Perspectives on Future Power System Control Centers for Energy Transition

Marot, Antoine; Kelly, Adrian; Naglic, Matija; Barbesant, Vincent; Cremer, Jochen; Stefanov, Alexandru; Viebahn, Jan

DOI
10.35833/MPCE.2021.000673

Publication date
2022

Document Version
Final published version

Published in
Journal of Modern Power Systems and Clean Energy

Citation (APA)
Marot, A., Kelly, A., Naglic, M., Barbesant, V., Cremer, J., Stefanov, A., & Viebahn, J. (2022). Perspectives on Future Power System Control Centers for Energy Transition. *Journal of Modern Power Systems and Clean Energy*, *10*(2), 328-344. https://doi.org/10.35833/MPCE.2021.000673

Perspectives on Future Power System Control Centers for Energy Transition

Antoine Marot, Adrian Kelly, Matija Naglic, Vincent Barbesant, Jochen Cremer, Alexandru Stefanov, and Jan Viebahn

***Abstract*—Today's power systems are seeing a paradigm shift under the energy transition, sparkled by the electrification of demand, digitalisation of systems, and an increasing share of decarbonated power generation. Most of these changes have a direct impact on their control centers, forcing them to handle weather-based energy resources, new interconnections with neighbouring transmission networks, more markets, active distribution networks, micro-grids, and greater amounts of available data. Unfortunately, these changes have translated during the past decade to small, incremental changes, mostly centered on hardware, software, and human factors. We assert that more transformative changes are needed, especially regarding human-centered design approaches, to enable control room operators to manage the future power system. This paper discusses the evolution of operators towards continuous operation planners, monitoring complex time horizons thanks to adequate real-time automation. Reviewing upcoming challenges as well as emerging technologies for power systems, we present our vision of a new evolutionary architecture for control centers, both at back-end and frontend levels. We propose a unified hypervision scheme based on structured decision-making concepts, providing operators with proactive, collaborative, and effective decision support.**

***Index Terms*—Artificial intelligence, cyber-physical system, decision-making, digital architecture, digital twin, energy transition, hypervision.**

I. Introduction

POWER systems continue to evolve to accommodate new demands and challenges, to support the energy transition. Today's power systems are more interconnected than ever within the cyber and physical spaces. While their evolution was mostly driven in the past by grid infrastructure and capacity expansion, it now becomes a matter of greater grid management and optimization over existing infrastructure. As the central nerve of the power system, control centers have always supported its evolution [1], [2], and will continue to do so. Control centers [3] provide groups of human operators with the necessary working and decision-making environment to remotely monitor the system and properly operate it in real time.

Today, the energy transition is forcing radical changes on the working environment of system operators, at an even faster pace [4]. A rethinking of the architecture of the control center and the role of the operator is now required. New architecture should enable more evolutionary, standardized, and modular integration. More importantly, as control centers are primarily environments made for operators to regularly make decisions when operating the system, more human and decision-centric design should also be considered. In particular, it is now necessary to develop smart and unified human-machine interfaces, referred to as "hypervision", leveraging advances in these fields for the last two decades.

This paper reviews why the underlying systems are changing today and the consequences for operating the power system in Section II. It further develops a vision on what needs to change in the control center. An holistic approach for rethinking decision-making that enables operators become "hypervisors" of cyber-physical systems (CPSs) [5] is presented in Section III. This approach is complemented with an enabling digital platform architecture in Section IV. After reviewing emerging technologies and functionalities that could be integrated in the platform in Section V, operational perspectives are shared in Section VI over proactive and assisted decision-support, risk-based security paradigm shift, as well as continuous realistic testing and simulator training. We conclude this paper in Section VII.

II. Changing Environment for Control Centers

A. Redesigning System for Energy Transition

To address climate change, governments around the world have set aggressive targets for carbon emission reductions in the coming decades. The paths of the various sectors towards zero emissions are uncertain. There may be unavoidable adaptation to some climate change level with rising temperatures and extreme weather events [6]. However, as of 2022 there is a noticeable trend towards electrification of sectors, i. e., transport, agriculture, domestic heating [7] to participate in decarbonisation. Hence, the power system will

Manuscript received: October 1, 2021; revised: January 28, 2022; accepted: March 12, 2022. Date of CrossCheck: March 12, 2022. Date of online publication: March 30, 2022.

A. Marot (corresponding author) and V. Barbesant are with Reseau de Transport d'Electricite, Paris, France (e-mail: antoine.marot@rte-france.com; vincent.barbesant@rte-france.com).

A. Kelly is with Electric Power Research Institute, Dublin, Ireland (e-mail: akelly@epri.com).

M. Naglic and J. Viebahn are with TenneT, Arnhem, the Netherlands (e-mail: Matija.Naglic@tennet.eu; Jan.Viebahn@tennet.eu).

J. Cremer and A. Stefanov are with TU Delft, Delft, the Netherlands (e-mail: j.l.cremer@tudelft.nl; A.I.Stefanov@tudelft.nl).

DOI: 10.35833/MPCE.2021.000673

likely become an increasingly important part of all sectors of society and the economy [8]. This increased reliance, will likely mean that the transmission and distribution systems will need to be ever more reliable and resilient. The system may shift dynamically, which will increase uncertainty.

Driven by renewable resource integration, the operation uncertainty of the power system will increase beyond what it was designed for [9]. Transmission and distribution networks were designed for transporting steady power flows from large fossil-fueled generators to demand centers. Future systems require redesigning to accommodate uncertainties in power flows and in injections, as well as more distributed energy resources (DERs) [10]. Uncertainties will further increase as the inverter-based resources (IBRs) add novel dynamics to grid operation, lowering the inertia available to balance autonomously grid stability with novel control complexities [11]. Unfortunately, the past design paradigms to build stronger grids to ensure the security of supply while transporting more electricity are not suitable anymore [12]. The increase in uncertainty with the same designed safety margins would require unjustifiable grid investments as the willingness of society to build new electricity infrastructure decreases (due to visual and environmental impacts). The required flexibility will hence come from smarter operations, devices, and resources as it is likely that flexibility can not come from new infrastructure. Operators will have to do more with the existing grid as summarized in Fig. 1, and the grid will be pushed closer to its limits [4]. It can be observerd from Fig. 1 that given the energy transition and other drivers, the grid is already changing from the outside and the inside. This has operational impacts, leading to operational needs in terms of grid flexibility and decision-making capability.

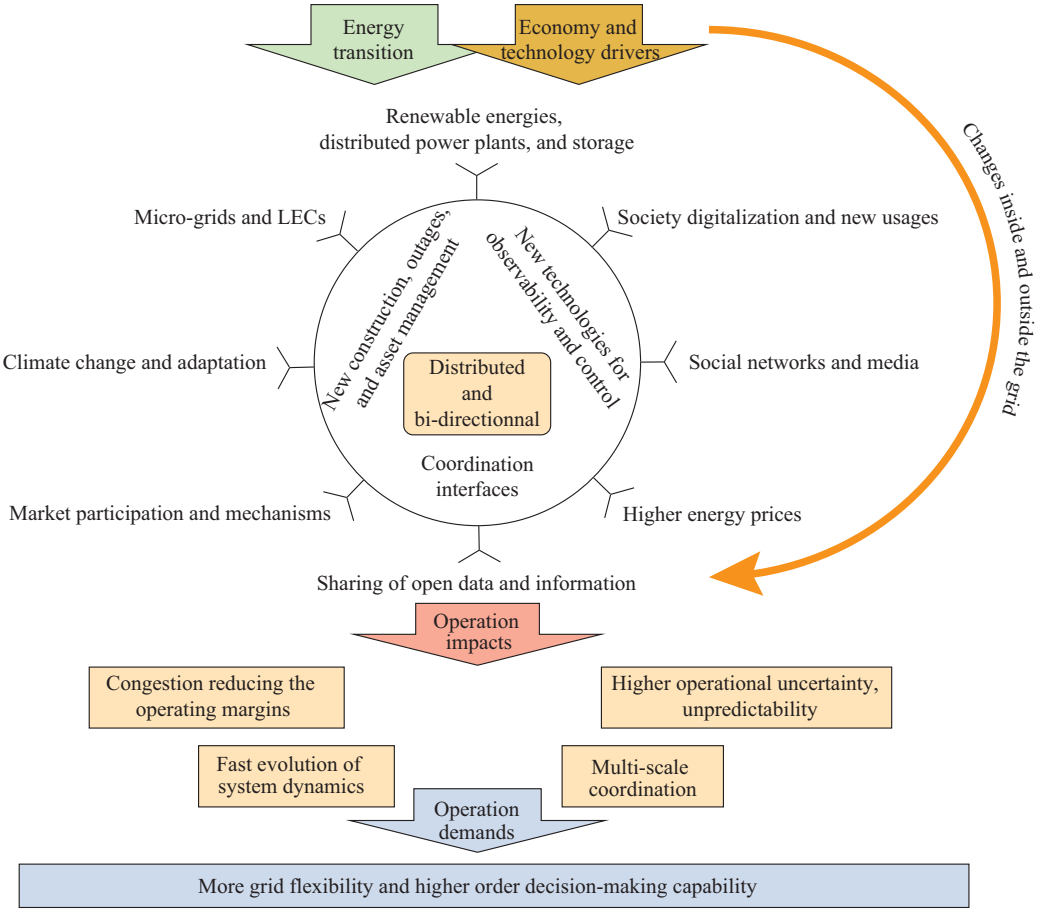

Fig. 1. New operational needs under energy transition that is impacting operations along different dimensions.

B. Changing Environment – from Outside

Control centers may be redesigned to consider several changes to the power and market system that are being imposed externally and are described below.

1) Micro-grids and local energy communities (LECs) are small entities such as towns or villages that are aiming to balance their own energy demands. Driven by the trend towards more DERs, LECs are rapidly increasing across the world [13]. Smart meter technology allows end-users more observability and control of their energy, hence their own local control becomes more autonomous and LECs are participating in markets [14]. These micro-grids and LECs represent challenges and opportunities for control centers, e. g., their uncontrollability, unobservability, and demand variability. The opportunity lies in using their flexibility for balancing and congestion management on distribution and transmission systems [15] through demand-side management [4], [16].

2) Market participation and new mechanisms will increase, which require the interactions with a larger number of market participants [17], [18], both via verbal communication and electronic messaging. With most participants, these interactions are expected to be autonomous, in real time, via secure information and communication technology infrastructure. There will be more widely shared generation capacity, and shared operation flexibility which must be allocated between neighbouring systems [19] will add new operation constraints. These constraints and tasks must be added to current tasks of control center operators which will likely require additional tools and software [4]. Power-to-gas and hydrogen are likely to be key components of a future climate neutral energy system, which brings consequent challenges for electricity system control and new co-optimized multi-energy markets [20].

3) Sharing of open data and information will likely increase as per current regulatory and policy directions for increased transparency, sensitivity, and privacy [21]. These regulations aim at increasing market participation, reducing energy prices and spurring innovations. For instance, in Europe, ENTSO-E developed a transparency platform which is tied to the European network codes which have articles related to data transparency [22]. While most of these platforms are automatic data exchanges, there may be some manual new reporting tasks for operators and transmission system operators (TSOs) to report on events and disturbances soon after an event. Through fast processing with application programming interface (API) and social media, consumers have accurate access to near real-time information.

In the future, the manual process of report generation in control rooms should be more automated. This should free up valuable operator cognitive load to analyze the risk in real time, by studying the system and applying their experience and engineering knowledge. One slight drawback of an open data policy is that the general public with little knowledge and experience of the actual system dynamics may make incorrect interpretations of events, which may have to be repudiated by the TSO in case it spreads as misinformation. Open data should be accompanied [23] by a strong, authoritative voice of the TSO in the industry with a reactive crisis communication team for emergency scenarios, possibly taking inspiration from the COVID-19 worldwide crisis management in media [24].

