IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 11 November 2022, accepted 21 November 2022, date of publication 24 November 2022,
date of current version 1 December 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3224425

RESEARCH ARTICLE

Toward Resilience in Mixed Critical Industrial Control Systems: A Multi-Disciplinary View

ROBERT-JERON REIFERT[1], (Graduate Student Member, IEEE), MARTIN KRAWCZYK-BECKER[2], LAURIN PRENZEL[3], SVYATOSLAV PAVLICHKOV[4], MOHAMMAD AL KHATIB[4], SANDESH ATHNI HIREMATH[4], MANAR AL-ASKARY[5], NAIM BAJCINCA[4], SEBASTIAN STEINHORST[3], (Senior Member, IEEE), AND AYDIN SEZGIN[1], (Senior Member, IEEE)

[1]Digital Communication Systems, Ruhr University Bochum, 44801 Bochum, Germany
[2]KROHNE Innovation GmbH, 47058 Duisburg, Germany
[3]Embedded Systems and Internet of Things, Technical University of Munich, 80333 Munich, Germany
[4]Department of Mechanical and Process Engineering, Technical University of Kaiserslautern, 67663 Kaiserslautern, Germany
[5]PHYSEC GmbH, 44803 Bochum, Germany

Corresponding author: Robert-Jeron Reifert (robert-.reifert@rub.de)

This work was supported by the Federal Ministry of Education and Research [Bundesministerium für Bildung und Forschung (BMBF)] of the Federal Republic of Germany (Förderkennzeichenand ReMiX) under Grant 01IS18063A-E.

ABSTRACT Future industrial control systems face the need for being highly adaptive, productive, and efficient, yet providing a high level of safety towards operating staff, environment, and machinery. These demands call for the joint consideration of resilience and mixed criticality to exploit previously untapped redundancy potentials. Hereby, resilience combines detection, decision-making, adaption to, and recovery from unforeseeable or malicious events in an autonomous manner. Enabling the consideration of functionalities with different criticalities, mixed criticality allows prioritizing safety-relevant over uncritical functions. While both concepts on their own feature a huge research branch throughout various disciplines of engineering-related fields, the synergies of both paradigms in a multi-disciplinary context are commonly overlooked. In industrial control, consolidating these mechanisms while preserving functional safety requirements under limited resources is a significant challenge. In this contribution, we provide a multi-disciplinary perspective of the concepts and mechanisms that enable criticality-aware resilience, in particular with respect to system design, communication, control, and security. Thereby, we envision a highly flexible, autonomous, and scalable paradigm for industrial control systems, identify potentials along the different domains, and identify future research directions. Our results indicate that jointly employing mixed criticality and resilience has the potential to increase the overall systems efficiency, reliability, and flexibility, even against unanticipated or malicious events. Thus, for future industrial systems, mixed criticality-aware resilience is a crucial factor towards autonomy and increasing the overall system performance.

INDEX TERMS Autonomy, functional safety, industrial control systems, mixed criticality, resilience.

I. INTRODUCTION

Many industrial sectors are facing an increasing volatility of markets, e.g., through varying demand, reduced lot sizes down to individualized production, disrupted supply chains, or a varying availability of resources. These challenges call for new and ingenious ways to increase the flexibility of production, while still maintaining a high efficiency. At the same time, highly flexible production facilities also pose their own challenges, e.g., with respect to maintaining efficiency and functional safety in all potential configurations with limited resources, specifically in the face of unanticipated events or even cyberattacks. In this contribution, we consider two concepts to tackle these challenges and put a focus on the potential we see in combining both concepts: *resilience* and *mixed criticality*.

The associate editor coordinating the review of this manuscript and approving it for publication was Jjun Cheng.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

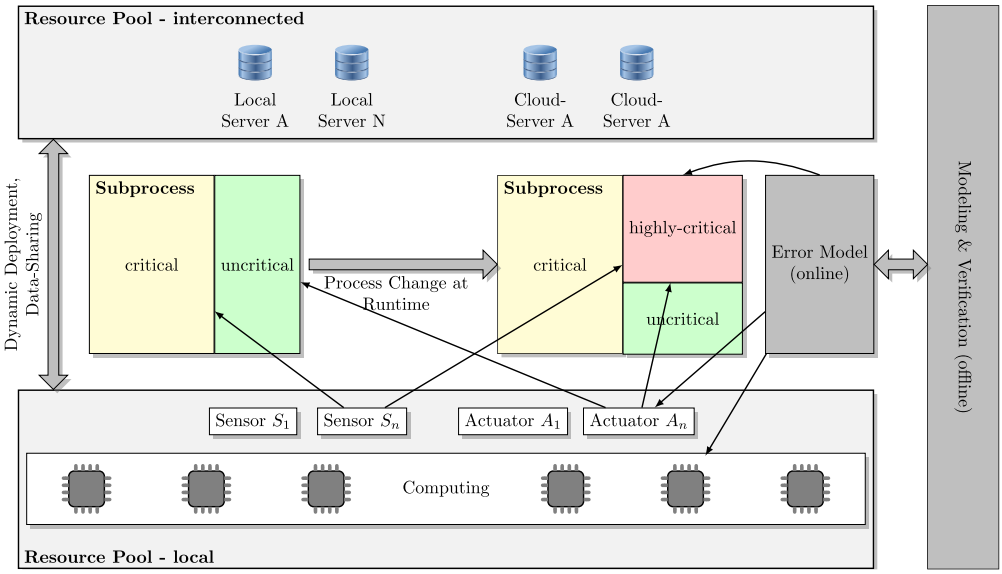


FIGURE 1. Example of an industrial control system or a mechatronic system with local and cloud resources. Resilient behavior as a subprocess undergoes criticality changes at runtime.

While the term resilience originates from the field of psychology, over time, the concept has also been transferred to other domains, including organizational, social, economic, and engineering domains [1]. Also due to this adaptation to such a broad range of fields, multiple definitions of resilience exist in literature, e.g., [1]. To the best of the authors' knowledge, currently, there is no universally accepted cross-area definition. Here we follow the rather broad definition in [2], where resilience is defined as the intrinsic ability of a system to adjust its functionality in the presence of a disturbance and unpredicted changes. The term mixed criticality originates from the domain of scheduling [3], where critical tasks are prioritized over less critical ones, e.g., in terms of computation time. Here, however, we extend the concept to a functional level, where different criticalities are assigned to different tasks or functionalities within a production plant.

An example illustrating the two concepts and their combination is presented in Fig. 1. Hereby, Fig. 1 represents an ICS or a general mechatronic system, e.g., the configuration of a modern vehicle or robot cell. In every plant, there are multiple resources, such as computational nodes, communication channels, instrumentation, physical assets, such as pipes, tanks, etc. In case of disruptions of one or multiple components of the system, resilient behavior can be achieved by ''intelligently'' redistributing the tasks onto the remaining resources to alleviate the effects of the disruptions. As long as there are enough redundant components in the system, the pre-disruption state may be reachable. If the disruption is so severe, however, that the remaining resources do not allow to fully maintain all functionalities, the concept of mixed criticality comes into play. Combining the flexible reorganization with mixed criticality allows to automatically prioritize more critical functions (e.g., safety relevant) over less critical functions (e.g., optimization) to achieve an acceptable behavior of the system even in presence of severe and unanticipated disruptions.

Both concepts, resilience and mixed criticality, are intrinsically multi-facetted, even within the scope of flexible production and process control systems considered here. In this contribution, we provide multiple viewpoints of the concepts, namely system design, communication, control, and security. We are looking for differences, similarities, and potential synergies of both concepts between the different research fields. We highlight the potential and challenges that implementing the concepts in control systems hold and propose ideas to combine resilience and mixed criticality in a meaningful way. Please note that the herein considered concepts are motivated and applied to ICS, however, such considerations are perfectly extendable to various application fields such as the automotive market, industrial robotics, and thus general mechatronic systems.

A. MULTI-DISCIPLINARY PERSPECTIVE

Joining the concepts of resilience and mixed criticality for industrial control systems (ICS) in a meaningful and effective manner requires efforts in a wide-range of research fields. We now proceed to provide a perspective for the system design, communication, control, and security domain, respectively.

