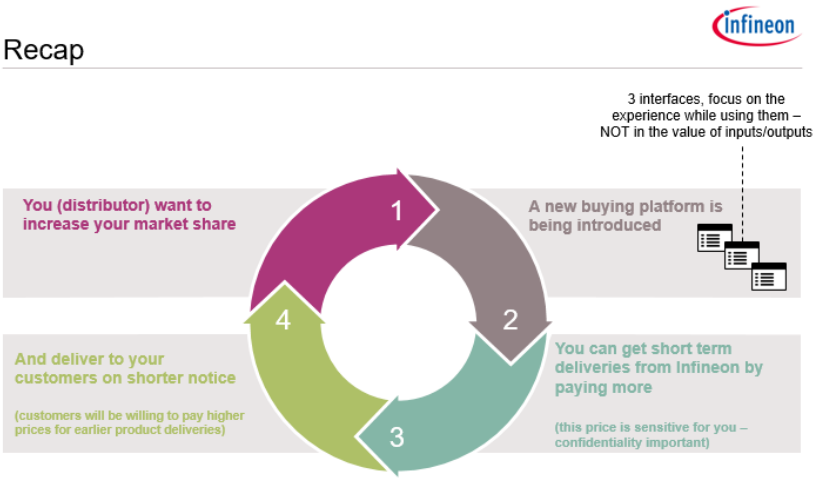
Structure:

1	Introduction + existing interface	Understand and familiarize with current system
2	Use 3 interfaces	Experience 3 different interfaces for revenue management
3	Interview	Discussion of how you felt while experiencing the 3 interfaces

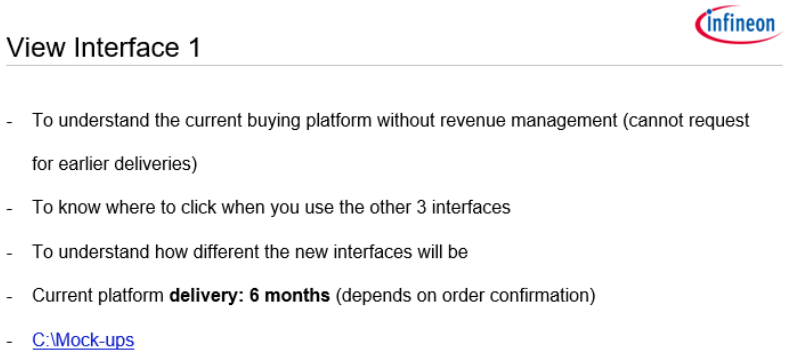
Think critically about:

- Your attitudes and feelings towards the preferences and experience, in interacting with the 3 new platforms as a distributor.
- Focus on:
  - Who is able to see it?
  - How secure you think it is for your data?
  - What is the value of confidentiality for you?
  - How much you trust the platform interfaces?
  - What you feel will happen to your data?

Fig_of_Appendix 7: Document provided to the participants to read and understand the setting



Fig_of_Appendix 8: Recap of the document read by the participants



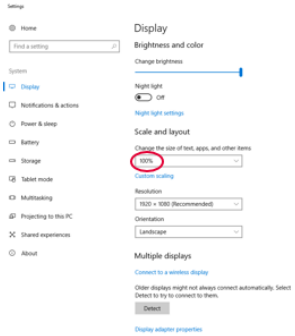
Fig_of_Appendix 9: Video of interface 1



Fig_of_Appendix 10: An input guide for the participants for the revenue management interfaces