C. Changing Environment – from Inside

In parallel to externally forced changes, new technology integration, asset management, or system interconnections are also changing the power system from the inside.

1) New Technologies for Observability and Control

Technological advancements in sensor, information, and communication technologies provide state-of-the-art ones for power system monitoring. Power electronics in high-voltage direct current (HVDC) [25], onshore and more and more offshore [26] wind farms as well as photovoltaic panels is challenging the way in which the grid is designed. Yet, power electronics also allows the possibility of new rapid controls. More and more rapid remote controllers and devices are also making the system more complex to understand and manage overall with current tools in the control center. Existing grid flexibilities such as topological changes could also be exploited with new advance controllers. At the same time, the technology of phasor measurement units (PMUs) [27] can allow system operators to monitor the dynamic performance of the system. Beyond the development of the smart substation, new light Internet of things (IOTs) [28] sensors installed along power lines also give more fine-grained information and greater observability. This enables asset monitoring and allows for new predictive models used, for example, in dynamic line rating (DLR) [29].

The digitisation of infrastructure has brought the power grid into a new era, which creates many opportunities for greater flexibility by allowing the collection of more data or capability on the edge [30]. But it also makes the network more vulnerable to cyber attacks [31], and the availability of more data requires the new and improved software systems, platforms, and hardware in the control center.

2) New Construction, Outages, and Asset Management

In most countries around the world, the power grid is well established. Investing in the development of new power lines in such grids is becoming increasingly difficult. The historical approach to accompany system transitions is often not viable anymore: existing structural grid topology will not change much. However, most transmission systems around the world are experiencing rapid growth in construction projects to interconnect new renewable energies at the periphery of grids (mountains and near coasts) while most of the existing backbone infrastructure grid is aging. Each new project requires outages of the existing grid, which can further stress the grid. Outages require the coordination and consultation between the responsible TSOs and associated TSOs or market operators [32]. Each outage requires more people to work and track on site, involving more numerous interactions and greater risk of human error. When asset protection and control upgrades are carried out on the network, this has typically led to a vast increase in the number of alarms or data points being sent back to the control center.

This development has led to alarm and information overload, where operators are swamped by superfluous information. For the future control center, a streamlined and analytical approach to outage management that optimises cost, duration, and factors in variable resources will be required [30]. For situational awareness, a new approach to alarm management that requires intelligent decision support, improved information visualization and analysis on asset data to indicate stress points would be ideal.

3) Coordination and Interfaces

Control centers now have increased interactions with similar system operators, market operators, or security and reliability coordinators. This trend is likely to continue in North America with multi-state independent system operators (ISOs), in Europe with regional coordination centers (RCCs) [33] and in Australia and Asia. Country or regional states will likely become more interconnected via HVDC links, offshore grids, and market coupling which will require additional coordination over initially heterogeneous operation practices.

Similarly, the interaction between TSOs and distribution system operators (DSOs) is likely to intensify and some control approaches for this interaction were proposed [34]. Conventionally, DSOs served customers vertically from the transmission system, while now distribution systems are active networks, with DERs contributing to markets and congestion issues on increasingly meshed distribution networks [35]. The issues around area of responsibility between balancing the frequency with DER versus managing voltage and congestion on distribution networks are difficult to resolve and will require standardized data exchange, improved data visualization, and social interaction with operators in distribution control centers.

Control centers are likely to be more connected to collateral aspects of the grid: telecommunication network, supervision of information system or asset monitoring, market variations or even social networks. Models and processes that assess the feasible operation domain should be commonly shared online during real-time operations across all those interfaces. They could possibly be co-designed between stakeholders and regularly re-adapted offline ahead of operations. This web of interactions constitutes an additional workload for the operator. In Europe, ENTSO-E is working with TSOs to achieve this vision for future control centers, enabled by common grid models and data platforms [36].

D. Consequences of These Changes

Given this context, a number of consequences can be anticipated for the way in which electricity transmission systems are operated as partly outlined in [37] and [38].

1) The dependence of DER on weather conditions, the decommissioning of conventional generation and an aging grid, and the electrification of sectors of society will lead to higher operation uncertainty.

2) The decentralisation or market participants and lack of new infrastructure will lead to a reduction in operating margins of the power system, and the operation of the system will be closer to its limits.

3) Increased interconnection between transmission systems will require coordination and oversight. Increased interaction between transmission and distribution systems will require more active monitoring and control.

4) The dynamics of evolution (market rules, behaviours of actors, technologies on the grid) in the power system will be faster, requiring rapidly deployed new process, tools, and monitoring capability.

5) The power system will become cyber-physical but less predictable while relying on extended delegation or sharing of aspects of control, the splitting of areas of responsibility and functions.

6) Operations and decisions will become more complex and require more anticipation, coordination, and automation in real time.

Faced with these changes, the traditional decision-making process, which is mostly based on the operators' knowledge and real-time awareness, will not be feasible anymore: it will have to be adaptive and well-structured.

III. Rethinking Decision-making in Control Centers

As operations and decisions become more complex, there is now a requirement to rethink the operator's decision-making environment through human-centered design through: ① renewed definition of operator's role, functions, processes, and tasks; ② integrating structured decision-making frameworks; and ③ greater integration of the working environment ecosystem with a simplified, adaptive, and modular smart interface.

More consistent and structured decision-making processes will allow for improved coordination and automation integration.

A. Evolution in Operator Roles and Tasks

1) Increased Real-time Task Automation

Figure 2 shows the evolution of operator's decision-making environment over decades with increasing number of tasks. This was first compensated through tool development and support, combined with the automation of some processes. Nowadays, application ecosystem integration behind unified interface and extended operator's time horizon are further needed to continue taking proper decisions. Conventionally, operators in a control room worked in real time. This meant manually managing the dispatch of generation, manually forecasting the demand, managing power flows on lines and transformers, and planned and unplanned outages of transmission equipment as they occurred in real time. Lines always had to be manually reconnected to the system by operators. Other manual processes include reporting, logging, and workforce management. These manual processes are generally cognitively intensive and do not increase situational awareness.

In recent decades, control centers have automated some of these manual processes [39]. Automatic generation control (AGC) and enhanced market systems manage the dispatch of generation, reserves, and interconnector flows based on automated demand and renewable forecasting. Auto-reclosing and special protection schemes have proliferated, reducing the manual interventions for unplanned outages. Security assessment is automated, and automatic voltage optimization and control is now becoming part of normal system operations.

Today, operators in most control centers still manually switch on the system, study the network for outages and do planned switching and intervene for unplanned outages and emergencies. They still manually perform ex-post reporting and workforce management, but unplanned outages that do not reclose (or transformer or cable outages) are likely to become the only process that is managed in real time. This can be considered as very rare events and manual interventions when automation fails – in a way similar to manually dispatching generation if AGC fails.

In the future control center, the aim should be to continue the trend of automation of manual processes that do not increase operators' situational awareness, but are time-consuming, tedious, and repetitive tasks. This is especially relevant when considering manual administrative processes such as logging and reporting on incidents, logging and dispatching asset health anomalies, and managing workforce.

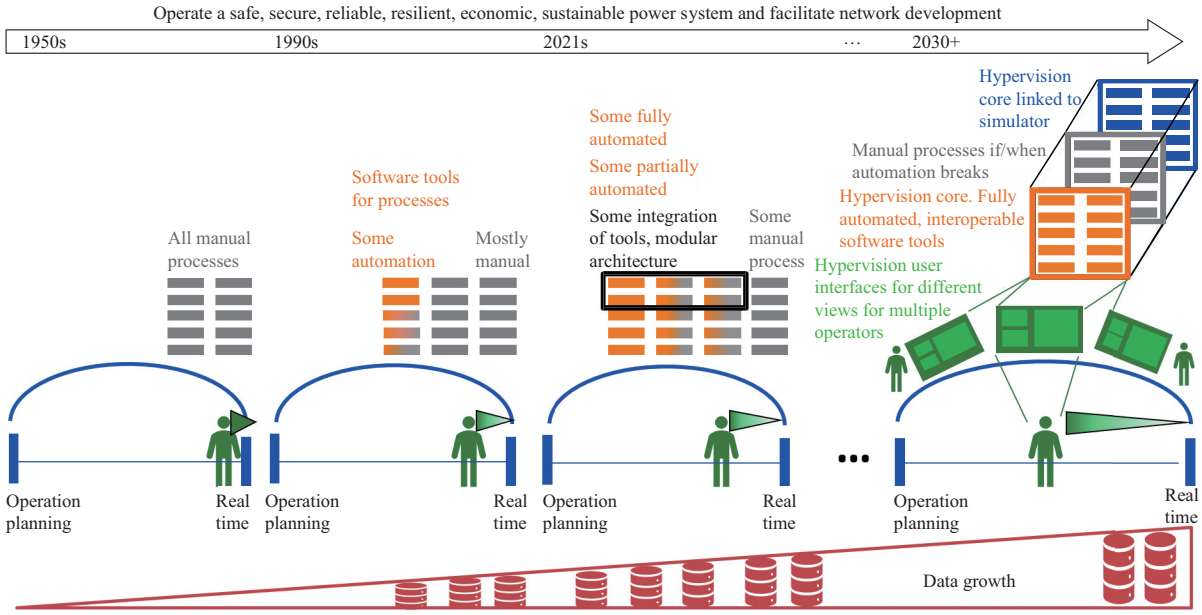

Fig. 2. Evolution of operator's decision-making environment over decades with increasing number of tasks.

2) Towards Planners and Navigators

Due to the trend of automation, the operators' time horizon can be considered to be moving further away from real time, where they monitor the system and assess risks associated with real-time market operations, system peaks, and renewable energy ramps. This is because decisions are getting more numerous, complex, and inter-dependant under greater uncertainty [40], coordination, and reduced margins, as highlighted in Section II-D. Because of this, operators no longer have time to make the most optimal decisions in real time and thus must rely on both the automation of the system in real time and in the accuracy of forecasts and study tool optimization ahead of real time. As shown in Fig. 2, it may be the case that the operator's time horizon moves away from real time to an operation role more defined as an operation planner, eventually on the way towards a unified framework in planning and operation [41]. With this longer horizon, operators can dynamically anticipate trajectories, strategize and assess risks for upcoming forecasted system issues, ramps or peaks and reconfigure the grid ahead of time and be prepared to do so when needed. Operators may only intervene in real time if automation is not available or does not work as expected.

As an inspirational analogy, aeroplane pilots moved away from continuously steering the plane, based on real-time perception and indicators. They eventually became navigators by planning most of the flight trajectory ahead of time with forecasts, relying on an autopilot to follow this trajectory. Occasionally they would adjust the trajectory in or close to real time. Similarly, in the future, it can be expected that grid operators become grid navigators, planning and defining expected future trajectories supported by forecasts with an assistant that assesses risks, makes recommendations, and helps plan and execute tasks and reporting.

3) New Hierarchical Cyber Architecture for Autopilot

Within a range from a defined trajectory, an autopilot could help handle local or global fast system dynamics with proper reactivity. Large-scale automatic frequency regulations or local simple automatons are the examples of automatic control that have been deployed. However, to develop a more integrated autopilot that operators can rely on, coordinate with, and reconfigure, a supporting and unified cyber architecture beyond individual task automaton needs to be deployed. This would come as hierarchical modular and configurable cyber layers. At the top, the operators must manage an "optimize" layer, from which they have a global view of the system and can receive aggregated information and send macro orders to the underlying layers (voltage setpoint, automaton configuration, etc.). Zonal distributed "control" layers, a new type of layer, would monitor local areas covering several substations and provide advanced control with automatic remedial action schemes around configured setpoints or delimited operational domains. The "protect" layer, located at the substation, eventually ensures that material limits are respected at all times.