1) SYSTEM DESIGN

From the system design perspective, current ICS and their life cycles are unable to meet the requirements of a quickly evolving and uncertain world. From the perspective of the demand, the orders to be filled are affected by the global economy and require an immediate adaptation of the system to

fulfill these demands. The need for safety inevitably requires a higher level of autonomy when it comes to handling faults, failures, or accidents, without causing lengthy down-times or awaiting manual intervention. Additionally, new qualities and quantities of adversaries necessitate enormous efforts in keeping these systems secure. Traditional measures of relying on exceptional system design and a quick manual response are insufficient in dealing with uncertainty. Future ICS must be able to adapt and respond autonomously and flexibly to unforeseen and unforeseeable events. Entailing the aspects of absorption, adaptation, and recovery, *resilience*, i.e., the capacity to recover from perturbations or adverse conditions, captures a missing property in current ICS: While the organizational structures surrounding the plant will eventually recover from a fault or attack, the ICS by itself is incapable of performing this recovery. We envision future ICS that are empowered to detect, diagnose, and respond autonomously to unexpected scenarios, and resilience is a key component of this development. Further, current architectures are comprised of numerous concurrent system functions. These functions are of diverse priorities and as such, can and should be treated accordingly in the event of a fault or an attack. Pooling of resources, e.g., see Fig. 1, can provide the required flexibility to improve the resilience of highly critical system functions at the cost of uncritical functions.

2) COMMUNICATION

Future ICS pose strict requirements to the underlying communication infrastructure, e.g., consider Fig. 1, where numerous sensors, actors, servers, and computation resources communicate with each other. These ICS require the communication systems to provide real-time connectivity and ensure reliable communication in an autonomous manner. In this context, especially the broadband and critical Internet of Things (IoT) connections are expected to grow from 0.8 billion in 2021 to over 2 billion in 2027, approximately [4]. With the advantages of low-costs, high flexibility, easy deployment, as well as self-configuration, wireless communication is an excellent candidate for future industries [5]. Especially in the context of ICS, where mixed critical functions coexist within the network, such criticality levels need to be accounted for. Under heterogeneous quality of service (QoS) demands, a cross-layer perspective to serve the mixed critical network participants is necessary. Moreover, fundamentally, the wireless channel in particular is highly unreliable due to fading, blockage, or outage [6]. Providing a robust communication system is, therefore, vital. As faults are inevitable, it is equally important to provide mechanisms to adapt the communication and recover in a timely manner to an acceptable service level. Thereby, the concept of resilience arises, especially to handle the tremendous real-time mixed critical communication traffic.

3) CONTROL

Along with the system design and communication perspective, future ICS rely on sophisticated control mechanisms. Therefore, from the control perspective, resilience plays an increasing role in nearly all cyber-physical system (CPS) featuring a high functional and infrastructural criticality. Such instances are frequently found in various time and geographic scales of power systems, autonomous driving, robotics, process engineering, civil security, etc. [7], [8]. From the perspective of control theory, a formal definition of resilience and its distinctive features to the established concepts of robustness and fault-tolerance need to be found. Resilient behavior counteracts a higher lever of unforeseen system degradation with respect to system-relevant quality criteria which on its own requests an unambiguous mathematical description. Another aspect that one should stress is how resilience is related to the system autonomy. In fact, by its definition resilience excludes readjusting of the system parameters or/and its architecture by a human operator. Resilient systems are autonomous in pursuing these tasks. Therefore resilient behavior requires and it expresses a certain level of autonomy. Currently two control theoretical paradigms in addressing the system resilience need to be discriminated: the model-based and the data-driven one. A common ground to these techniques where multiple challenges reside in terms of algorithmic efficiency, structure, flexibility and robustness is represented by the need for optimization in continuous and discrete variable spaces. Natural model-based approaches offer adaptive control (AC) and model-predictive control (MPC) techniques. Data-driven and Machine Learning (ML) techniques, (also in light of its close relationship to the autonomous behavior) offer appealing decision making strategies, in particular in complex environments, including reinforcement learning.

4) SECURITY

Given the above considerations, enabling resilience and mixed criticality for ICS in a meaningful manner still requires to account for an IT security perspective. From this point of view, mixed criticality scenarios are gaining more attention. Cloud computing, the IoT, and the prevalence of mobile devices have fundamentally changed the requirements for security mechanisms. Sophisticated malware and extensive cyberattacks have set a new stage for threat assessment. Further, in order to cope with the skyrocketing amount of digitalization, an effective security strategy is a necessity. In this context, incident response and analysis is an essential consideration. In terms of cyber security, resilience refers to an organization's ability to adapt to and counteract damaging cyber incidents, regardless of whether these incidents are deliberate or unintentional, triggered by employees or third parties. The level of resilience is measured in maintaining confidentiality, integrity, and availability of data and services. Security mechanisms are usually strictly aligned with the criticality of the system to protect. For instance, security policies may depend on the state of a process, i.e., the current criticality for the whole system, see Fig. 1. Due to specifications, the whole system can be shifted from an uncritical state to a highly-critical state during runtime. The same may apply to

the results of data analysis branching to different ways of threat response.

B. RELATED WORKS

In what follows, we provide a brief overview of related works on resilience and mixed criticality. As these concepts are even multi-facetted in each discipline, the respective sections provide further details about related works in the fields.

1) DEFINITION & METRICS

Resilience is considered in many different domains, and thus, definitions can vary. Reference [1] provides an extensive overview of definitions and metrics that can be used to assess the resilience of organizational, social, economic, and engineering systems. Further, [9] describes the limitations of existing metrics and provides a new metric, combining the aspects *absorption*, *adaptation*, and *recovery* in one metric.

Resilience is applied to a large array of problems and can be implemented by many means. Resilient architectures can be described by three characteristics: The resilience variables (e.g. function, structure, behavior), the resilience conditions (e.g. disruptions, events, adversaries), and the resilience properties (e.g. recovery, adaptation, graceful degradation) [10].

2) RESILIENT SYSTEM DESIGN

The need for resilience in critical infrastructure and safety-critical systems is well understood and relates to the concept of risk management [11], [12], [13], [14]. In particular, resilience extends the notion of reliability through adaptation to events that may be impossible or difficult to anticipate or quantify. Thus, resilience plays a more important role for dependable systems with critical elements. Compared with traditional systems design, the IoT provides fresh opportunities for resilience through decentralization, diversity, or evolution [15]. By incorporating critical infrastructure into the IoT, the need for resilience is even more clear, as critical and uncritical services must coexist in close proximity [16]. The deeply interconnected networks of the IoT also create new challenges that require more advanced resilience strategies [17].

3) MIXED CRITICALITY SCHEDULING

The presence of critical and less-critical components or tasks inevitably leads to the topic of task scheduling. The initial discussion sprung from a seminal paper [3], which quickly led to a large number of contributions on the general topic of how to schedule tasks in the presence of mixed criticalities [18], [19].

C. CONTRIBUTION

The contributions of this work include the joint consideration of resilience and mixed criticality within a multi-disciplinary point of view. Especially, considering ICS to ensure being highly adaptive, productive, and efficient while preserving functional safety requirements under limited resources is tackled from a system design, communications, control, and security domain. To the best of the authors' knowledge, this is the first work to provide such a perspective with a focus on enabling mixed criticality-aware resilience in ICS. The detailed contributions, respecting individual and joint aspects, are given as follows:

- We investigate existing definitions and metrics of resilience and assess their suitability for ICS.
- We examine and classify key characteristics and technologies that enable mixed criticality-aware resilience in ICS.
- From a system design perspective, we analyze the opportunities and challenges that resilience may provide for ICS, and investigate the potentials of considering the various criticalities or priorities of system functions.
- From the communication perspective, we, with a focus on the lower communication layers, propose a vision of a mixed criticality-aware resilience controller, and evaluate these considerations in a case study.
- From the control perspective, we survey and classify the methods of adaptive control, and analyze them in the context of resilience and mixed criticality.
- We explore the implications of mixed criticiallity on a system's cyber security.
- We identify trends and challenges that promote or inhibit the adoption of resilience and mixed criticality among the domains.