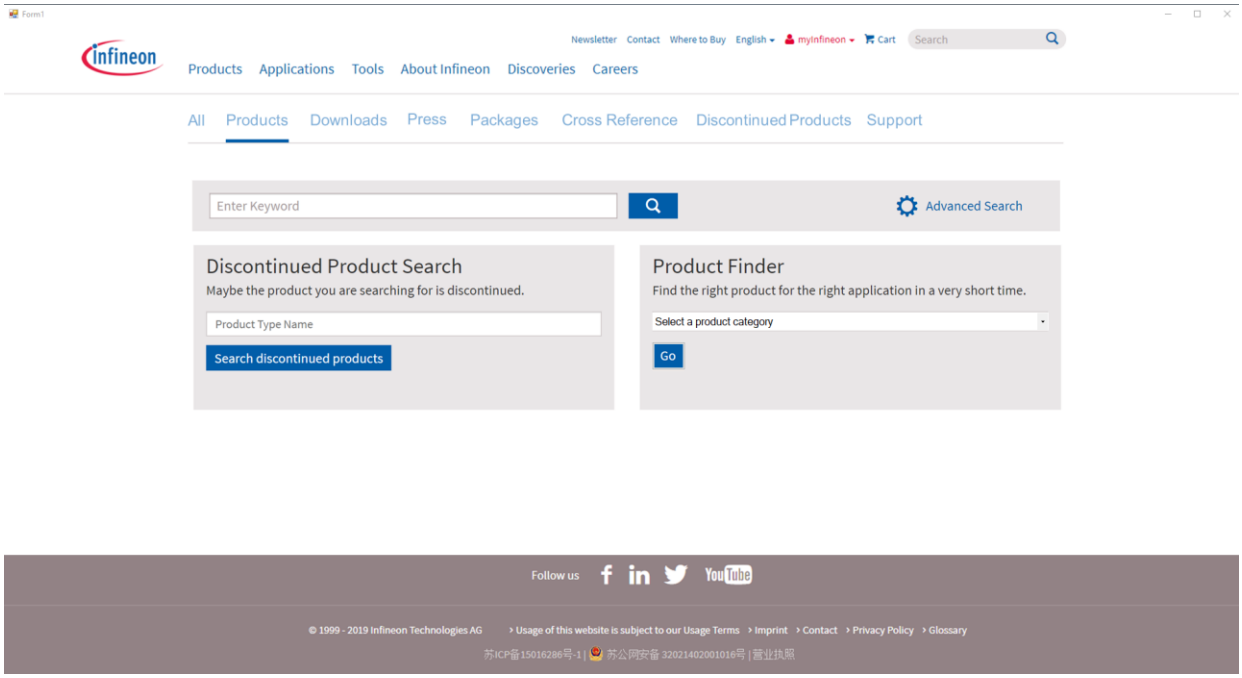
Use 3 Interfaces

- Pretend to be a customer of Infineon – The **Distributor**.
- You **buy from Infineon** and **sell to your customers** at a **higher price**.
- **Competing** with each other for the same product.
- **\\mucsdn32.eu.infineon.com\csc_bs\02_public_Faujdar\Thesis\Experiment**



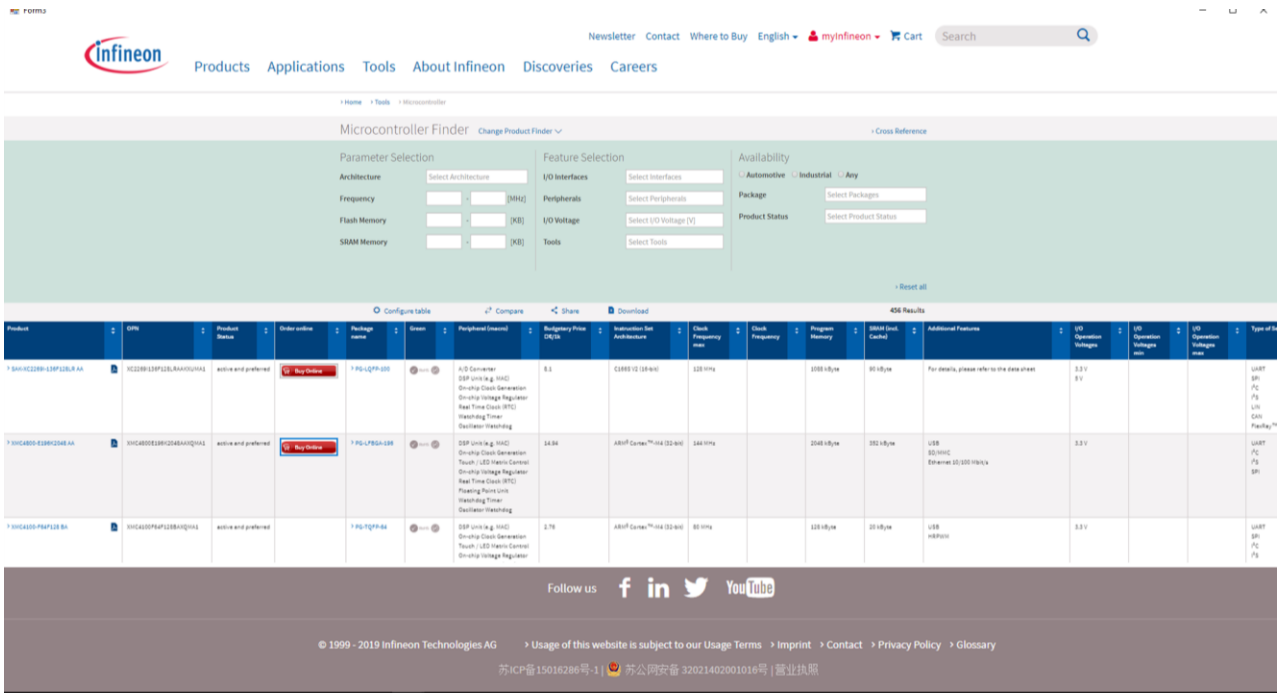
Fig_of_Appendix 11: Instructions to use the mock-ups and change the display resolution to fit the mock-ups best