4) Structured Design for Automation of Processes

When thinking further about the process of automation in decision-making, it is important to consider which processes are carried out and in what time horizon, how much the process contributes to situational awareness of the operator [42], and how manual the process is within the time horizon.

An automated process may still require manual confirmation by the operator, in particular to select or validate and confirm non-trivial decision-making. Keeping the human in the loop should increase situational awareness. However, the operator confirmation might be omitted where fast response is required, possibly during some emergencies, and when an automated process continuously produces the expected outcome.

Ultimately, the level of process automation depends on the process being automated. For example, some straightforward processes can be fully automated and executed autonomously, while some can be automated only in parts or not at all. Nevertheless, the first step for any kind of process automation is to standardize the execution sequence and associated information exchange between the process steps. Moreover, the application that executes the process should be able to detect any inconsistencies in the process execution and process step failures with related reasons, and communicate to operators.

B. Structured Decision-making

1) A New Approach for Decision-making of Transmission Control Center

Transmission system operations have changed incrementally over the preceding decades and experienced operators have ingrained mental models for operations. However, if the system operating modes change, as predicted for the coming decades, operators may not be able to rely on existing mental models to solve new challenges. As an example, contingencies are generally slow to emerge, which is predictable, and thus operators typically have ready-made solutions. But with changing resource and demand mix, newer contingencies will emerge faster and unpredictably, meaning solutions may be more complex.

A better approach may be to equip operators with techniques to adjust to new paradigms and operation modes, so that they can think through problems and develop the optimal solution in a standardized manner. Structured decision-making frameworks also have the added benefit of being good proxies for task automation and artificial intelligence (AI) [43].

2) Framework of Rasmussen's Decision Ladder

The decision ladder was theorized and developed by Jens Rasmussen [44] and reproduced in Fig. 3, which shows the cognitive steps that operators require as they process information on the system.

It is a very effective model for how operators in high reliability control center make decisions in critical scenarios. The decision ladder is not intended to describe how the brain works to process information via human physiology, which is a realm of complexity beyond the scope of this paper. It is intended to define the states of knowledge and process activities that occur while an operator is facing a system challenge. The decision ladder starts as a linear process flow, starting with activation on the left and finishing with execution on the right. The innovation with the decision ladder comes with the "ending" of the process flow, to make the process visually more intuitive and to enable leaps between states, as can be observed in Fig. 3. Novice operators can start at bottom left and work their way through each state and process until they arrive at the execution action. When applying it to transmission operations, it should be obvious that:

1) Not all processes or tasks will require all steps of the ladder, hence there are in-built leaps from left to right.

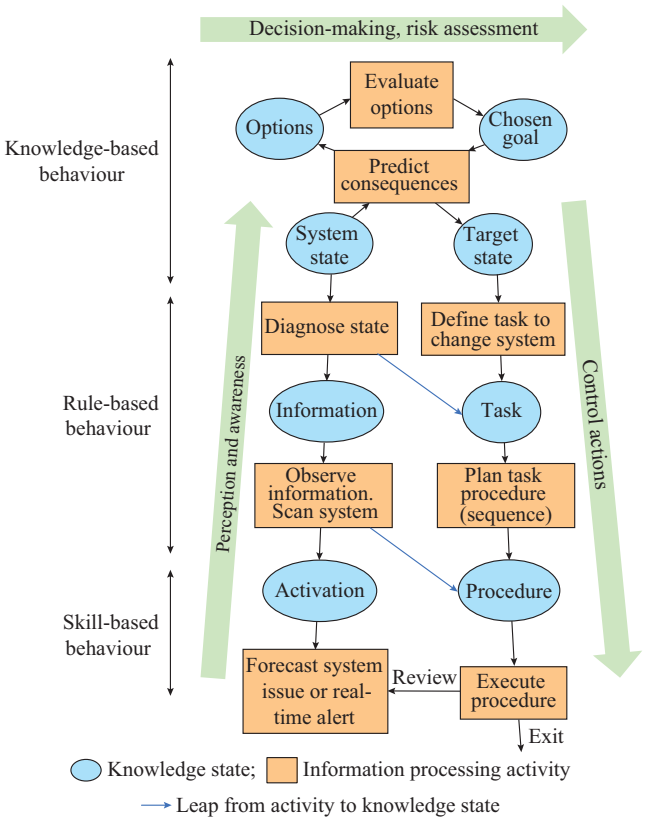

Fig. 3. Rasmussen's decision ladder with additional possible leaps by expert operators and a refreshed feedback loop when adapting ladder to forecasting for anticipation.

2) Experienced operators generally do not move through every stage of the ladder. Their inherent system knowledge and experience allow them to leap between stages or across the ladder, to fast track task execution.

3) The bottom level of the ladder represents "skill-based behaviour", or automatic response. The middle level of the ladder represents the "rule-based behaviour" or operators following procedures or checklists in response to an event. The top level of the decision ladder is the "knowledge-based behaviour", which relies on high cognitive workload and experience.

Ideally, operators should spend most of their time in the knowledge-based behaviour loop, diagnosing problems, optioneering, testing hypothesis, and assessing risk. Similarly in an automation scheme, this "simulation" and "validation" part of the algorithm might be the most computationally expensive.

3) Model Limitations

The decision ladder is serial in nature, thus it is a useful proxy for a single and independent manual task decomposition and automation such as voltage control. But in real-time operations, tasks are highly interconnected, so voltage control can be linked to asset monitoring, stability monitoring, contingency management, and generator monitoring. As multiple tasks also need to be completed in varying time periods, task prioritization is not included. These can be improved by a move from a serial supervision structure to hypervision interface, as shown in Sections III-C and V-A. Hy-

pervision would, in theory, takes the outputs of all serial processes in a control center and streamline decision-making and relevant information into one interface. But the decision support activity would be structured by the decision ladder. The system state, target state, option nodes of the decision ladder would take inputs from all processes, not just a single process, and the task, procedure, and execution would be optimized control actions for all the processes, not just a single process.

The original version of the decision ladder does not have a loop, review, or check stage (a review stage is added in the modified version in Fig. 3) to loop back in the ladder if needed or if there is still time before executing the decision. In the orginal ladder, when operators execute the task, it is expected for instance that the correct course of action was taken, and if there is an anomaly, the process starts again at the bottom left of the ladder. With a hypervision ladder representation and step-by-step progress logging and tracking, more incremental backward steps in the decision-making process could be more efficiently achieved without restarting the decision-making process from scratch.

C. Hypervision as a Unified and Simplified Smart Interface

Today's supervision over many screens and applications leaves the user the cognitive load to prioritize, organize, and link disparate displayed information and alarms before considering any decision or action. It can be regarded as a fragmented ecosystem from an operator's viewpoint. While it has been manageable for up to ten applications, it becomes impractical with more information to process and non-integrated applications under heterogeneous formats. It contributes to the problem of information overload and does not add context to system problems that need to be managed. This fragmented system dilutes the operator's attention while making tasks often not explicit, eventually leaving the operator connecting the dots. Human-machine interfaces and interactions were mostly disregarded in the past in the control centers, but they now need to be considered more carefully. Sub-optimal design of human-machine interfaces and interactions has been identified as a risk factor to human error in operations [45].

A single and unified interface should support the decision-making process, and prioritisation of tasks for the operator. A new "hypervision" scheme will likely be required for the future control center, which will define and represent individual tasks with their context providing: ① relevant context and the problem diagnosis associated with the left part of the decision ladder; ② possible recommended decisions associated with the top of the ladder; and ③ related plans, procedures, and execution means to apply the decision associated with the right of the ladder.

All applications would still be running in the background while the hypervision will aggregate information to be represented in a meaningful way for operators to take decisions. It will also prioritize tasks based on the urgency and the time horizon, not just real-time tasks. This will allow the definition of an expected operation trajectory monitored by the hypervision core. If it goes as expected, the operator can continue planning its future trajectories without worrying about real time. Otherwise, if some refreshed information requires adaptation of the defined trajectory, it will ask the operator for reconfiguration and suggest solutions. Finally, the hypervision core is one system for all operators through which tasks can be shared, coordinated, and tracked without any loss of information.

IV. Enabling Digital Platform Architecture

Typical control center systems, used nowadays to operate the power system, were initially designed to meet the system operation and control requirements defined in the late 1960s. The design practices of the first system were based on the available technology of that time. Nevertheless, the legacy of typical all-encompassing and centralised software solutions is often still present today in a form of a monolithic energy management system (EMS) or data management system (DMS), provided by one vendor. As the system outdates and expires, it gets typically completely replaced by a newer version, also bringing long-enduring and costly impacts on the organisation. Such customer specific maintenance is consuming a great deal of time and resources to adapt, integrate, and interconnect the new system with the existing processes and vice versa. Yet, that still leads to limitations due to vendor lock-in, in particular, with respect to the ability to continuously and simply adjust and extend the system functionality according to user needs.

However, as elaborated in Section II, the power system operation challenges and requirements have changed significantly and are expected to change even further, mainly as a result of the ever-evolving grids and energy markets, and wide-spread digitisation among others. Additionally, the necessity for system-wide security coordination and market transparency drives the need for more and more data and information exchange between stakeholders and market participants, respectively. In order to provide reliable, safe, and economically efficient energy supply today and in the future, and comply with regulation in all times, there is a need for continuous advancement and adaptation of control center functionalities and applications. To timely meet the increasingly complex requirements, there is a pressing need for a paradigm shift in the design of control center systems from typical monolithic, all-encompassing, and closed vendor solutions towards modular, decentralized, distributed, vendor-neutral, and open systems.

As discussed in [1], the future control center is characterised by the distributed, decentralized, integrated, flexible, and open-service-oriented information and communication technology architecture, ranging from dynamic provisioning of computation and communication resources, serving of data, event data processing, up to applications delivering various functionalities as services. Moreover, [2] outlines a smart transmission framework, spanning from substation over transmission system to control center, which delivers digitisation, flexibility, intelligence, resilience, sustainability, and customisation. Inspired by industry-leading implementation of modular control center system [46] by 50Hertz TSO, we build on top of [1], [2], [46], and present the concept of

data and application integration and modular platform for future control centers.

The main aim of the presented modular architecture is to provide high-level design directions of the digital platform with a goal to unlock: ① the potential of ever increasing operational and non-operational data; ② use of event-driven technologies for design of new applications; ③ seamless information exchange between modules via standardized interfaces; and ④ unbound flexibility with respect to maintainability of modules. Another benefit is the possibility to reuse the modules by other stakeholders, which also facilitates stakeholder collaboration and speeds up the innovation. Notably, the proposed platform can at first run in parallel to the existing legacy EMS or supervisory control and data acquisition (SCADA) system to complement the functionality, and over time in steps takes over the remaining legacy system functionality.

As visualized on Fig. 3, the proposed platform architecture consists of four layers, which are explained below. It is important to note that the layers also include modules of some key services/applications for example purposes only. Also, the platform is not limited to specific services/applications of control centers, but can be also used, for example, to host asset management and cyber-resilience related functionalities. Different instances of the platform can be used by different stakeholders, e.g., operator's training, as shown in Section VI-C. The platform modularity is particular suitable for the development of hypervision interface, as shown in Section V-A, including proactive decision support shown in Section VI-A) in the underlying modules with AI and other technologies shown in Section V.