D. ORGANIZATION

The rest of the paper is organized as follows: Section II provides more insights into the resilience and mixed criticality domain for ICS and provides general definitions. Definitions and metrics from the system design perspective are revisited in Section III. Especially, the role of resilience during a system life cycle is emphasized. A perspective of the communication domain is provided in Section IV, a resilience and criticality-aware network controller and detailed definitions are provided. Thereafter, Section V depicts the control perspective, where existing methods of robust and adaptive control are surveyed and their application for resilient ICS is described. Section VI provides a security perspective on resilience and mixed criticality, and conducts a case study on detecting malicious behavior. After introducing the multi-disciplinary framework of resilience and mixed criticality for ICS, Section VII links the proposed framework to related paradigms for enhancing reliability and safety. Future perspectives are discussed in Section VIII, and Section IX concludes the paper.

II. RESILIENCE AND MIXED CRITICALITY IN ICS

Many recent approaches towards increasing flexibility of production and process systems fall into the category of digital transformation in manufacturing, often referred to as the 4th industrial revolution or Industry 4.0 [20]. The approaches tackle the problem in a multitude of ways and on various

levels, i.e., on different hierarchies (from product to enterprise level), at different stages of the life cycle (from development to service), and on different architecture components (from physical things, to their digital representations, to higher level business processes). The solution space has been concisely summarized in the Reference Architectural Model Industry 4.0 (RAMI 4.0) [21].

Take the process industry as an example. ''Traditionally'', plants have mostly been designed as a whole, in a monolithic fashion, optimized for the production of a specific quantity of a specific product. Such plants allow for a plant-wide optimization that can achieve a very high degree of efficiency. However, this high efficiency comes at the price of a limited flexibility regarding the product, the quantities to produce, as well as unforeseen events. An established way to increase the flexibility of the production is to consider a modular plant design. Instead of engineering a complete plant from scratch, the plant is built by combining pre-designed functional modules. On the one hand, the reuse of pre-designed modules promises the reduction of engineering overhead and also build time, effectively reducing the time to market. On the other hand, the use of modules allows a more flexible reaction to changing market conditions, e.g., by numbering up the modules to quickly react to an increased demand or by reorganizing or exchanging modules to enable the production of another product. This makes modularity especially interesting for multi-purpose plants and specialty chemicals. Taking the idea of modular plants a bit further, each module can be realized as a cyber-physical system and the complete plant as a CPS of Systems (CPSoS) that orchestrates the modules, enabling new levels of flexibility through potentially automatic on-demand adaptations.

While promising significant benefits, new levels of flexibility also introduce new challenges. Besides still needing to ensure productivity and profitability, the plant must be safe for personnel, equipment, and the environment at all times, independent of the configuration of the plant.

So far, identification and evaluation of potential risks in a plant are usually based on structured risk analyses such as HAZard and OPerability (HAZOP) studies [22]. Although there are works on modular HAZOPs that reduce the overhead [23], thorough analyses remain costly, take time, and involve multiple stakeholders. Based on the identified risks, appropriate countermeasures can be derived and implemented to make the plant robust to *known* incidents. However, in highly flexible plants, a plethora of possible configurations may occur during runtime. This makes it practically infeasible to perform analyses that cover all eventualities and implement dedicated countermeasures that make the plant robust to all events in all possible future configurations with limited resources. As a result, there is an increased chance that *unanticipated* incidents will occur for which no dedicated countermeasures are in place. Alternative strategies are needed to appropriately handle such unforeseen incidents, especially in flexible plants. A promising approach towards this goal we see in the emergence of *resilient* systems - systems that

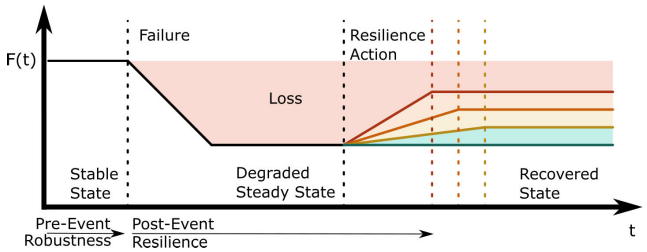


FIGURE 2. Illustration of resilience considering mixed criticality.

are capable of recovering from and/or adapting to these incidents.

In addition to robust design, where the aim is to harden the system to withstand adverse events, the goal of resilient design is to create systems that are inherently capable of adapting to and recovering from adverse events. For instance, a robust design can be achieved by introducing back-up redundancy for critical components, e.g., safety-critical systems, to withstand failures of the respective component. In case all redundant devices fail, or no redundancy has been implemented, a resilient design allows for a meaningful adaptation of the system, such that a complete shutdown is avoided and the functionality is recovered to a certain degree. In this light, flexibility of plants is both, a reason for introducing resilient design, as well as a prerequisite for enabling the desired adaptation during runtime that is characteristic for resilient systems.

This behavior is illustrated in Fig. 2. On a high abstraction layer, the function $F(t)$ could be the productivity of a specific plant. The degradation of $F(t)$ could be due to a failing module. Without any actions, the productivity will drop to a low degraded steady state, which for instance could be a complete stand-still of the plant. Once the event has been detected, a ''resilience action'' can be triggered, which in this case could be a reorchestration of the remaining modules such that the failed module is avoided in automatically created production plans that optimize the productivity $F(t)$ under the new limiting circumstances. This can be interpreted as an optimization problem with increasing resource limitations.

With respect to Fig. 2, work [9] proposes a general resilience metric combining the aspects of *anticipation*, *absorption*, *adaption*, and *recovery*. Before the failure happens in Fig. 2, i.e., in the stable state, *anticipation* corresponds to defending against threads to the normal operation, which can be done actively and passively. *Anticipation* is therefore regarded as a pre-failure aspect. The remaining post-failure resilience aspects are characterized as follows:

- *Absorption* is the ability to maintain the functionality on error occurence, i.e., restraining the failure's severity. In Fig. 2, this is measured in terms of the functionality loss at the degraded steady state.
- *Adaption* is the ability to mitigate failure consequences using the remaining system resources. In Fig. 2, *adaption* is denoted as resilience actions.

- *Recovery* is the ability to reach a recovered state (with reasonable functionality) in a timely manner after experiencing failure degradations. In Fig. 2, this can be found on the right hand side.

Specifically for the latter aspects of resilience, i.e., the adaption and the time to recovery, we see a significant potential in introducing the concept of mixed criticality to resilient design.

In any plant, there are multiple functionalities with varying degrees of criticality. As an illustrative example, ensuring the safety of personnel has a higher criticality than optimizing the inspection intervals through predictive maintenance. In a non-degraded state, the plant has enough resources to fulfill functionalities of all criticalities at the same time. In case of degradations however, this is not necessarily the case. One way to deal with this is to integrate sufficient back-up redundancy, following design principles looking for robustness of the system. This, however, might come at a potentially prohibitive cost. Alternatively, or additionally, following the concept of resilience, we can implement measures that aim at ensuring the proper functioning of the most critical tasks (e.g. safety relevant) on the available resources even during degradations, while less critical tasks (e.g. productivity relevant) can be temporarily reduced or halted.

While on such a high level, the concept of reconfiguring the plant to react to an adverse event is intuitive, concrete realizations require a situation-dependent adaptation of systems with complex, interconnected components. Deriving such solutions require *multi-disciplinary* technological and scientific efforts. In CPSs these include system design, communication, control, and security perspectives.

III. SYSTEM DESIGN PERSPECTIVE

There is currently no universal definition of resilience that applies to all domains and problems. Any definition broad enough to capture every domain will lack the specificity to grasp the issues and challenges of a particular application area.

ICS pose specific requirements on resilience. Since these systems interact with physical processes, safety is of utmost importance. A resilient ICS can implement sophisticated strategies to maximize the production while maintaining the safety of the process. To that end, any consideration of resilience should take a holistic point of view and integrate safety-critical, mission-critical, and non-critical functions of the system to maximize the potential for resilience. Resources of non-critical functions may potentially be used to improve the resilience of safety-critical functions. Nevertheless, improving the resilience of non-critical functions should not diminish the resilience of safety-critical or mission-critical functions.