Appendix 3: Artefact screens common to the three mock-ups



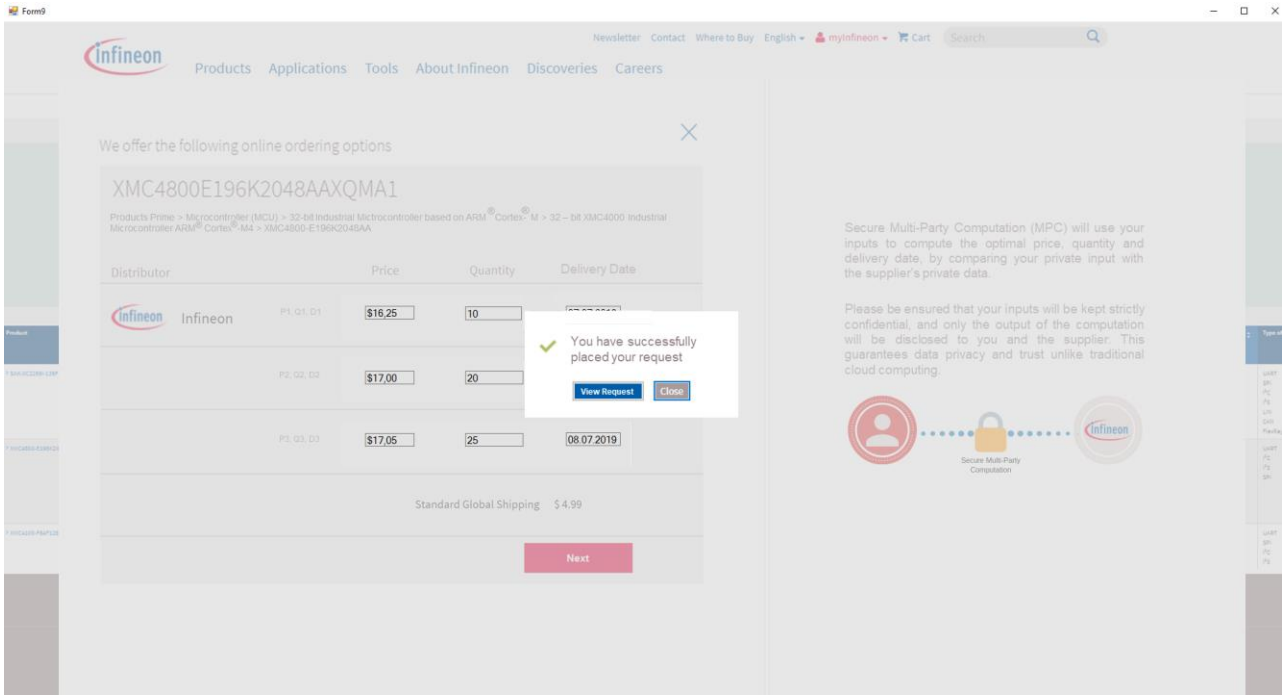
Fig_of_Appendix 12: Artefacts screen 1

Screen 1 is the landing page of the artefacts. Customers choose a product from the drop-down menu in the Product Finder. The program is developed to automatically choose "Microcontroller Finder" regardless of the chosen option. This is because the next screens are programmed on the information of Microcontroller Finders.