A. Enabling Platform and Data Management Solutions

The first layer acts as a platform foundation spanning from the central location all to the edge (substations) and enabling ① data ingress and storage, ② real-time data analytic on the edge or central location to extract business value, ③ distributed applications, and ④ remote management of the platform components. One of the most promising platform implementation includes hybrid cloud, which is partly realised using on-premise and public cloud infrastructure offering additional gains in terms of resource flexibility and security, in particular, for disaster recovery. The on-premise part of the cloud infrastructure is used to host internal applications, spanning from the central location all to the edge in substations. Besides, the public part of the cloud infrastructure is used to accommodate energy market related services and data exchange gateways between stakeholders for grid security coordination and market transparency as examples. Then, a container management system can be used to ease and automate continuous integration, development, and scaling of various container-based applications anywhere in the hybrid cloud. On top of it, an event streaming platform enables high-performance data pipelining, real-time event and batch stream processing, and high availability of hosted (distributed) applications. This layer is particularly important for efficient design of data-driven online and offline event-based applications [47], where data are often first enriched, curated, stored, and reused in multiple end-user applications. Finally, a data storage and versioning solution in combination with master and meta data management is added, for example, using cutting-edge data mesh principles [48] to store, catalogue, and provide all operational and non-operational data for various applications. An interesting and matured example of such data platform is the open source available OSDU data platform [49], which is tailored to the needs of oil and gas industry.

B. Decentralized Business Supporting Services

The second layer includes various distributed yet centrally located business functions as services that are shared and fundamental for operation of multiple end-user applications. Examples include but are not limited to (static/hybrid) state estimation, operational and non-operational data storage, alarm management, and data exchange gateways for inter-TSO/DSO security coordination, energy market and transparency purposes. Next, it also includes decentralised functions that run on the cloud edge in substations, such as asset condition monitoring, asset data acquisition, distributed (dynamic) state estimation, and vitalized protection and control schemes. The crucial parts of this layer are open software development kit (SDK) and API, which enable simple application design and seamless data exchange for application integration and visualisation purposes, respectively.

C. Decentralized Intelligence

The third layer includes advanced applications for improved situational awareness and decision support, power system optimization and control, and energy market participation. Examples include but are not limited to (dynamic) security assessment and optimization, congestion management, event detection and analysis, load frequency controller, and optimal power flow. The hosted applications are residual anywhere in the cloud, typically near data sources, and make use of the various shared functions and services that are residual in the lower layer through using the shared API.

D. Smart Human-machine Interface

Finally, the top user engagement layer consists of a stateless intuitive front-end or cockpit, which is used to connect users and applications, allowing funneling of information and immersive performance overview of the whole power system down to the level of individual power system components, as well as effective decision-making as emphasized in Section III. The cockpit interface is stateless, meaning that it can be dynamically and automatically adapted to meet the user needs for optimal user experience and performance. A brain-computer interface or simpler bio-sensors could possibly be used to monitor workload and stress of a user and dynamically adapt the level of decision support offered by applications. Besides, the human-machine interfaces and interactions also support voice control or other advance interaction modalities for simple confirmation of actions and recording of user actions for logging purpose.

V. Emerging Technologies and Functionalities

A. Hypervision Interfaces

Hypervision interface, as a part of one cockpit module in Fig. 4, allows for centralizing real-time business events into a single place to avoid having multiple screens or softwares and offer the operator one single coherent interface. It enables structured decision-making by representing each decision-making process (or simply regarded as a task) as a digital card. An hypervision interface further displays such a feed of ordered cards to represent multiple tasks ordered by priority. When a card is selected in the feed, the details of the card are displayed: information about the state of the process instance in the third-party application that published it, available actions, etc. A card with versioning eventually represents the full life cycle of the decision ladder through which we can proceed step-by-step or backward.

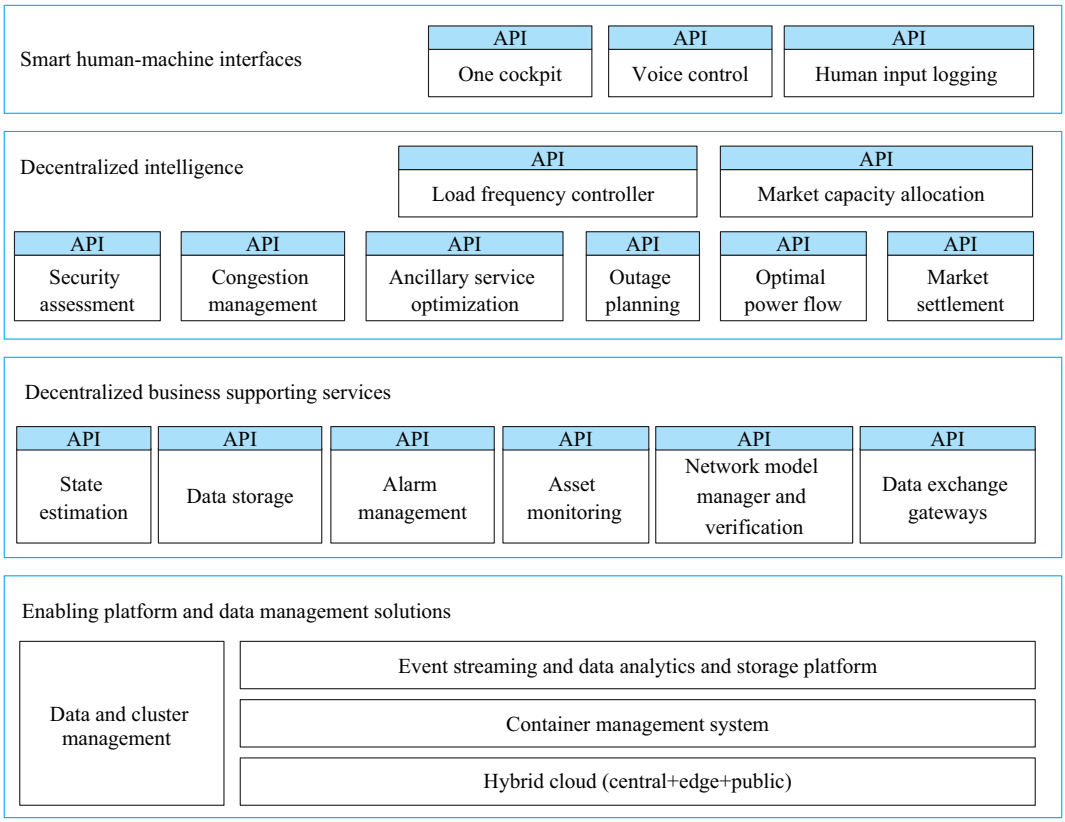

Fig. 4. Proposed enabling digital platform architecture featuring modular design and standardised API.

A card can first be automatically created and notified to the operator ahead of time based on forecasted alerts and contextual information, with a preliminary diagnosis. This can be refined and refreshed as refreshed forecasts or new information that comes in. Then recommendations for actions can be made available within the card or the operator can propose another one. The operator can further tag the card as representing a certain problem and objective. The operator can preferably select one option that will be considered as active. The card can eventually come with a procedure and configuration choices for execution. The card can then be send for automatic action execution on the grid once needed. A card can also be manually edited from scratch by the operator for more unusual situations. The card finally is shared across operators allowing for effective coordination.

As structured decision-making is applied to any field, hypervision interface frameworks in the end are applied to any industrial domain, only the underlying information management remains domain-specific. OperatorFabric [50] as shown in Appendix A Fig. A1 is such an example of a modular, extensible, and industrial-strength framework and interface developed on top of modern web technologies for use in electricity, water, and other utility operations. OperatorFabric embeds a routing mechanism to dispatch cards on a user basis (based on groups, organizational entities, processes, etc.). The cards can also translate as events are displayed on a timeline view or an agenda view. These views complement the card feed by allowing the operator to see at a glance the status of processes for a given period.

This solution facilitates the interactions between operation control centers, who can share information in real time, as pre-formatted cards that can be sent either manually by operators or automatically by external solutions.

B. AI

The goal of AI is to turn machines into intelligent agents that are able to learn from experience in order to optimally perform complex tasks [51]. AI can enhance the speed, precision, and effectiveness of human efforts by enabling decision support systems that complement and augment human

abilities. Moreover, human-centered AI that effectively cooperates and collaborates with people is increasingly needed, as shown in Section VI-A, instead of AI operating in isolation.

The most promising applications for using AI outside of the power system are within the domains of autonomous driving systems [52], [53], medical diagnosis and targeted treatment [54], [55], autonomous planning and scheduling [56], and climate science [57]. Some initial applications in these domains are already applied in the real world .

In the domain of power systems, the emerging AI methods are promising for future software tools to make stability analysis and control in smart grids tractable [58]. Within power systems, the key advancement is to unpack the complexity and uncertainty of the (real-time) operation and planning tasks as AI can process quickly large amounts of data. Driven by the much-needed energy transition (see e.g., Section II), power grid operation and planning are heavily shifted towards higher complexity and uncertainty as well as drastically increased state spaces and action spaces. In the energy transition, these spaces involve multiple scenarios and multiple time intervals (e.g., through the introduction of energy storage, electric vehicles, etc.), which increases the complexity of the operation and planning tasks. This increased complexity makes conventional stability analysis and control approaches too limited in terms of speed and effectiveness.

AI applications deliver initial but promising results that include online security assessment in multiple renewable energy scenarios, fault location identification under different operating conditions, stability control, or others [59]-[61]. Additional applications support building advanced knowledge graphs [62] to provide overall an augmented understanding of the system and its operations. The enabling digital platform architecture in Fig. 4 would allow the integration of AI capabilities within many of the highlighted functions thanks to APIs and modularity. Additionally, AI development would largely benefit from accessing multi-source data from all APIs.

However, AI applications still face several challenges in practice that are currently actively studied and developed, which relate to the methods or applications. The methodological challenges are, for instance, related to learning from imbalanced data, difficulties in transfer learning, or robustness against attack or adversarial examples. The application-specific challenges include high requirements on data (both quantity and quality), platform design for efficient and effective development and deployment in production, as shown in Section IV, a collaboration between the power systems and AI communities, and generally accepted and shared benchmarks. One specific challenge to use AI for critical tasks such as operation or planning of power systems relates to the trust required by operators before using tools with AI. Making AI trustworthy in a systematic way is highly important in critical infrastructure workflows. This means that on top of satisfying basic performance measures, AI needs to satisfy requirements related to reliability, human interaction, interpretability, and bias, and eventually offer explanations. Implementing a common language between human experts and machines such as ontologies [63] that describe the concepts over a knowledge graph could be one practical foundation to improve trust in AI.

C. CPSs and Cyber Security

Digitalization paves the way for energy transition towards carbon neutrality and energy system integration. The physical energy infrastructure, e.g., power plants, substations, and power lines, is increasingly dependent on operation technology (OT) systems and industrial IoT for real-time monitoring and control of the physical facilities. Utilities, aggregators, and service providers use high-speed information technology (IT) networks for business operations. It can be imagined that on top of the power infrastructure reside IT-OT network layers. Together they form a complex and interdependent CPS for the power system. CPS combines the cyber system comprising of communication, control, and computation functionalities with the physical world, which typically consists of a natural and/or man-made system governed by the laws of physics. Modern CPS involves multiple and complex physical subsystems with varying degrees of interactions via communication networks. Hence, their holistic analysis is a challenge that needs to be addressed, as comprehensively posited in [5]. New foreseen advanced control and automation schemes as proposed in parts 3 and 4 of Section III-A increase the cyber dimension of the system. Furthermore, it is increasingly difficult to keep the utility private communication networks isolated from the public communication networks. At the edge of grid, industrial IoT is deployed for data connectivity and easy market participation for all energy system participants. Opening the system to everyone by means of information and communication technologies requires careful considerations with regard to information security. The cyber security and resilience requirements of the power system become even more critical.