Resilience plays a role in all phases of the system life cycle. During design time, resilience requires the consideration of redundancies that provide the necessary potential for resilience, in particular with respect to a mixed criticality context, e.g., multiple antennas for communications, see section IV. During run-time, these redundancies can be leveraged to provide resilience against a broad spectrum of faults, failures, and attacks, e.g., adaptive beamforming in section IV, and learning-based adaptive control in section V. The resilience of the system is mainly defined by the behavior in the four phases of *Monitoring*, *Analysis*, *Planning*, and *Execution* of the MAPE cycle [24], [25]. Thus, we analyze the impact of these four phases in particular, and what parameters can influence the system resilience.

A. MONITORING

Detection is the ability to find and diagnose an event. This can apply to failures or faults just the same as to cyberattacks. The ICS must be able to detect an event to be able to react to it. This detection may mean that the exact event is observed (e.g. detection of the execution of malicious code), or by the detection of correlated events (e.g. missing heartbeat may indicate failed hardware). The first type of detection may be implemented by means of additional or smart sensors. The second type of detection can be facilitated through interconnection, data collection, and data analysis, e.g., see Section VI, where a case study validates a detection scheme.

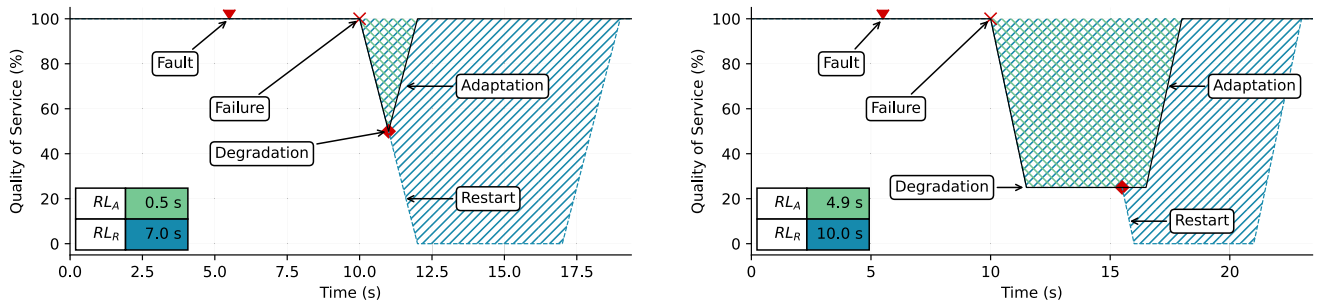
B. ANALYSIS

While monitoring concerns the raw cata collection, this data must be analyzed. Within the MAPE-K model, this can be performed in decentralized design patterns [26]. The analysis is performed over the knowledge K, where the reason to perform a change is detected. At this stage, various methods can be used to extract information from the raw data, such as data mining. Different sources of information can also be combined to form a complete picture, e.g. if suspicious activity in the network is inconclusive, yet other sources indicate an active attack. Similarly, a fault that leads to erroneous behaviors may not be directly visible to a single device. In the greater scheme, however, it may be possible to precisely diagnose the underlying issue.

C. PLANNING

Once an event has been detected, a decision must be formed regarding the response. In the simplest form, resilience strategies are provided beforehand for specific scenarios. This limits strategies to events that are anticipated. In the most advanced form, an advanced decision making algorithm is able to determine the appropriate response to an event autonomously. These decision making algorithms may be centralized or decentralized. A centralized algorithm will suffer from network outages, while a decentralized algorithm puts additional pressure on the network and the individual devices. Depending on the scale of the system, a middle ground may be found in which centrally controlled clusters are able to cooperate in a decentralized manner.

A decentralized architecture was presented in [27], where the planning is limited to computationally powerful devices, whereas all devices participate in a decentralized consensus.



(a) Survival (b) Recovery

FIGURE 3. Depending on the time of detection and response, resilience can manifest in different ways. In a prevention scenario, a fault is fixed before a failure. In survival, a fast adaptation can prevent degradation while it is appearing. In recovery, a degraded system or function can be recovered without requiring a restart.

The consensus allows the optimization and verification of a planned reaction by all participants, without relying on a central authority that could be unavailable or compromised.

D. EXECUTION

Most events will require an adaptation of the system, e.g. through hardware and/or software reconfiguration. Reconfigurable or flexible manufacturing systems may provide some of the needed capabilities. Compared to pure software systems, ICS have additional constraints regarding timing, safety, and the consistency of the process. Any adaptation of the system must be able to guarantee the satisfaction of these constraints, in particular the consistency of the physical process, and the satisfaction of any real-time constraints.

The consistency requirements can be satisfied by careful selection and ordering of the reconfiguration or adaptation sequence. These sequences contain the necessary steps to change a system during its execution. In [28], this consistency in the reconfiguration of distributed control applications based on the IEC 61499 is achieved by choosing an ordering, in which the application is reconfigured in alignment with the flow of events through the system. Thus, ICS can be reconfigured without compromising the consistency of the physical process.

The timeliness of these reconfiguration sequences is analyzed in [29]. If strict hard real-time requirements are expected, an exhaustive schedulability analysis of the reconfiguration is needed. In [29], this is solved by introducing a strict schedulability condition for preemptive, rate monotonic scheduling. Using this condition, the timing impact of the adaptation / reconfiguration can be quantified and an optimal reconfiguration sequence can be found. Depending on the size and complexity, an adaptation can be performed within milliseconds to seconds, while preserving the real-time guarantees necessary to ensure safety.

In Fig. 3, two examples of resilient behavior are displayed: Survival and Recovery. A traditional, non-resilient system requires a restart or other lengthy downtimes to react to a failure. A resilient system, by contrast, is able to respond to the failure by timely detection and reaction. This limits the impact on the system performance. The resilience loss (RL) indicates the lost production time due to the failure. Using dynamic adaptation of the system, the loss can be drastically reduced. In the survival scenario, the reaction can take place before a degraded steady state is reached. In a recovery scenario, the system performance is recovered after a delay, yet this recovery can take place online. If the fault was detected earlier, a degradation could be entirely prevented without any loss. Which of these scenarios may take place depends on the fault / failure and the system. If, for example, not enough resources are available, the reaction may be delayed. In a mixed criticality context, the prevention of a failure of a critical function may require a temporary degradation of a less critical function.

Resilience at run-time requires redundancy at design-time. This does not have to be static redundancy in the form of passive systems that run in parallel and are available at all times. Instead, in large systems, there commonly are hidden redundancies and untapped potentials, e.g., over-provisioned computational resources that can be pooled and used flexibly. Using a mixed criticality prioritization scheme, non-critical functions can be temporarily degraded to provide additional resources for highly critical functions.

IV. RESILIENT WIRELESS COMMUNICATIONS

From the communications perspective, resilience and criticality awareness are highly relevant and timely topics, e.g., in smart factory use cases [4]. As can be seen in Fig. 1, communication is a central building block, uniting different entities within the ICS. Thereby, automated network and resource management from the communications discipline builds one of the pillars towards resilience in mixed critical ICS.

A. RELATED WORKS

A great amount of work towards (network) resilience in communication systems has beed conducted by the ResiliNets initiative [30]. Axioms, strategies, and principles of resilience for communication networks have been reviewed and

proposed in [31]. With a focus on the Internet, the authors gave detailed insights into the general framework providing a basis for future research in various directions. Disaster-resilient communication networks were extensively studied in the book [32], where fundamentals of communication networks' resilience are provided including many works of various researchers around the globe. A plethora of works discuss, propose, and analyze criticality-aware systems in communications [33], [34], [35]. For example, [33] proposes a priority-aware wireless fieldbus protocol and studies the scheme using a plastic extrusion process monitoring scenario. The works [34], [35] in particular propose the AirTight wireless communication protocol under mixed criticality systems, which also provides resilience. The authors present the motivation, design, analysis, and implementation of the protocol for time-critical CPSs including real-time and mixed criticality requirements. Results imply the feasible performance of AirTight w.r.t. packet deadlines and fault experience [34], and w.r.t. schedulability [35]. The authors base the protocol upon the physical (PHY) layer and medium access control (MAC) layer of IEEE 802.15.4. While some lower layer considerations are there, these works mostly conduct system analysis on higher communication levels. In this context, we identify a need to jointly consider mixed criticality and resilience metrics for exploring the capabilities of lower communication layers.