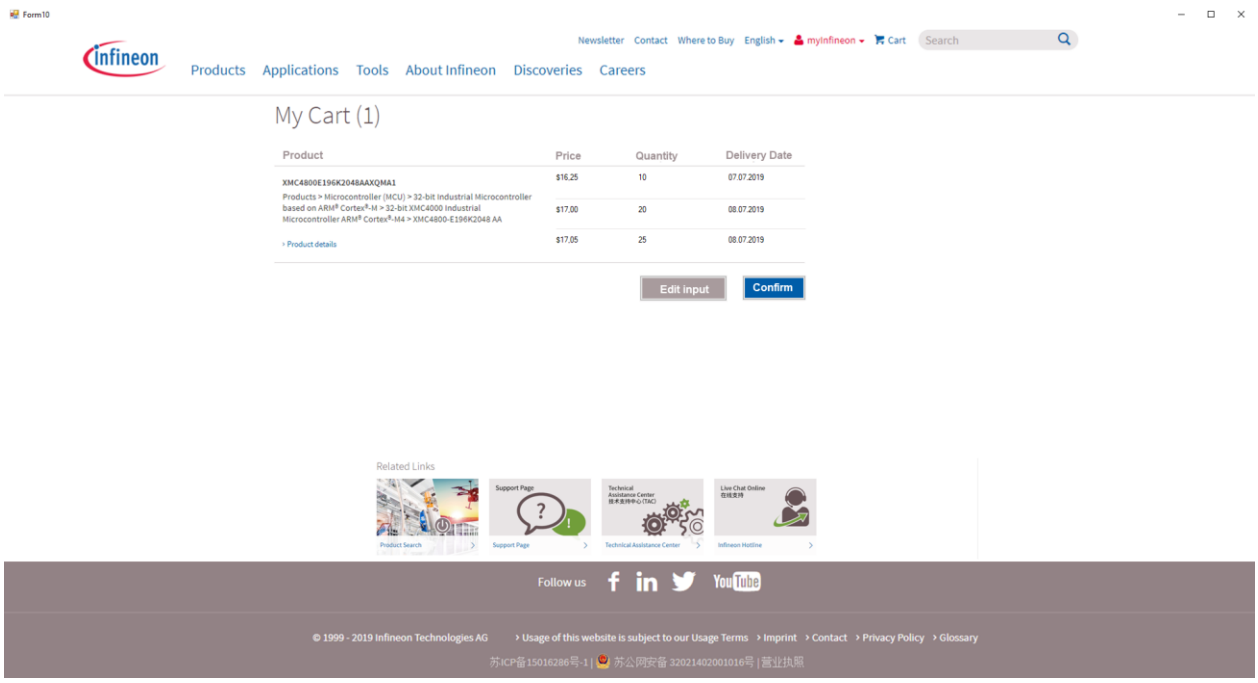
Fig_of_Appendix 13: Artefacts screen 2

Screen 2 presents the options available for buying. The two red "Buy Online" buttons are interactive here and clicking either of them would take the customer to the next screen.