It is well recognized that information and communication technologies are vulnerable to cyber attacks. Examples of cyber security incidents related to power systems already exist around the world. On December 23, 2015, cyber attacks were conducted on the power grid in Ukraine. Hackers intruded into IT-OT systems of the control center of three DSOs. Attackers took control of the SCADA systems and disconnected seven 110 kV and twenty-three 35 kV substations from the grid for hours. The cyber attacks in Ukraine resulted in power outages, which affected 225000 customers [64]. More sophisticated cyber attacks on the Ukrainian power grid followed on December 17, 2016, which resulted in a power outage in the distribution network where the total unsupplied load was 200 MW. Such laborious cyber attacks conducted by powerful adversaries on control centers, substations, and edge of grid are a real threat to the security of power systems. They can initiate cascading failures and result in a blackout. With respect to security of supply and reliability of the future power system provision, special attention is needed for new cyber threats and vulnerabilities that come with the rapid digitalization of the power system. Accordingly, without consideration of cyber security and resil-

iency to cyber attacks, a further digitalization of the power system may be difficult. Cyber resilience is thus emerging as a key topic to ensure the security of supply and stable operation of the CPS. It is the ability of the power system to withstand and reduce the magnitude or duration of cyber attacks, which includes the capability to anticipate, absorb the shock, adapt, and rapidly recover.

Utilities play a central role in grid digitalization, spearheading the energy transition and energy system integration. They invest in cyber security solutions to secure the control centers from cybercrime and hacktivism. However, they are also the main targets of state-sponsored cyber attacks. Video evidence of the 2015 cyber attack in Ukraine shows an engineering workforce not adequately responding to attackers taking remote control of the power grid OT system and not knowing if it is a cyber attack or their own IT department is controlling the SCADA system. The kill chain of cyber attacks on power system operators typically starts by exploiting vulnerabilities in the utility IT system through phishing emails and similar methods. Malware is installed to open gateways and facilitate remote access for system reconnaissance, weaponization, and OT targeting. Attackers can intrude from the IT system into the OT system by stealing log-in credentials, escalating access privileges, and discovering networked OT systems and hosts. In the OT system, they can take control and tamper with the SCADA system, disconnect power plants and entire substations, and cause physical damage to power equipment by interfering with their control systems.

Segregating the IT-OT systems of control centers by using firewalls is not enough for the cyber security of power systems. Advanced mathematical and computational foundations, methods, and technologies are needed for incident response to protect utilities from state-sponsored cyber attacks to ensure cyber security of the future control room. Operation resilience of power systems to such cyber threats is achieved by combining innovative technologies, incident response strategies, and human factors. Furthermore, it is imperative to build trained human capital for grid operators to deal with the ever-growing cyber threats. Threat intelligence plays an important role in preventive and reactive cyber security. Utilities share knowledge among a network of trust via information sharing and analysis centers (ISACs). Cyber threat management is emerging as the best practice for managing threats beyond the basic risk assessment found in security information and event management systems.

D. Digital Twin (DT)

Dynamic analysis of a very large, fast, interconnected, and complex power system is currently only possible with numerical models. Despite calibration efforts, widely used physical-based models fail to be general and accurate enough for describing the system in any state of functioning, not capturing, for instance, system uncertainties, asset health status and life-cycle effects, cyber-interactions, or usual operation schemes. As defined in [65] and [66], the DT bridges the gap between physical-based design simulation of an asset or system and its exploitation during operation. DT is a virtual representation of a system (here the power system) and its physical assets supported by a combination of numerical models and powerful simulation hardware, representing cyber interactions and operations in addition to the physical assets. Depending on decision and on data available, physical-based models can be reduced for the real-time application and enriched with data by various machine learning (ML) techniques to capture life-cycle evolution [67]. Physics modeling is in some sense hybridized and augmented by data modeling.

DTs hence offer the possibility to connect and tune the digital models with measurements of the real assets to mimic the reality. A detailed and virtual replica of the power grid provides system operators with the enhanced capabilities for real-time prediction and fast and reliable decision support. It is foreseen in the next decade that DTs will be widely deployed for various industrial applications due to recent advances in parallel computing, solvers, data processing and management tools, big data, and AI [68], [69]. For example, [70] presents an application of real-time and high-fidelity DTs of physical components to develop, train, and validate ML models to secure critical infrastructures.

The wide-area monitoring system (WAMS), in addition to the conventional SCADA systems, greatly enhances the situational awareness since it provides information on the essential variables for system operation with a high resolution. This enables the near real-time monitoring of the dynamic power system phenomena and facilitates a dynamic security assessment (DSA). A DT mirrors the system state in real time and consolidates the control center system architecture. It improves the model accuracy by combining WAMS and DSA. The DT facilitates an operator assistant system for fast and reliable decision support [71].

DT may be part of the enabling digital platform given in Section IV as the modules used for cyber resilience analysis, planning, and operation of integrated CPS. They comprise of detailed discrete-time models of OT networks for substation automation and continuous-time models of the power system. The discrete-time systems are used to model and simulate the substation communication networks and processes. Therefore, DTs extend the current modeling, simulation, and analysis capabilities of power system planners from only a physical domain to the integrated cyber-physical domains. DTs allow the real-time simulation of cyber attacks at the cyber system layer and the impact analysis at the physical layer in an integrated co-simulation environment. Power system operators can assess and improve the grid operation resilience to cyber attacks and plan the cyber security operation of the integrated CPS. Cyber resilience should be an integral part of control center systems and should be taken into account when designing new EMS applications.

E. Real-time DSA

New operating tools for advanced monitoring in support of managing the operational reliability are needed in order to improve the situational awareness in a system growing in complexity, decentralization, and uncertainty [9]. Reliability management fulfills two functions of adequacy and security.

Planning for adequacy is to ensure that the probability is high enough to supply electricity which is evaluated over months and years. Security refers to the imminent and real-time operation risk to survive imminent disturbances without service interruptions, and involves the assessment of security and real-time control actions.

When assessing the dynamic security, a model that considers equipment failures such as the failure of a generator or a transmission line is simulated by current tools. While DTs consider rather active type of simulations and have a broad capability supporting active decision-making including modeling the entire intelligence of system operations, the simulations for security assessments are rather passive. An analysis of the post-fault simulation results provides the security information. Unfortunately, with current tools, the computational time is too long to analyze many faults (combinations) for possible operating conditions in real time. Hence, the tools limit the DSA to offline studies, which makes the simulation results inaccurate and unsuitable for real-time DSA. The reason for such long computational time is that the methods that underlie the current tools rely on numerical integration that solves the dynamical model described by ordinary differential equations (ODEs) in the time domain [72]. Several alternative methods aim at reducing the computational time. The Kron method [73] and the single-machine equivalent method [74] reduce the dynamical model which is then simulated. The energy function method theoretically analyzes the stability [75]. Special hardware can further reduce the computational time [76]. These aforementioned methods simplify the power networks and in some cases can be useful; however, they have respective limitations, mostly in their applicability to larger interconnected systems which can have novel equipment integrated.

New promising AI and ML methods for real-time assessment of security and control (preventive and corrective) of reliability are emerging [77], [78]. The approach is to train an ML model offline when the computational time for simulations is abundant, and use the trained model to predict security and control actions in real time immediately before a fault or in response to it. Such methods are promising for real-time operation [79], [80] as their prediction requires minimal computational time, but have challenges related to the generation of training data [81], the interpretability of the prediction [82], their risks and probabilities of success [83], and their usability to other operating conditions and topologies [84], etc. Recently promising methods use the known dynamical model, i.e., the ODEs, to inform directly the ML training which can reduce the demands for training data [85], [86]. Real-time DSA could soon become a reality and upgrade the security assessment module of Fig. 4.

VI. New Operation Perspectives

A. Proactive and Assisted Decision Support for Operations

Operators will get assisted through an hypervision interface with smart recommendations, continuous situational awareness of projected operational trajectories augmented by AI, as shown in Section V-B, and in the end more automatic execution functions when actions get implemented. Operators can choose when to delegate further a task to the hypervision assistant at any step of the decision ladder if appropriate. This goes in the direction of semi-automation as described by [71]. But how much operators will remain in the loop?

A usual trend when going through more automation while not considering the demands for human decision-making is to see operators slowly going towards on-the-loop mere verification of recommendation (much like security scanner airport operators), hence moving from strong human operation intelligence to strong machine intelligence. Not to mention an unrealistic target of eventually getting them out of the loop of a fully autonomous grid. While on the loop, an operator will be prone to anchoring bias (i.e., over-relying on the first piece of given information) and automation bias (i.e., accepting without thinking the single recommendation displayed) [87]. This brings the risks of deskilling, perverse instantiation [88], and fast crashes because of misunderstandings, misalignment, or relevant information not yet considered by the machine.

An assistant [89] should be able to dialog consistently with an operator over iterative interactions and refinements, through queries, explanations, and context considerations, going beyond single-shot interactions. How humans perceive machines should also be considered [90] for appropriate design. Fluid, well-conceived, and more transparent interactions [91] will build up necessary trust between operators and assistant [92].

Resulting hybrid intelligence [93] would eventually be a more desirable path by developing true human-machine partnerships [94] with synergetic interactions, where the human and the machine would continuously learn from one another, sharing knowledge and representations. In that prospect, it will be essential to regularly think of the role and task dynamics of the grid operator in her environment [95] to allow for the proper interactions to drive her decision-making.

More specifically, Fig. 5 summarizes three relevant dimensions that need to be taken into account when developing hybrid intelligence. The first dimension is concerned with "knowledge and information support" which in a rudimentary form is already present in current control rooms. For example, operators are currently provided with basic summaries of the real-time and near-future situations. However, the related functionalities can still greatly be enhanced by, for instance, offering apprehension of complex and atypical situations or by more targeted syntheses of events. The other two dimensions, which are unprecedented in current control rooms and will greatly enhance decision support, are focused on fine-tuned "interactions with the operators" (operator in-the-loop) and "assisted decision-making" (decision) via situated explanations and action recommendations. Overall, it would enable shared knowledge representations and situational awareness over relevant time-horizon, to allow for contextual collaborative decision-makings through adapted interactions. Practically speaking, we think that there is no necessary development sequence of these dimensions, but elements of each dimension can be developed directly with the

advice to include (feedback by) the operators early in the development process. DT availability shown in Section V-D could accelerate its development.

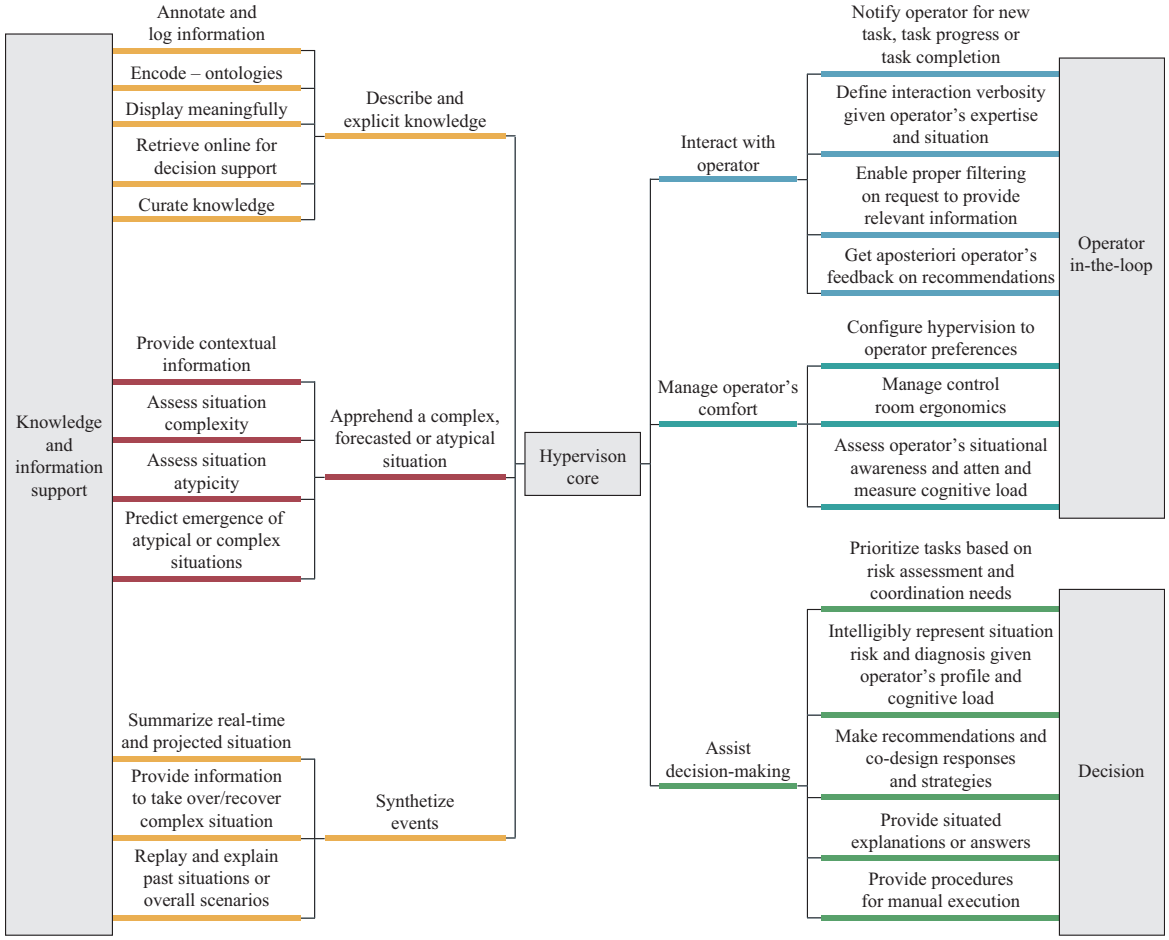

Fig. 5. Desired functionalities for an operator when designing proactive decision support through hypervision.