B. THE MAPE SCHEME IN COMMUNICATIONS

To provide resilient communications, a resilience controller (RC) implementing the four MAPE phases, i.e., see also section III, across all ISO/OSI communication layers becomes essential. Especially, we herein consider the lower layers, i.e., transport, network, data link (DL), and PHY layer. An interplay of these layers and the proposed RC can be observed in Fig. 4. In *regular operation*, the RC alternates between monitoring and analysis. Upon detecting a failure condition, the state switches to *remediation*, and the planning of possible ways to adopt to the erroneous condition starts. Through smart and autonomous decisions, the execution of an remediation mechanism is started. By continuously monitoring and analyzing the network performance, eventually, the network and RC are able to recover the functionality and return to *regular operation*.

Monitoring: To be able to monitor the network performance during run-time, either special sensors in the network processing chain (physical assets), or special digital blocks (software), e.g., software defined networking (SDN) [36], are necessary. Parameters to monitor on the PHY layer may be received signal power or throughput, on the DL layer cyclic redundancy check (CRC) results, on the network layer packet error rates (PER) or delay, and on the transport layer acknowledgements.

Analysis: This phase is responsible for interpreting the monitored parameters. An erroneous condition may be detected by the signal power or throughput falling below a given threshold, and CRC errors, the PER, or the number of not acknowledged segments rising above certain predefined numbers. In this context, mixed criticality comes into play by defining different constraints and thresholds on tolerated faults for the diverse network participants, e.g., see [34]. Further techniques include one-class classifiers, which can detect anomalies in communication systems [37], and machine learning, e.g., for intrusion detection [38].

Planning: To choose appropriate mechanisms to remediate the effects of a detected failure, the RC needs to be aware of the exact location (layer) of the failure. For example, a DL layer failure may not be remediated at the PHY layer, however, a PHY or DL layer failure can be remediated by re-routing traffic on the network layer [31]. Similarly, the DL layer is able to utilize a fallback PHY layer, and the PHY layer may, for example, utilize a frequency fallback mechanism [39], or diversity techniques, i.e., time/frequency/spatial-diversity through retransmissions, sub-carrier coding, and multiple antennas [6]. This phase is eligible to respect different criticalities by prioritizing the resource allocation towards safety-(or mission)-critical network participants.

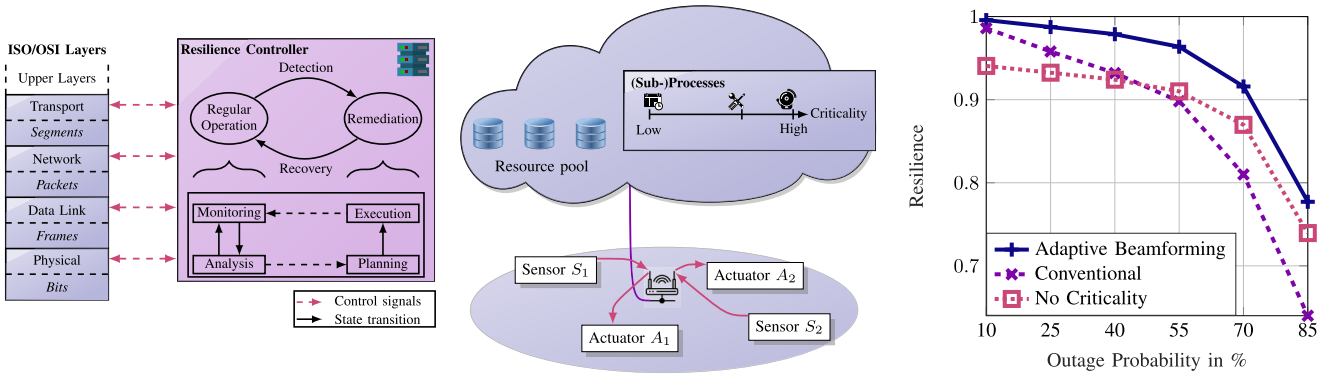
Execution In this phase, the previously made plans are executed at the respective layer via control signals by the RC. Hence, closely monitoring and analyzing the effects of the mechanism is important, to on the one hand prevent resource waste and be able to promptly recover to *regular operation*, and on the other hand control the mixed criticality prioritization.

C. RESILIENCE AND MIXED CRITICALITY IN COMMUNICATIONS

From a lower-layer communications perspective, Fig. 2 shows the functionality $F(t)$, which can be translated as PER, delay, etc., on the network layer [40], and data rate, signal-to-noise ratio, etc., on the PHY layer. Especially the achievable data rate is of fundamental importance to most upper layer metrics, which are build upon (and rely on) the underlying PHY layer. As such, herein, the monitoring and analysis phase focus on measuring the data rate (throughput).

The related works on mixed criticality for communication systems considered the PHY layer solely for data transmission without mixed criticality properties. However, an essential building block to criticality-aware resilience in communications is a cross-layer perspective on criticality levels. Mixed criticality can be incorporated into wireless communication resource management as: (a) Weights to optimization metrics, e.g., weighted sum rate [41]; (b) QoS constraints, which might differ for network participants [42]; (c) An optimization metric for respecting mixed criticality based upon the QoS requirements of network participants [43].

With these considerations at hand, the recent work [44] proposes a criticality-aware QoS-based resilience metric, utilizing the aspects from [9] taylored to the PHY-layer resource management. Linking to section II, the metric consists of *absorption*, *adaption*, and *recovery* or rather



(a) Cross-layer resilience controller including the MAPE phases, namely monitoring, analysis, planning, and execution.

(b) Communication system model with cloud resources and a multi-antenna access point.

(c) Resilience metric over channel outages for the *adaptive beamforming*, *conventional*, and *no criticality* schemes.

FIGURE 4. Communications perspective including a network resilience controller, an exemplary system model, and results.

time-to-recovery. In an optimal case, the metric yields 1, i.e., a failure does not impact the network, also known as survivability.

While such metric quantifies the resilience of a system and helps measuring and evaluating different resilience techniques, the network has to implement resilience as planning and execution phases. Examples for resilient design in the context of wireless communications are manifold, and extend over the considered communication layers. Due to the unreliability of the wireless channel, various techniques promise to ensure connectivity of the receiver on outage events. To only name a few mechanisms: The transport layer provides different loss recovery mechanisms, which utilize a form of retransmission. Re-routing or redundant routing are techniques for the network layer. On the DL layer, a different access strategy or multi-association of access points and receivers is possible. At last, the PHY layer can operate on signal-to-noise ratio margins and adapt the modulation, the coding scheme, or the beamforming. In the context of the MAPE phases, the RC is aware of such methods and allocates them accordingly upon facing erroneous-events.

D. CASE STUDY: MIXED CRITICAL MSE MINIMIZATION

Analogously to [43], consider an arbitrary communication system consisting of a multi-antenna transmitter and K receivers, as depicted in Fig. 4b. The heterogeneous receivers represent mixed critical network participants with different requirements regarding QoS. Under a similar optimization metric as [43], the network initially reaches an optimized stable state. Through optimization, robustness is a pre-event characteristic of the system, as the resources are allocated to best achieve the given objective. Thereby, optimization is a key technology for achieving reasonable *absorption*. Due to the multi-antenna nature of the transmitter, beamforming by linear precoding is able to spatially separate the signals in order to achieve less interference [45] and higher rates. Such technique contributes towards *absorption*, and especially enables opportunities for *adaption*. While modeling channel outages, hardware impairments, or receiver mobility is out of this work's scope, we note that each of these scenarios impacts the wireless channel and thereby the network performance under (optimal) resource allocation suffers performance loss. After detecting such loss, *adaptive beamforming* using updated precoding coefficients becomes a key enabler of achieving timely (*recovery*) and good-quality (*adaption*) resilience within the mixed critical network.