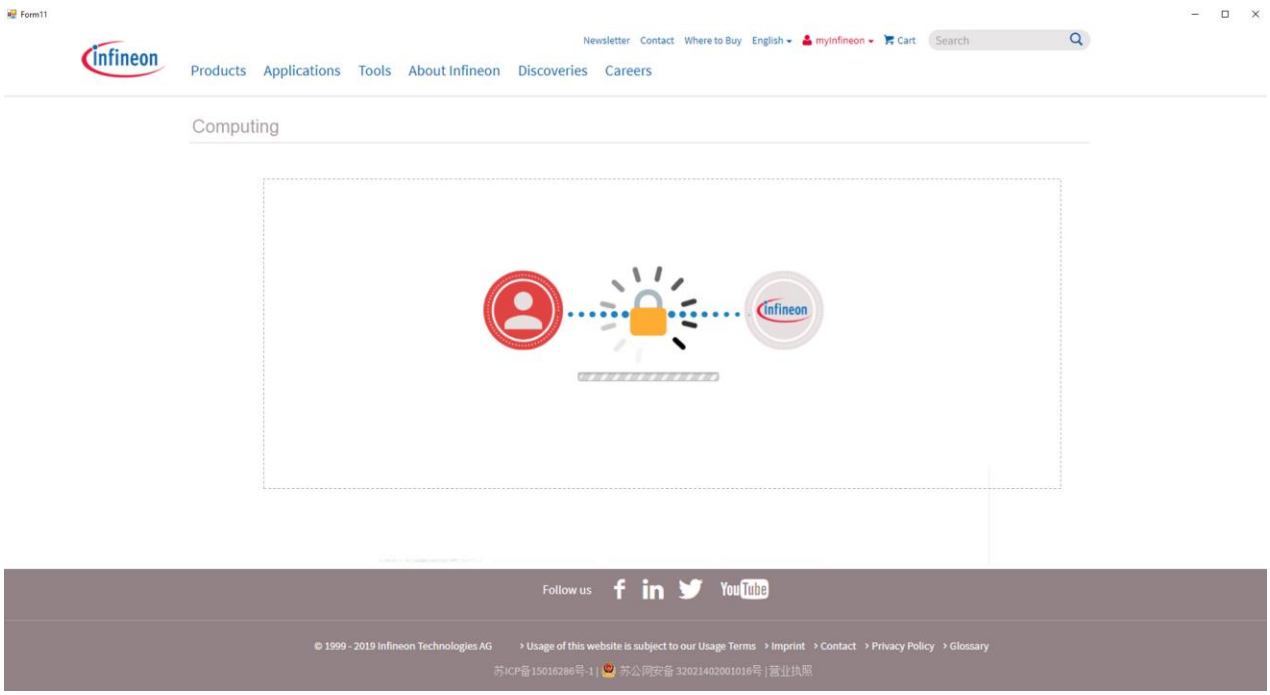
Fig_of_Appendix 14: Artefacts screen 3

The screen before this (not pictured here) and Screen 3 changes with the three artefacts. The previous screen (in Chapter 3) is the main input screen which changes for every artefact. While the left-hand side panel remains the same, the panel on the right changes with regards to text and visuals (disclaimer, blurry or clear).