In summary, hybrid intelligence essentially represents a form of human-in-the-loop decision-making in which assessing the operator's situation and vivid human-machine interactions are key. For instance, different underlying strategies for human-machine interface design, annotation, and data sampling continuously need to be aligned [96]. Consequently, a human-centered approach requires iterative and interactive development, as developed in Section IV, such that the hybrid intelligence can constantly adapt to new demands of operators. This is also key for establishing trust of the operators in the decision support system.

B. Risk-based Security Paradigm Shift for Operator Planners

The current operating paradigm is to assess the steady-state security of power system operation with $N-1$ security, meaning to study when single fault occurs at maximal at the same time. The assumptions of this paradigm are no longer suitable [97] as it does not take into account the increasing dynamics of the probability of faults, nor the increasing probability of cascading faults [98]. Also, implementing renewables with power electronic converters results in lowered inertia and shorter time intervals for escalating dynamics [99]. As mentioned in Section III, operators become planners over extended time horizon in real-time anticipation. In this challenging future, probabilistic paradigms are suitable to replace the $N-1$ based security criterion which might not be realistically met anymore under all possible uncertainties making this criterion outdated. But this requires computing accurately the operation risks [83], [100], [101] over this time horizon. Current state-of-the-art tools show limited suitability to efficiently support a probabilistic operation paradigm; however, several promising methods are emerging for DSA, as explored in Section V-D. Automation may also introduce different types of risks that operators have to follow up. In the past, errors have been made in modeling and decision-making, and the assumptions for operating tools for specific tasks had inaccuracies, resulting in risks. Hence, operators includes safety margins to ensure a secure operation. When moving towards more automation of control centers, new risks arise from that automation and coordination. As shown through the GARPUR European project [102], proxies of the tasks and automated parts of the system allow for a probabilistic quantification of the automation.

The new probabilistic paradigm for security assessment can be used to quantify risks [103], allowing operators for a higher level of automation and integration. The probabilistic paradigm is to consider uncertainties and analyze a large set

of possible contingencies considering their probabilities, instead of analyzing a limited set of "credible" contingencies securing determinacy against them [104]. The contingencies with the highest risks are flagged to the human operator [83]. In this paradigm the risk becomes quantifiable by the severity of contingency and the probability of contingency. The objective of the paradigm is then to minimize the residual risk by making risk-aware decisions. The risks take into account physical [105], socio-economic [101], end-consumer [106], or directly system-security [105] dimensions. While the paradigm shift from deterministic operating paradigm to probabilistic paradigm is demonstrated to provide significant benefits, such a shift would nonetheless require profound changes in operation practices, which should be supported by new training programs, revised testing procedures, and changes to technical operation data collection such as estimating accurately the likelihood of contingencies where some approaches exist to address this challenge as it depends on weather and asset health [107].

C. Realistic Testing and Training Simulator

As the system becomes more complex, especially considering the current numerous cyber and multi-agent interactions, as well as rapidly evolving technologies and applications, comprehensive and continuous testing and training become of utmost importance. Continuous testing of new functionalities also helps speed up acceptance and improve the users' satisfaction. As a healthy check, a process which we cannot be tested on demand is probably too complex to manage and should probably not be eligible for deployment. Testing should support proper design of application ecosystem development and ensure that this still make the system predictable and controllable enough to be run under various operating conditions (normal, emergency, cyber attack) or in degraded modes. Continuous training should be offered to operators to learn how to best use evolving applications, revise their intuitions and understanding of changing system behavior, and best coordinate with various operators under different configurations.

Several testing layers discussed are needed: in-silico, in-vitro, and in-vivo. Lots of physical testing processes and hardware have already existed for years for in-vitro lab testing over small-scale systems or replica as in RTDS or OPAL-RT. Parallel runs have also been done punctually in control rooms when bringing in some new applications to be validated by operators. This often requires lots of preparation, and yet only covers a reduced set of system conditions: the ones encountered during this operation testing period. More systematic and continuous in-vitro lab testing is therefore needed, especially through comprehensive "shadow control room", as a replica of real control room (EMS/IT, audio/video/human ergonomics), with added grid simulation capabilities that can be reconfigured very quickly for tests and experiments only. Evaluations of ergonomics and decision support tools and processes could be more rigorously tested in regard to their impact on operator's decision-making.

In-vivo lab testing also becomes more necessary to regularly assess the proper configuration of different control layers, as well as underlying asset reliability and health. As the power system needs to run continuously without interruption, invasive in-vivo lab testing have been regarded as risky and not considered extensively. Nonetheless, the open-and-close reliability testing of breakers through periodic maneuvers, power system stabilizer (PSS) power plant controller testing, as well as primary reserve frequency control verification are examples of existing in-vivo lab testing. New and more numerous in-vivo testing could be implemented to test cyber system behavior over different scales possibly in the form of frequently planned on-off asset maneuvers under different but secure system conditions. These controlled interventions should also help test the accuracy of predictive models and grid models at the core of decision support tools.

Finally, in-silico testing also comes as a new opportunity thanks to the developments of virtualisation and DTs shown in Section V-D to replay real environments, much like flight or car simulators. In particular, collections of real edge cases when captured can be simulated to be systematically tested over and over as done for autonomous vehicle development. Combined with comprehensive knowledge bases and artificial agent allowing one to virtually run operation scenarios realistically and automatically, it can test the potential of new designs or functionalities for cheap. This also limits more demanding in-vitro or in-vivo testing.

Such in-silico environments can also form the basis of advance operator's training simulator (OTS). Instead of artificial agents virtually running power system operation scenarios, human operator could just simply run these on their own with the available decision support tool to test their decisions and learn about the behavior of contextual systems. This goes beyond today's existing OTS limited to single canonical snapshots and low-level actions (without use of support decision tool) instead of full contextual scenarios over time with possible high-level strategies. Human operators would also learn and train themselves by watching "games" from others, either human or artificial agents. Depending on their level of expertise, specific play or games could be recommended to them. OTS should quantify and compare the operators' performance, assessing their strength and making recommendations for improvements. Finally, it should have future operators trained in multi-domain and in coordination with other agents, either other human operators or artificial assistants.

VII. Conclusion

In this paper, we present the transformative perspectives of future control centers to handle the operation consequences of ongoing and upcoming changes in the power system through the energy transition. Control centers will have to evolve continuously to adapt. Consequently, we propose an enabling digital platform architecture to unlock the potential of data, the integration of emerging technologies, and the design of new applications and their flexible integration in an always extending ecosystem. We also highlight the evolving roles of the operators as planners and coordinators. It is supported by additional automation, but also importantly by a new approach for decision-making. We indeed propose the

integration of hypervision, a simplified and unified interface for all operators that instantiates structured decision-making framework based on the Rasmussen's decision ladder. Some hypervision frameworks already exist and could be deployed in a very near future. Complemented with upcoming technologies such as AI and DTs, one perspective is to develop a comprehensive and collaborative artificial assistant for the operators within the next decade while relying on advance probabilistic security assessment. This security paradigm shift may require a profound cultural change for operators and within the company at the same time, which should be conducted as early as possible. Retraining the operators will be needed. More generally, continuous training and learning should become necessary to keep operating an always evolving system. New advance training simulator integrating all discussed dimensions should be developed. It could be further used as a testbed for experimenting the effectiveness of the new design, and hence be a fruitful intermediate milestone. In parallel, extending the testing capabilities of the system, applications, and processes before integrating this new level of complexity is as usual mandatory. The culture of testing should be enlarged and reinforced within the companies. Testing should eventually be run continuously. In the end, succeeding at the proposed control center transformation will depend on the close collaboration between stakeholders, research institutions, vendors, and possibly open communities.

APPENDIX A

Fig. A1. Hypervision interface of OperatorFabric with feed of cards, selected card details, and timeline.

REFERENCES

[1] F. Wu, K. Moslehi, and A. Bose, "Power system control centers: past, present, and future," *Proceedings of the IEEE*, vol. 93, no. 11, pp. 1890-1908, Jun. 2005.

[2] F. Li, W. Qiao, H. Sun *et al*., "Smart transmission grid: vision and framework," *IEEE Transactions on Smart Grid*, vol. 1, no. 2, pp. 168-177, Jun. 2010.

[3] S. Abram and A. Silvast. (2021, May). Flexibility of real-time energy distribution: the changing practices of energy control rooms. [Online]. Available: https://www. researchgate. net/publication/351853073_Flexibility_of_real-time_energy_distribution_the_changing_practices_of_energy_control_rooms

[4] ENTSO-E. (2021, Apr.). ENTSO-E position paper on assessment of future flexibility needs. [Online]. Available: https://www. entsoe. eu/2021/12/02/entso-es-position-paper-on-the-assessment-of-future-flexibility-needs/

[5] F. Allgöwer, J. B. de Sousa, J. Kapinski *et al*., "Position paper on the challenges posed by modern applications to cyber-physical systems theory," *Nonlinear Analysis: Hybrid Systems*, vol. 34, pp. 147-165, May 2019.

[6] M. Bartos, M. Chester, N. Johnson *et al*., "Impacts of rising air temperatures on electric transmission ampacity and peak electricity load in the united states," *Environmental Research Letters*, vol. 11, no. 11, p. 114008, Nov. 2016.

[7] T. T. Mai, P. Jadun, J. S. Logan *et al*., "Electrification futures study: scenarios of electric technology adoption and power consumption for the United States," National Renewable Energy Lab (NREL), Golden, USA, Tech. Rep., 2018.

[8] H. de Coninck, A. Revi, M. Babiker *et al*. (2018, May). Strengthening and implementing the global response. [Online]. Available: http://www.ipcc.ch/report/sr15/

[9] P. Panciatici, G. Bareux, and L. Wehenkel, "Operating in the fog: security management under uncertainty," *IEEE Power and Energy Magazine*, vol. 10, no. 5, pp. 40-49, Aug. 2012.

[10] P. Panciatici, W. Leader, C. Pache *et al*., "e-highway 2050 modular development plan of the pan-European transmission system 2050," European Commission, Brussels, Belgium, Tech. Rep., 2016.