Simulation results for a network consisting of an 8 antenna transmitter and 5 receivers, with two high critical and three low critical nodes, over the channel outage probability can be seen in Fig. 4c. We show the resilience of the proposed adaptive beamforming scheme and two reference schemes, namely *conventional*, i.e., a communication system that does not include any adaption and recovery mechanisms, and *no criticality*, i.e., a system disregarding the QoS demands, which essentially boils down to a sum-rate maximization problem, e.g., see [41]. It can be observed that the total resilience, quantified in [44], suffers minor decline in the face of high outage probability, thanks to well-suited robustness and adaption mechanisms. Putting things into perspective, *adaptive beamforming* outperforms *conventional* in every point, where the loss of the non-resilient scheme increases with outage probability. Similarly, the proposed scheme outperforms *no criticality*, which, despite including the same adaption mechanisms, can not achieve the same resilience. Overall, especially at higher outage probabilities, the need for sophisticated adaption mechanisms is emphasized. Additionally, the need for considering the mixed criticality aspect is highlighted, as this paradigm is shown to enhance the network's resilience.

In synergy with the system design, the change of production plans at run time was proposed in [27]. In that work, centrally controlled clusters of ICS components cooperate in a decentralized manner and verify production plans utilizing a distributed consensus. Thereby, communication protocols that operate distributively, e.g., [46], [47], are vital for

enabling such processes. Taking this as an example, we note that mixed criticality-aware resilience in ICS requires considerations from both the system design as well as the communication domain.

V. RESILIENT CONTROL SYSTEMS

Introducing a third perspective, control systems are of equal relevance towards enabling resilience and mixed criticality in ICS. Speaking generally, resilient control systems are systems, whose performance is not severely degraded in presence of attacks and corresponding variations of their structure, design, and control parameters. As defined in [7], "A resilient system is one that maintains state awareness and an accepted level of operational normalcy in response to disturbances, including threats of an unexpected and malicious nature". Accordingly, we expect that a resilient controller should ensure that the performance of a closed-loop system affected by a malicious attack must follow the Disturbance and Impact Resilience Curve depicted above in Fig. 2, or speaking more generally, it should track the Disturbance and Impact Resilience Manifold (see Fig. 5 from [8]).

Therefore, intuitively, one may expect that, if one tries to apply some adaptive control algorithm to a control system which is damaged by some malicious attack, and, therefore, its parameters are instantly and unpredictably changed due to this attack, then (to some extent) its performance can follow Fig. 2's behavior. Hence, it is natural to try to upgrade the existing classical adaptive control algorithms and to make them applicable to resilient control systems.

A. MODEL-BASED ADAPTIVE CONTROL

In order to give some introductory survey of various problems of adaptive control and stabilization, we begin with a control system in the following form

$$\dot{x} = F(\theta, x, u), \tag{1}$$

with states $x \in \mathbb{R}^n$, controls $u \in \mathbb{R}^m$, and with unknown parameter $\theta \in \mathbb{R}^p$. We assume that the origin is the equilibrium point and that *(known)* function F is smooth enough, and, therefore, (1) satisfies some standard conditions of the existence and uniqueness of its trajectories. The simplest version of a typical adaptive control problem for system (1) with *unknown* parameter θ is to find a feedback, which stabilizes system (1) at the equilibrium and/or provides the following property: $x(t)$ tends to the equilibrium as $t \to +\infty$. Thus, such a design incorporates both extension of the state space by adding a new "dynamical variable" $\hat{\theta} \in \mathbb{R}^p$ (sometimes called "parameter estimate") and appropriate design of its dynamics to achieve our control goal. This is equivalent to extending control system (1) with $\dot{\hat{\theta}} = H$, states $[\hat{\theta}, x]$, and controls $[H, u]$. Then, designing its suitable feedback $H = H(x, \hat{\theta})$, $u = u(x, \hat{\theta})$ such that the corresponding closed-loop system satisfies the desired property, i.e., that $x(t)$ approaches (1)'s equilibrium point for $t \to +\infty$.

In *model-based adaptive control* problems, it is assumed that some information about the structure of system (1) is available. For example, it is often assumed that system (1) has the following form

$$\dot{x} = f(x) + g(x)u + \Phi(x)\theta, \tag{2}$$

where functions f, g, and Φ are known, but vector θ is unknown. For instance, in engineering applications, θ can be the vector of dynamic parameters, e.g., those obtained from the inertia matrix of the vehicles considered in [48]. If the vehicle considered in [48] is accidentally damaged, then θ instantly changes, and then the corresponding adaptive control algorithm applied to the system is actually doing either the same or a similar job as that depicted in Fig. 2. A similar problem is resolved by the adaptive recursive design for the control of two-stage chemical reactors [49] as well as for power networks [50]. Hence, the problem formulation of model-based adaptive control is meaningful for resilient control. In general, if system (2) has the lower-triangular form, or strict-feedback form, then backstepping designs originating from [51] and [52] are very fruitful not only for the case of ordinary differential equations [53], but also for other classes such as stochastic systems [54], etc.

B. NETWORK CONTROL

A parallel and related line of research deals with the problem of control and stabilization in presence of dynamic uncertainties. Let system (1) be affected by the state of another uncertain system, which can be described as the following interconnection

$$\begin{aligned} \dot{\xi} &= \Phi(\xi, x), \\ \dot{x} &= F(\theta, \xi, x, u), \end{aligned} \tag{3}$$

where x, θ, u play the same role as in (1), but the new additional component of the state vector $\xi \in \mathbb{R}^k$, is *unknown*, i.e., it is not available for any measurement, and function Φ is also unknown. The only information about the ξ-subsystem $\dot{\xi} = \Phi(\xi, x)$ of system (3) is that this subsystem $\dot{\xi} = \Phi(\xi, x)$ is input-to-state stable (ISS) with ξ treated as the state and x treated as the input, and the corresponding gain is known. Raising the same problems for (3) as those discussed above for system (1), ISS theory and small gain theorems emerge as promising tools. The first basic step was done in [55] for the case when there are no unknown constant parameters θ in (3), i.e., system (1) is affected only by external dynamic uncertainty ξ; then this approach was extended to the case when system (3) has also unknown constants (parameters) θ, e.g., see [56]. This research line led to solution of various problems of decentralized and distributed control for large-scale networks and multi-agent systems [57], [58]. The use of the ISS approach in the context of resilient control is the same as in the previous subsection V-A, because this is the same problem for the same classes of systems as those from the previous subsection V-A, but under the assumption that they are also affected by dynamic uncertainties described by the ξ-subsystem of (3). The latter allows one to consider

the same problems of adaptive control for interconnected systems, for instance, for networks of systems of the form (2), e.g., see [59] and [50].

C. MODEL-PREDICTIVE CONTROL

The main idea of *model-predictive control (MPC)* is that many real world nonlinear processes can be regarded as either approximately linear or even exactly linear over a small operating/prediction horizon. Then, assuming first that there is no unknown parameter θ in (1), the MPC method proposes to replace the design of a control Lyapunov pair, i.e., control Lyapunov function $V(x) \geq 0$ and the corresponding stabilizing feedback $u = u(x)$, with a recursive solution of a certain optimal control problem minimizing some suitable cost function

$$J = \int_{t}^{t+T} l(x(\tau|t), u(\tau|t))d\tau, \tag{4}$$

where $l(x, u)$ is a positive definite function with respect to x, u, t is the initial instant, and $T > 0$ is the prediction horizon within which the model is simplified (i.e., is ''predictable''), for instance where it is locally exactly or approximately linearizable. Having resolved the MPC problem for each initial instant t, one defines the solution as $u(t) = u^*(\tau|t)$, $\tau = t$, where $u^*(\cdot|t)$ is the corresponding control minimizing (4), see, for instance, [60].

Accordingly, the *adaptive MPC* approach consists of the following steps: First, design of an adaptive estimator in a way, which is similar to the design of an adaptive estimator for system (2), then, design of an MPC controller for the estimated system, and finally, proving that the constructed adaptive and model predictive controller resolves our original problem of stabilization, or regulation. This program is efficiently demonstrated, for instance, in [60] for system (2), when the vector functions f, g, Φ are not necessarily in lower-triangular form. Actually, they can be in any form, but it is assumed that the pair $f(\cdot)$, $g(\cdot)$ is *locally* feedback linearizable, i.e., the dynamics of the system

$$\dot{x} = f(x) + g(x)u \tag{5}$$

can be *locally* brought by a *local* diffeomorphism $z = \Phi(x)$, $v = \Psi(x, u)$ of states and controls to a linear system in the Brunovsky canonical form in a *small neighborhood* of every operating point (x, u). Then one applies the above-mentioned MPC approach and it works efficiently as it is shown in [60]. Adaptive MPC is indeed implemented in real-time systems using the GRAMPC (GRadient-based Augmented Lagrangian MPC) library [61], often used also in Learning-based Control Systems [62] as well.