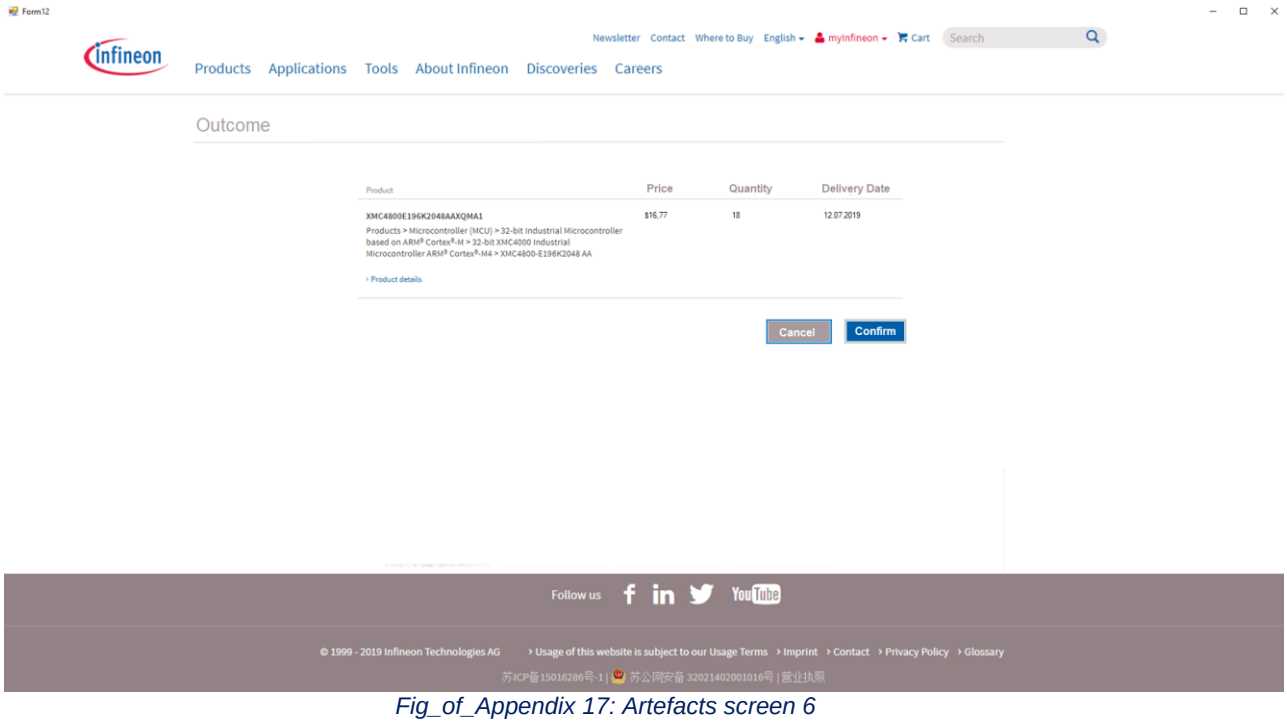
Fig_of_Appendix 15: Artefacts screen 4

Screen 4 shows the customers' cart, which is a reconfirmation of the product ordered with the wish delivery date, price and quantity bids.