[11] M. O'Malley, T. Bowen, J. Bialek *et al*., "Enabling power system transformation globally: a system operator research agenda for bulk power system issues," *IEEE Power and Energy Magazine*, vol. 19, no. 6, pp. 45-55, Nov. 2021.

[12] M. Panteli and P. Mancarella, "The grid: stronger, bigger, smarter? Presenting a conceptual framework of power system resilience," *IEEE Power and Energy Magazine*, vol. 13, no. 3, pp. 58-66, Apr. 2015.

[13] R. Leonhardt, B. Noble, G. Poelzer *et al*., "Advancing local energy transitions: a global review of government instruments supporting community energy," *Energy Research & Social Science*, vol. 83, pp. 1-11, Jan. 2022.

[14] G. Mendes, J. Nylund, S. Annala *et al*. (2018, Jun.). Local energy markets: opportunities, benefits, and barriers. [Online]. Available: https://www. researchgate. net/publication/325851921_Benefits_Barriers_and_Opportunities

[15] G. Strbac, N. Hatziargyriou, J. P. Lopes *et al*., "Microgrids: enhancing the resilience of the european megagrid," *IEEE Power and Energy Magazine*, vol. 13, no. 3, pp. 35-43, May 2015.

[16] P. Palensky and D. Dietrich, "Demand side management: demand response, intelligent energy systems, and smart loads," *IEEE Transactions on Industrial Informatics*, vol. 7, no. 3, pp. 381-388, Jun. 2011.

[17] S. Chatzivasileiadis and D. Ernst. (2017, Jan.). The state of play in cross-border electricity trade and the challenges towards a global electricity market environment. [Online]. Available: https://www.researchgate.net/publication/325869318_The_state_of_play_in_cross-border_electricity_trade_and_the_challenges_towards_a_global_electricity_market_environment

[18] A. Bublitz, D. Keles, F. Zimmermann *et al*., "A survey on electricity market design: insights from theory and real-world implementations of capacity remuneration mechanisms," *Energy Economics*, vol. 80, pp. 1059-1078, May 2019.

[19] P. F. Borowski, "Zonal and nodal models of energy market in European Union," *Energies*, vol. 13, no. 16, p. 4182, Aug. 2020.

[20] E. Parliament. (2021, Mar.). EU hydrogen policy hydrogen as an energy carrier for a climate-neutral economy. [Online]. Available: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689332

[21] European Commission. (2017, Jun.). "Commission regulation (EU) 2017/2195 of 23 November 2017 establishing a guideline on electricity balancing. [Online]. Available: https://eur-lex. europa. eu/legal-content/EN/TXT/?uri=CELEX%3A32017R2195

[22] L. Hirth, J. Mühlenpfordt, and M. Bulkeley, "The ENTSO-E transparency platform – a review of Europe's most ambitious electricity data platform," *Applied Energy*, vol. 225, pp. 1054-1067, Sept. 2018.

[23] L. Hirth, "Open data for electricity modeling: legal aspects," *Energy Strategy Reviews*, vol. 27, p. 100433, Jan. 2020.

[24] H. Sharma, "Role of social media during the COVID-19 pandemic: beneficial, destructive, or reconstructive?" *International Journal of Academic Medicine*, vol. 6, no. 2, pp. 70-75, Jun. 2020.

[25] S. M. Amrr, M. J. Asghar, I. Ashraf *et al*., "A comprehensive review of power flow controllers in interconnected power system networks," *IEEE Access*, vol. 8, pp. 18036-18063, Jan. 2020.

[26] H. Diaz and C. G. Soares, "Review of the current status, technology and future trends of offshore wind farms," *Ocean Engineering*, vol. 209, p. 107381, Aug. 2020.

[27] D. K. Mohanta, C. Murthy, and D. S. Roy, "A brief review of phasor

measurement units as sensors for smart grid," *Electric Power Components and Systems*, vol. 44, no. 4, pp. 411-425, Feb. 2016.
[28] G. Bedi, G. K. Venayagamoorthy, R. Singh *et al*., "Review of Internet of things (IOT) in electric power and energy systems," *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 847-870, Feb. 2018.
[29] E. Fernandez, I. Albizu, M. Bedialauneta *et al*., "Review of dynamic line rating systems for wind power integration," *Renewable and Sustainable Energy Reviews*, vol. 53, pp. 80-92, Jan. 2016.
[30] F. R. S. Sevilla, Y. Liu, E. Barocio *et al.*, "State-of-the-art of data collection, analytics, and future needs of transmission utilities worldwide to account for the continuous growth of sensing data," *International Journal of Electrical Power & Energy Systems*, vol. 137, p. 107772, May 2021.
[31] J. E. Sullivan and D. Kamensky, "How cyber-attacks in Ukraine show the vulnerability of the US power grid," *The Electricity Journal*, vol. 30, no. 3, pp. 30-35, Apr. 2017.
[32] S. Patel. (2021, Dec.). 2021: a dark year for electricity security, reliability. [Online]. Available: https://www. powermag. com/2021-a-dark-year-for-electricity-security-reliability/
[33] J. M. Birkebæk and E. M. Carlini, "Regional coordination of power system operations," in *Proceedings of 2018 IEEE International Conference on Environment and Electrical Engineering and 2018 IEEE Industrial and Commercial Power Systems Europe (EEEIC/I&CPS Europe)*, Palermo, Italy, Jun. 2018, pp. 1-6.
[34] A. G. Givisiez, K. Petrou, and L. F. Ochoa, "A review on TSO-DSO coordination models and solution techniques," *Electric Power Systems Research*, vol. 189, p. 106659, Dec. 2020.
[35] F. Capitanescu, "TSO-DSO interaction: active distribution network power chart for TSO ancillary services provision," *Electric Power Systems Research*, vol. 163, pp. 226-230, Oct. 2018.
[36] ENTSO-E. (2020, May). Research, development innovation roadmap 2020-2030. [Online]. Available: https://www. entsoe. eu/2020/10/14/entso-e-research-development-innovation-roadmap-2020-2030/
[37] M. Alizadeh, M. P. Moghaddam, N. Amjady *et al*., "Flexibility in future power systems with high renewable penetration: a review," *Renewable and Sustainable Energy Reviews*, vol. 57, pp. 1186-1193, May 2016.
[38] A. Akrami, M. Doostizadeh, and A. F., "Power system flexibility: an overview of emergence to evolution," *Journal of Modern Power Systems and Clean Energy*, vol. 7, no. 5, pp. 987-1007, Sept. 2019.
[39] A. Clark, C. J. Pavlovski, and J. Fry, "Transformation of energy systems: the control room of the future," in *Proceedings of 2009 IEEE Electrical Power Energy Conference (EPEC)*, Montreal, Canada, Oct. 2009, pp. 1-6.
[40] M. I. Alizadeh, M. Usman, and F. Capitanescu, "Toward stochastic multi-period AC security constrained optimal power flow to procure flexibility for managing congestion and voltages," in *Proceedings of 2021 International Conference on Smart Energy Systems and Technologies (SEST)*, Vaasa, Finland, Sept. 2021, pp. 1-6.
[41] E. Karangelos and L. Wehenkel, "An iterative AC-SCOPF approach managing the contingency and corrective control failure uncertainties with a probabilistic guarantee," *IEEE Transactions on Power Systems*, vol. 34, no. 5, pp. 3780-3790, Mar. 2019.
[42] Y. Liu, J. Liu, G. Taylor *et al*., "Situational awareness architecture for smart grids developed in accordance with dispatchers thought process: a review," *Frontiers of Information Technology & Electronic Engineering*, vol. 17, no. 11, pp. 1107-1121, Nov. 2016.
[43] Electric Power Resarch Institute. (2021, May). Structured decision-making techniques in transmission control centers. [Online]. Available: https://www.epri.com/research/products/000000003002019185
[44] J. Rasmussen. (1985, Jul.). A framework for cognitive task analysis in systems design. [Online]. Available: https://link. springer. com/chapter/10.1007/978-3-642-50329-0_12
[45] E. Flaspöler, A. Hauke, P. Pappachan *et al*. (2009, Aug.). The human machine interface as an emerging risk. [Online]. Available: https://op. europa. eu/en/publication-detail/-/publication/1195a30e-bd64-4ff1-a9bd-ec24ce74619c
[46] M. Pracht and R. Heisig. (Mar. 2021). Modular control centre system: the next generation. [Online]. Available: https://f.hubspotusercontent30. net/hubfs/8156085/Mirko%20Pracht%20and%20Ralf%20Heisig%20-%2050Hertz.pdf
[47] C3 AI. (2020, Jul.). White paper: a new technology stack. [Online]. Available: https://c3. ai/digital-transformation/a-new-technology-stack-white-paper/
[48] I. A. Machado, C. Costa, and M. Y. Santos, "Data mesh: concepts and principles of a paradigm shift in data architectures," *Procedia Computer Science*, vol. 196, pp. 263-271, Jan. 2022.
[49] The Open Group Community Projects. (2021, Apr.). Open subsurface data universe (OSDU) software. [Online]. Available: https://community. opengroup.org/osdu
[50] LFEnergy. (2019, Jul.). Operator fabric: a smart assistant for system operators. [Online]. Available: https://opfab.github.io/
[51] S. Russell and P. Norvig, *Artificial Intelligence: a Modern Approach*. New York: Pearson, 2021.
[52] S. Grigorescu, B. Trasnea, T. Cocias *et al*. (2019, Nov.). A survey of deep learning techniques for autonomous driving. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/rob.21918
[53] Tesla. (2021. Mar.). Artificial intelligence & autopilot. [Online]. Available: https://www.tesla.com/AI
[54] X. L. Mbchb, L. F. Md, A. U. Mbchb *et al*., "A comparison of deep learning performance against health-care professionals in detecting diseases from medical imaging: a systematic review and meta-analysis," *The Lancet Digital Health*, vol. 1, no. 6, pp. 271-297, Oct. 2019.
[55] E. Topol, *Deep Medicine: How Artificial Intelligence Can Make Healthcare Human Again*. New York: Basic Books, 2019.
[56] J. Barreiro, M. Boyce, M. Do *et al.*, "Europa: a platform for AI planning, scheduling, constraint programming, and optimization," in *Proceedings of 4th International Competition on Knowledge Engineering for Planning and Scheduling (ICKEPS)*, Toronto, Canada, Jun. 2012.
[57] D. Rolnick, P. L. Donti, L. H. Kaack *et al.*, "Tackling climate change with machine learning," *ACM Computing Surveys*, vol. 55, no. 2, pp. 1-96, Jan. 2022.
[58] F. Li and Y. Du, "From alphago to power system AI: what engineers can learn from solving the most complex board game," *IEEE Power and Energy Magazine*, vol. 16, pp. 76-84, Mar. 2018.
[59] Z. Shi, W. Yao, Z. Li *et al*., "Artificial intelligence techniques for stability analysis and control in smart grids: methodologies, applications, challenges and future directions," *Applied Energy*, vol. 278, p. 115733, Nov. 2020.
[60] A. Marot, B. Donnot, C. Romero *et al.*, "Learning to run a power network challenge for training topology controllers," *Electric Power Systems Research*, vol. 189, p. 106635, Jun. 2020.
[61] A. Marot, B. Donnot, G. Dulac-Arnold *et al.* (2021, August). Learning to run a power network challenge: a retrospective analysis. [Online]. Available: http://proceedings.mlr.press/v133/marot21a/marot21a.pdf
[62] H. Huang, Z. Hong, H. Zhou *et al*., "Knowledge graph construction and application of power grid equipment," *Mathematical Problems in Engineering*, vol. 2020, pp. 1-10. Oct. 2020.
[63] L. Crochepierre, L. Boudjeloud-Assala, and V. Barbesant. (2020, Sept.). Interpretable dimensionally-consistent feature extraction from electrical network sensors. [Online]. Available: https://link. springer. com/chapter/10.1007/978-3-030-67667-4_27
[64] D. Whitehead, K. Owens, D. Gammel *et al*., "Ukraine cyber-induced power outage: analysis and practical mitigation strategies," in *Proceedings of Annual Conference for Protective Relay Engineers (CPRE)*, Texas, USA, May 2017, pp. 1-8.
[65] M. Grieves and J. Vickers, "Digital twin: mitigating unpredictable, undesirable emergent behavior in complex systems," in *Transdisciplinary Perspectives on Complex Systems.* Hobken: Springer, 2017, pp. 85-113.
[66] S. Boschert, C. Heinrich, and R. Rosen, "Next generation digital twin," in *Proceedings of TMCE*, Las Palmas de Gran Canaria, Spain, Apr. 2018, pp. 7-11.
[67] F. Chinesta, E. Cueto, E. Abisset-Chavanne *et al*., "Virtual, digital and hybrid twins: a new paradigm in data-based engineering and engineered data," *Archives of Computational Methods in Engineering*, vol. 27, no. 1, pp. 105-134, Nov. 2018.
[68] A. Rasheed, O. San, and T. Kvamsdal, "Digital twin: values, challenges and enablers from a modeling perspective," *IEEE Access*, vol. 8, pp. 21980-22012, Jan. 2020.
[69] Y. Wu, K. Zhang, and Y. Zhang, "Digital twin networks: a survey," *IEEE Internet of Things Journal*, vol. 8, no. 18, pp. 13789-13804, Sept. 2021.
[70] B. Sousa, M. Arieiro, V. Pereira *et al*., "Elegant: security of critical infrastructures with digital twins," *IEEE Access*, vol. 9, pp. 107574-107588, Jul. 2021.
[71] C. Brosinsky, R. W. D. Sennewald, and T. Krebs, "An operator assistant system for fast and reliable decision support based on a dynamic digital mirror," in *Proceedings of CIGRE Session 48*, Paris, France, Jul. 2020 pp. 1-11.
[72] H. Gould, J. Tobochnik, and W. Christian, "An introduction to computer simulation methods," *Computer Physics*, vol. 10, pp. 652-653, Jul. 2007.
[73] F. Dorfler and F. Bullo, "Kron reduction of graphs with applications to electrical networks," *IEEE Transactions on Circuits and Systems I:*