D. LEARNING-BASED ADAPTIVE CONTROL

Past decades have seen a rapid and widespread success of machine learning (ML) techniques, especially (deep) neural networks (NN/DNN), primarily due to their generalization power as function approximators ([63], [64]). Similarly, the success of DNN based reinforcement learning (RL) technique allowing effective generalization to continuous Markov decision process (MDP) has reignited interest for using it for control applications. In particular, the Deep-Q-Network (DQN) method proposed by [65] which uses DNN for vision based perception in combination with RL technique to learn to determine an optimal control policy for vision based computer games. This technique has been successfully applied in different industrial applications, e.g. [66], [67]. The main advantage of deep learning based RL technqiue is its ability for online adapation which enables learning about unseen events from newly obtained data. Moreover, since the method provides a (computational) function for the control value it promises to be computationally faster than traditional optimization based methods thus making it suitable for realtime and time-critical systems.

If, instead of (2), one deals with a control system

$$\dot{x} = f(x) + g(x)u + \Psi(x), \tag{6}$$

in lower-triangular form, but with *fully unknown* triangular, smooth vector function Ψ, then *learning-based adaptive control* methods are commonly used. Let us recall that the structure of Ψ was known in the above-mentioned special case (2), more specifically, we had $\Psi(x) = \Phi(x)\theta$ with *known* triangular matrix function $\Phi(\cdot)$ and *unknown* constant vector θ. The main idea stems from the classical Stone–Weierstrass theorem about approximations of any continuous function on a compact set. Roughly speaking, learning-based adaptive control designs are based on the idea of replacing the *fully unknown* $\Psi(x)$ with its approximation by some linear combination of *known* and smooth enough functions such that the coefficients of this linear combination are *unknown*. Such an approach reduces this kind of adaptive control problem to the previous case of model-based adaptive backstepping designs (then, the remainder of the approximation can be treated as a kind of ''disturbance''). Known functions of this linear combinations are often called ''NN approximation nodes'', and they are not polynomials as in the Weierstrass approximation theorem, but, for example, they are Gaussian functions in many cases [68]. This problem was tackled in many papers, as examples we mention [50], [69]. Alternatively, in [70], authors have incorporated learning concepts for the design of an adaptive control architecture. In there, the tasks of different sub-systems such as planning, system identification, and control are accomplished via NNs which are then stacked together to result in a single adaptive controller. On this way, one comes to various learning-based algorithms and fuzzy control [71], [72]. Again, in engineering applications like the robotic system [73], the reinforcement learning adaptive control algorithm proposed in [73] is actually doing a similar job like that from Fig. 2, indicating that learning-based adaptive control algorithms are useful in the context of resilient control as well. Finally, with the increased use of learning based concepts in the controller, the safety of their closed loop behavior is also an important factor. The recent work [74] provides an excellent review on different

strategies for ensuring safety. The techniques of uncertainty learning, risk-averse/uncertainty-aware RL, and safety certification, are useful also in the context of resilient control.

E. DATA-DRIVEN CONTROL

Modern systems are becoming more complex and parameter identification more costly. Simultaneously, data is becoming more readily available. Accordingly, scientists are starting to bypass the above-mentioned classical model-based techniques in favor of data-driven methods. Data-driven control relies on the measured data in order to model and design controllers for real-world processes. Within the behavioral approach of Willem [75] the system's model is defined as a set of trajectories. Then the Fundamental Lemma [75] states that every input/output trajectory of a deterministic linear time-invariant (LTI) system can be parameterized by a single persistently exciting measured input/output trajectory. Therefore controllers based on the trajectory-based representation of LTI models are designed, such as the data-driven predictive controllers in [76], where the authors compute online optimal controls for unknown systems using real-time output feedback via a receding horizon implementation, allowing for the incorporation of input/output constraints to ensure safety. Linear quadratic regulators, state-feedback controllers, as well as robust controllers based on input/output data of a black-box linear system are designed in [77]. Data-driven controllers are adaptive as well in the sense that the model's trajectories, which enters into the constraints when designing the controller, are updated online to capture the real-time behavior of the process. Such a property gives a key advantage towards a resilient design of data-driven control systems where controllers are able to adapt to disturbances and faults that alter a system's behavior as shown in the next section.

F. MIXED CRITICALITY AND RESILIENCE

Modern CPS are often interconnections of coupled subsystems of mixed criticality when sharing a set of resources and vulnerable to cyberattacks. Then researchers from different disciplines must guarantee, for instance, that the systems are stable, schedulable, and resilient. In addition, in a mixed criticality setup, higher priority tasks (as in [78]) needs to gain access to shared resources more often so that they could be stabilized or could recover from an attack faster than the other, lower priority tasks. Design and verification of resilient controllers to attenuate adverse effects of a cyber-attack targeting the sensor, controller, and actuator communication channels in a network-control system is addressed in [79]. Furthermore, the authors in [80] co-designed resilient MPC controllers and a scheduler for a collection of decoupled mixed critical linear systems sharing some computational/communication resources. In a mixed criticality setup, adaptive data-driven controllers monitor the trajectories for every control process and provides access to shared resources to each process based on the respective deviation from the desired behavior or predefined priorities.

VI. SECURITY PERSPECTIVE

Joining disciplines for enabling resilience and mixed criticality in ICS can not go without accounting for security aspects. Without such perspective, ICS components, as for example a generated production plan, an end-to-end communication link, or a resilient controller, may suffer from malicious attacks, be sabotaged, and the whole ICS could not be trusted anymore. Thorough but yet efficient cybersecurity mechanisms are challenging to implement. Measuring the degree of resilience is even more difficult. Without adequate means of measuring resilience, confidence in a system's integrity is limited and also impedes its hardening.

A. STATE OF THE ART

Several works propose mechanism to improve resilience and maintain functionality. The U.S. National Institute of Standards and Technology (NIST) has published a comprehensive catalog of potential techniques for enhancing the resilience of systems [81]. Some of these techniques are already contributing to the resilience of commercial products. For example, micro-segmentation is a widely used approach that improves resilience by slowing down cyber attackers as they attempt to navigate through the system. Cyber deception is an active topic of academic research [82]. RHIMES is a research program funded by the Office of Naval Research (ONR) that deploys a range of detection and recovery techniques to secure CPSs from cyberattacks [83]. A NATO research group has proposed a reference architecture for an Autonomous Intelligent Cyber Defense (AICA) agent that resides on a system, continuously assesses attacker activity on the system, and autonomously plans and executes mitigation and recovery actions [84], [85]. All these systems show the importance of carefully assessing the criticality of security related processes.

For the sake of clarification, *cyber resilience* means a system's ability to be robust and to recover from or adapt to a cyber compromise [86]. Common ways to measure cyber resilience focus on systems' abilities to withstand well-defined and predictable threats reflecting the traditional risk assessment and management process for compromise prevention [87]. Resisting threats, however, is a different component. If an event impacts the system's state, a high resilience means the system's ability to recover and adapt after a compromise. As a result, cyber resilience constitutes a preparation for known and unknown threats and establishes the process after an adverse event [88].

In addition to cyber resilience, prioritizing the criticality of processes is equally important. This allows system processes to be defined as mixed critical systems, where applications of varying importance and criticality are implemented on a common computing platform.

From the perspective of critical infrastructure cybersecurity, there is no mixed criticality within one single system, but between different systems in the same architecture. Either the entire system is secured and trusted, or it is unsecured and untrusted — there is no partial security. At the same time,

the ability to restore a system's functionality after a cyber compromise is extremely important. Specifically, cyberattacks on critical infrastructure such as water supplies, smart grids, communications networks, and healthcare facilities are extremely hazardous [89]. Such attacks can cause massive damage to the economic well-being of an organization and society in general and even endanger human lives. Ironically, impressive examples of cyber resilience come from malware operations. For example, the infamous TrickBot - a botnet that carries out ransomware attacks - demonstrated agile and effective recovery after competent malware mitigation organizations attempted to dismantle the botnet [90].