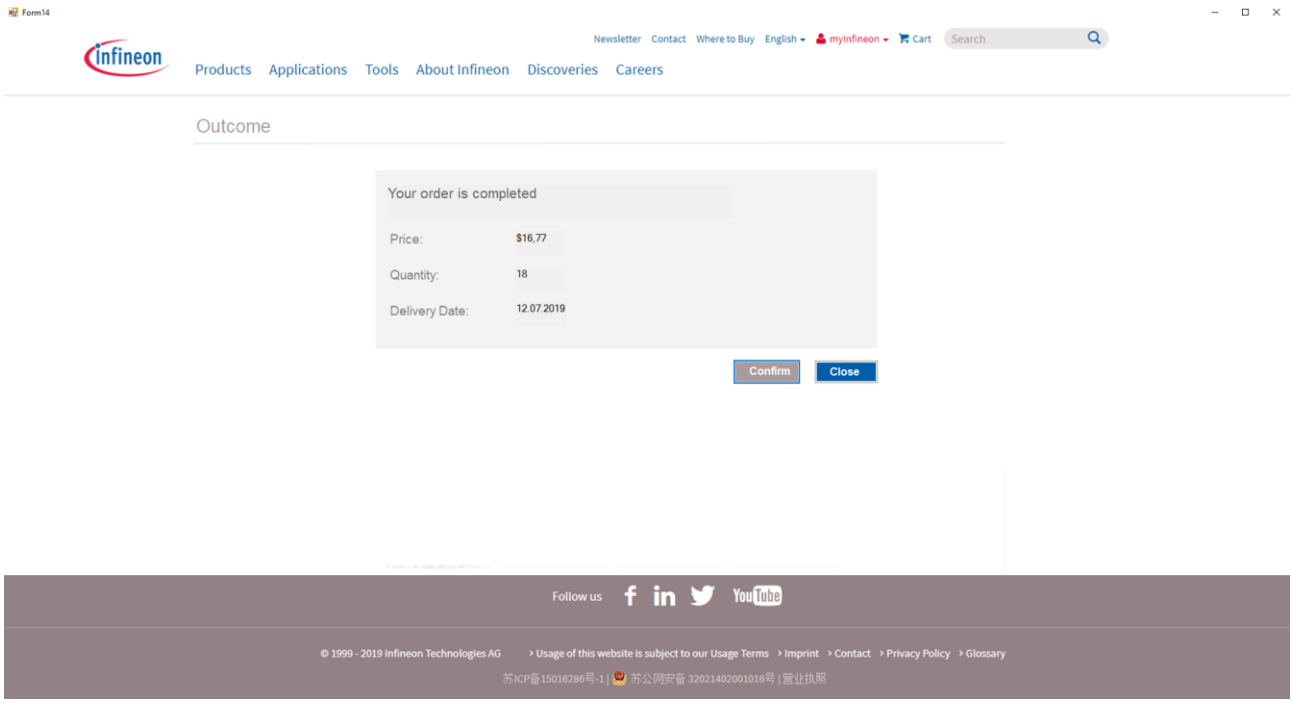
Fig_of_Appendix 16: Artefacts screen 5

Screen 5 shows the computation in progress. This screen is programmed to remain for five seconds before automatically switching to the next screen.



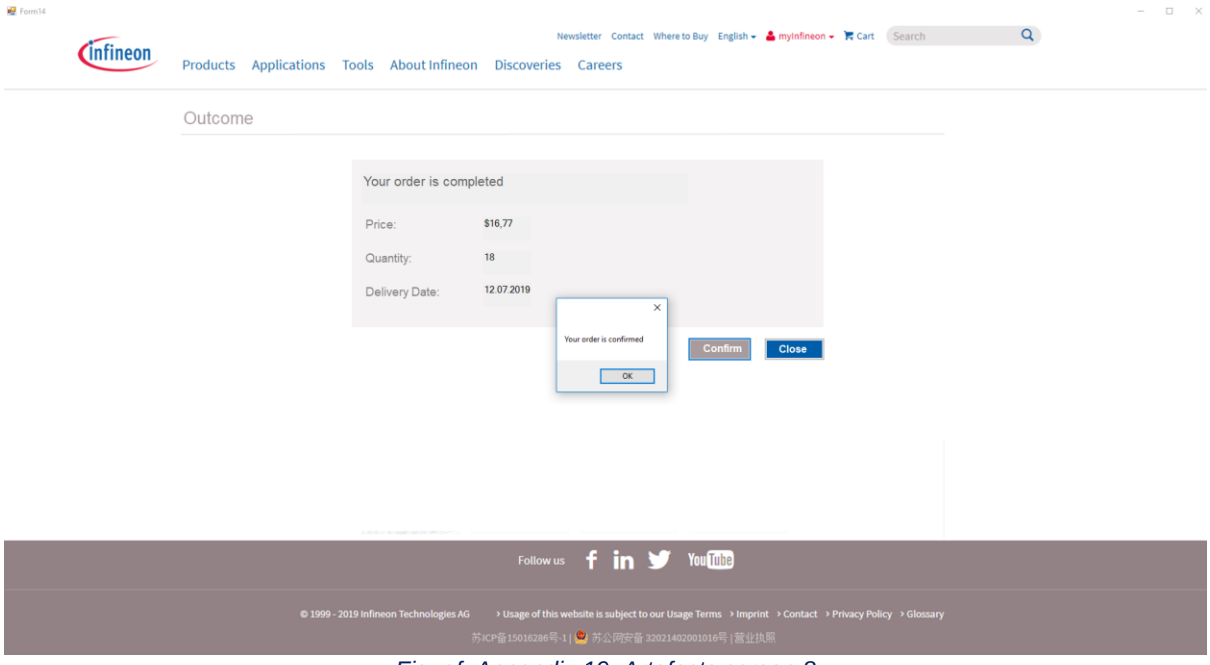
Fig_of_Appendix 17: Artefacts screen 6

Screen 6 shows the outcome of the computation. This shows customers that their bids have been accounted for and the optimal output as per everyone has been computed. The customer has the opportunity to confirm this outcome and proceed, or cancel the process if they are unhappy with the outcome.



Fig_of_Appendix 18: Artefacts screen 7

Screen 7 is the final screen to confirm or cancel the computed outcome.



Fig_of_Appendix 19: Artefacts screen 8

Screen 8 is the last screen of the artefacts, should the outcome be confirmed. This reads that the order is completed. The program closes automatically once “OK” is selected.

Appendix 4. Word cloud of the interviews (keywords)