Regular Papers, vol. 60, no. 1, pp. 150-163, Sept. 2012.
[74] M. Pavella, D. Ernst, and D. Ruiz-Vega, *Transient Stability of Power Systems: a Unified Approach to Assessment and Control*. Hobken: Springer Science & Business Media, 2012.
[75] T. L. Vu and K. Turitsyn, "Lyapunov functions family approach to transient stability assessment," *IEEE Transactions on Power Systems*, vol. 31, no. 2, pp. 1269-1277, May 2015.
[76] I. Nagel, L. Fabre, M. Pastre *et al*., "High-speed power system transient stability simulation using highly dedicated hardware," *IEEE Transactions on Power Systems*, vol. 28, no. 4, pp. 4218-4227, May 2013.
[77] K. Sun, S. Likhate, V. Vittal *et al*., "An online dynamic security assessment scheme using phasor measurements and decision trees," *IEEE Transactions on Power Systems*, vol. 22, no. 4, pp. 1935-1943, Oct. 2007.
[78] L. Duchesne, E. Karangelos, and L. Wehenkel, "Recent developments in machine learning for energy systems reliability management," *Proceedings of the IEEE*, vol. 108, no. 9, pp. 1656-1676, Sept. 2020.
[79] I. Konstantelos, G. Jamgotchian, S. H. Tindemans *et al*., "Implementation of a massively parallel dynamic security assessment platform for large-scale grids," *IEEE Transactions on Smart Grid*, vol. 8, no. 3, pp. 1417-1426, Sept. 2016.
[80] B. Donnot, I. Guyon, M. Schoenauer *et al*. (2018. Aug.). Fast power system security analysis with guided dropout. [Online]. Available: https://arXivpreprintarXiv:1801.09870
[81] F. Thams, A. Venzke, R. Eriksson *et al*., "Efficient database generation for data-driven security assessment of power systems," *IEEE Transactions on Power Systems*, vol. 35, no. 1, pp. 30-41, Jan. 2020.
[82] J. L. Cremer, I. Konstantelos, and G. Strbac, "From optimization-based machine learning to interpretable security rules for operation," *IEEE Transactions on Power Systems*, vol. 34, no. 5, pp. 3826-3836, Apr. 2019.
[83] J. L. Cremer and G. Strbac, "A machine-learning based probabilistic perspective on dynamic security assessment," *International Journal of Electrical Power & Energy Systems*, vol. 128, p. 106571, Jun. 2021.
[84] F. Bellizio, J. L. Cremer, and G. Strbac, "Machine-learned security assessment for changing system topologies," *International Journal of Electrical Power & Energy Systems*, vol. 134, p. 107380, Jan. 2022.
[85] G. S. Misyris, A. Venzke, and S. Chatzivasileiadis, "Physics-informed neural networks for power systems," in *Proceedings of 2020 IEEE PES General Meeting (PESGM)*, Virtual Event, USA, May 2020, pp. 1-5.
[86] J. Stiasny, G. S. Misyris, and S. Chatzivasileiadis. (2021, Jul.). Transient stability analysis with physics-informed neural networks. [Online]. Available: https://arXiv:2106.13638
[87] D. Kahneman, *Thinking, Fast and Slow*. London: Macmillan, 2011.
[88] N. Bostrom, *Superintelligence: Paths, Strategies, Dangers*. Oxford: Oxford University Press, 2014.
[89] A. Marot, A. Rozier, M. Dussartre *et al*. (2020, Sept.). Towards an AI assistant for human grid operators. [Online]. Available: https://arXiv: 2012.02026
[90] C. A. Hidalgo, D. Orghiain, J. A. Canals *et al*., *How Humans Judge Machines*. Cambridge: MIT Press, 2021.
[91] A. Schmidt, F. Giannotti, W. Mackay *et al*., "Artificial intelligence for humankind: a panel on how to create truly interactive and human-centered ai for the benefit of individuals and society," in *IFIP Conference on Human-Computer Interaction*, Hoboken: Springer, 2021, pp. 335-339.
[92] A. Marot, B. Donnot, K. Chaouache *et al*. (2021, Aug.). Learning to run a power network with trust. [Online]. Available: https://arXiv: 2110.12908
[93] Z. Akata, D. Balliet, M. de Rijke *et al*., "A research agenda for hybrid intelligence: augmenting human intellect with collaborative, adaptive, responsible, and explainable artificial intelligence," *Computer*, vol. 53, no. 8, pp. 18-28, Jul. 2020.
[94] M. Beaudouin-Lafon and W. E. Mackay, "Rethinking interaction: from instrumental interaction to human-computer partnerships," in *Proceedings of Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems*, Montreal, Canada, May 2018, pp. 1-5.
[95] A. M. Prostejovsky, C. Brosinsky, K. Heussen *et al*., "The future role of human operators in highly automated electric power systems," *Electric Power Systems Research*, vol. 175, p. 105883, Oct. 2019.
[96] R. Monarch, *Human-in-the-loop Machine Learning: Active Learning and Annotation for Human-centered AI*. Greenwich: Manning, 2021.
[97] F. Milano, F. Dörfler, G. Hug *et al*., "Foundations and challenges of low-inertia systems," in *Proceedings of 2018 Power Systems Computation Conference (PSCC)*, Dublin, Ireland, May 2018, pp. 1-25.
[98] B. Schäfer, D. Witthaut, M. Timme *et al*., "Dynamically induced cascading failures in power grids," *Nature Communications*, vol. 9, no. 1, pp. 1-13, May 2018.
[99] U. Markovic, O. Stanojev, E. Vrettos *et al*. (2019, May). Understanding stability of low-inertia systems. [Online]. Available: https://www. researchgate. net/publication/331188399_Understanding_Stability_of_Low-Inertia_Systems
[100] J. McCalley, S. Asgarpoor, L. Bertling *et al*., "Probabilistic security assessment for power system operations," in *Proceedings of IEEE PES General Meeting*, National Harbor, USA, Mar. 2014, pp. 212-220.
[101] D. S. Kirschen and D. Jayaweera, "Comparison of risk-based and deterministic security assessments," *IET Generation, Transmission & Distribution*, vol. 1, no. 4, pp. 527-533, Jul. 2007.
[102] G. Dalal, E. Gilboa, S. Mannor *et al*., "Chance-constrained outage scheduling using a machine learning proxy," *IEEE Transactions on Power Systems*, vol. 34, no. 4, pp. 2528-2540, Feb. 2019.
[103] B. Donnot, I. Guyon, A. Marot *et al*., "Optimization of computational budget for power system risk assessment," in *Proceedings of 2018 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)*, Sarajevo, Bosnia and Herzegovina, Aug. 2018, pp. 1-6.
[104] E. Heylen, M. Ovaere, S. Proost *et al*., "A multi-dimensional analysis of reliability criteria: from deterministic $n-1$ to a probabilistic approach," *Electric Power Systems Research*, vol. 167, pp. 290-300, Feb. 2019.
[105] N. Maruejouls, V. Sermanson, S. Lee *et al*., "A practical probabilistic reliability assessment using contingency simulation," *IEEE PES Power Systems Conference and Exposition*, vol. 3, pp. 1312-1318, Apr. 2004.
[106] D. Kirschen, D. Jayaweera, D. Nedic *et al*., "A probabilistic indicator of system stress," *IEEE Transactions on Power Systems*, vol. 19, no. 3, pp. 1650-1657, Aug. 2004.
[107] M. R. Jamieson, G. Strbac, and K. R. W. Bell, "Quantification and visualisation of extreme wind effects on transmission network outage probability and wind generation output," *IET Smart Grid*, vol. 3, no. 2, pp. 112-122, Jul. 2020.

Antoine Marot is the Lead AI Scientist at Reseau de Transport d'Electricite, Paris, France. His interests include augmentation of simulation, decision-making capability, and human-machine interaction with AI.

Adrian Kelly is a Principal at Electric Power Research Institute, Dublin, Ireland. He studied at University College Dublin, Dublin, Ireland, and previously worked with EirGrid, the TSO in Ireland. His interests include the control center of the future, situational awareness, alarm management, human machine interface (HMI) design, and machine learning in system operations.

Matija Naglic is a Technical Advisor at TenneT TSO, Arnhem, the Netherlands. He was before with Delft University of Technology, Delft, the Netherlands, and Milan Vidmar Electric Power Research Institute, Ljubljana, Slovenia. His interests include modernization of control center systems and tools, edge computing, and wide-area monitoring, protection and control.

Vincent Barbesant is a Project Lead in Research & Development Department at Reseau de Transport d'Electricite, Paris, France, and a Former Operator and Head Operator of a part of the French network. His research interests include power system operation and decision support.

Jochen Cremer is an Assistant Professor at TU Delft, Delft, the Netherlands, and Co-director of the Delft AI Energy Lab, Delft, the Netherlands. He was before with Imperial College, London, UK, and RWTH Aachen University, Aachen, Germany. His research interest is developing novel methods from AI and mathematical optimization and applying these to power system (real-time) reliability management.

Alexandru Stefanov is an Assistant Professor at TU Delft, Delft, the Netherlands, and a Technical Director of Control Room of the Future (CRoF) research and demonstration facility. He holds the professional title of Chartered Engineer from Engineers Ireland. His research interests include cyber security for power grids, resilience of cyber-physical systems, and next generation grid operation.

Jan Viebahn is a Data Scientist at TenneT in the Digital and Process Excellence Department, Arnhem, the Netherlands. His main research interests focus on developing decision support tools based on artificial intelligence.