When a cyber incident occurs, the functionality of the system deteriorates as it can be seen in Fig. 2. As a result, various mechanisms and processes start to combat the adverse effects and restore functionality. In this process, cybersecurity focuses on hardening the system to prevent such degradation. In contrast, cyber resilience focuses on partially or fully restoring functionality. This can also increase resilience to future adverse events. Cyber resilience, just like cybersecurity, depends on aspects of the system, such as design, control, preparation, anticipation, training, etc., that occur before the damaging event. The cornerstone of successful cyber resilience begins with recognizing the inevitability of adverse events: When the system is impacted, functionality is impacted, and the focus is on recovery speed.

Specialized organizations such as security operation centers, managed security service providers, and incident response providers are needed to restore functionality when a cyber incident occurs. They determine the nature of the compromise, isolate and contain it, turn on redundant computing resources, clean affected devices, reinstall software, and restore data from backups. All of these steps require significant and extensive human expertise. In addition, these processes take valuable time, often hours or even weeks. For some applications, which require faster responses, this is unacceptable, e.g., autonomous cars or en-route airplanes, whose control can be taken over by criminals [91]. In such cases, there is not enough time to wait for a human emergency response team. Instead, such systems require an intelligent, autonomous agent with minimal response time, in the order of seconds, onboard to take the necessary response and recovery actions [84], [85]. Similar approaches are discussed in sections III, IV, and V.

B. RESILIENCE AND MIXED CRITICALITY

From a security point of view, CPSs require well designed solutions to protect against physical impacts of system malfunctioning. For instance, cyberattacks on chemical plants may not only compromise the targeted system but also have disastrous implications on the environment [92]. The slightest liquid disparities for chemical processes or water ramp metering may have enormous effects. Reliable solutions are required to detect misbehavior or manipulation. To this end, a sensor based monitoring system may use signal analyses techniques to detect suspicious events. To put this into

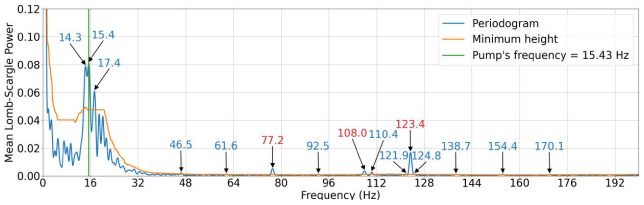


FIGURE 5. Periodogram with peak detection. Blue labels: Normal peaks. Red labels: Peaks at least six times higher than the rolling median.

perspective, i.e., apart from the system design, communication, and control side, the data can provide very strong security guarantees. While attackers can always go for the least resistance, defenders, on the other hand, must pursuit a holistic approach when hardening systems. To this end, security solutions that build on hard-to-manipulate physical properties are preferable [93].

One possible solution is based on properties of the physical surrounding. The underlying assumption considers the uniqueness of the environment reflected using wireless communications, which is discussed in more detail in section IV. During communication, signal transmissions are affected by, e.g., reflection, diffraction, absorption, scattering, refraction, etc. All these effects provide sufficient information to generate a digital fingerprint of the physical environment. Even the slightest change would also alter the digital fingerprint. As a result, this constitutes a holistic approach to harden devices against physical attacks. The underlying technique of assessing changes in a device's surrounding, however, can be assigned to various other use cases. We present one selected application of detecting the frequency of a fluid pump.

C. CASE STUDY: FREQUENCY OF A FLUID PUMP

Closely monitoring the behavior of CPSs is part of protective measurements to predict failures or detect manipulations. We implement sensors to assess the frequency of a fluid pump via electromagnetic signals. Since our sensors sample the signals in non-equidistant time-frames, we make use of the Lomb-Scargle periodogram. The periodogram is an estimator for the power spectral density of a signal. In a periodogram, the distribution of the power of the signal on the angular frequency is represented [94]. This periodogram can be evaluated at any frequency and choosing a frequency grid with a 0.1 Hz spacing will allow for a precise calculation of the interesting frequencies.

The observable frequencies are depicted in Fig. 5. Additional to the frequency of the pump (green line), we see further peaks (blue and red) up to the 8th harmonic. The analysis of harmonic frequencies makes it possible to detect the behavior of different pumps at higher frequencies. For example, when operating a pump, different states such as switch on, switch off, or personell-on-site can be distinguished. This processing can be run continuously to be able to detect deviations from the normal frequency range yielding indications for further investigations. When operating several pumps at

the same time, a basic differentiation of different pumps is prone to high noise impairing a clear identification. Moreover, these analysis results can be cross-checked against other sensor readings or values set in the pump control.

To bring all above considerations into perspective, joining all considered domains brings along synergies among them, and has promising potential towards enabling criticality-aware resilience in ICS. For example, by detecting malicious behavior, as per section VI, a new production plan, as per section III, is optimized utilizing distributed communication schemes, as per section IV, and controlled in a distributed manner, as per section V.

VII. RISK ASSESSMENT AND MAINTENANCE: RELATED PARADIGMS

In what follows, we consider related approaches in general ICSs to enhance reliability and safety. More specifically, we consider predictive maintenance (PM), prognostics and health management (PHM), Failure Modes and Effect Analysis (FMEA), and HAZOP. While a broad review of such paradigms falls out of this work's scope, we briefly introduce them, link the proposed combination of mixed criticality and resilience to such paradigms, and point out the strengths of our proposed generalized framework.

To deviate from traditional maintenance approaches, such as reactive maintenance and scheduled maintenance, more advanced paradigms have been proposed [95]. Reactive maintenance comes into play after an incident or failure, resulting in costly machinery downtimes and parts replacements. In contrast, scheduled maintenance may cause unnecessary downtimes and personell deployment. Hence, PM has been proposed as a promising strategy to overcome such downsides [95], [96]. Under PM, sensors monitor machine states constantly, putting heavy burdens on the corresponding data processing and analysis. We note that PM can be integrated into the proposed generalized framework as a specific implementation of the MAPE cycle. That is, sensors monitor machinery data, algorithms analyze the performance, and in case of anomalies, a maintenance action can be planned to achieve the best effect in downtime and cost-efficiency. A detailed survey of PM can be found in [96].

In the same vein, work [95] surveys prognostics and health management of industrial assets, i.e., PHM. In particular, PHM techniques aim at detecting and classifying a fault, as well as predicting the remaining machine uptime under the error, i.e., anomaly detection, diagnostic, and prognostic. Extending such PHM paradigm, note that the proposed mixed criticality and resilience framework adds an emphasize on overcoming the system failures and getting the performance back to acceptable levels.

In [97], a comprehensive overview of FMEA is provided. FMEA is a technique to identify potential failures and outcomes of such. That is, under FMEA individual system components are analyzed for their potential breakdown causes, including also the corresponding failure effects, and thus the severity of failure impact. While effects are ordered using ranges, e.g., local or system-wide, FMEA characterizes a component's probability of failure, the detectability, the severity, etc. With FMEA being an advanced paradigm for risk assessment and reliability enhancement, our proposed framework rather focuses on enhancing the system resilience aspect. That is, FMEA does not include the mixed criticality, adaption to, and recovery from failures aspects. Also, herein the system autonomy is a special focus of our framework.

Another widely used approach, in particular in chemical and process industries is the hazard and operability (HAZOP, [98]) method, which aims at identifying and evaluating possible hazards. More precisely, it involves steps such as prognosis (systematic search for possible deviations and faults), finding the causes (determining the causes within the examined system), estimating the effects (determining the logical consequences of the deviation), countermeasures (evaluating existing measures and decision on appropriate further countermeasures). The final step introduces the specifications regarding mixed criticality and system resilience. Whilst it traditionally possesses a human-oriented nature, i.e., its results depend on the team composition and the experience of the participant experts, recent research has dealt with utilizing ontologies for knowledge representation and implementation in order to automate the generation of HAZOP worksheets [99]. Thereby, inference algorithms based on semantic reasoners for automated risk assessment and reliable safeguards estimation are applied. In this manner, with consideration given to topology, aspects like the propagation of sub-scenarios through the plant subsystems and components can be systematically investigated. The coming years are expected to stream the research in this context towards the AI-methods (e.g., Knowledge Graphs). In this context, combining the ideas of the recent HAZOP-related literature and the proposed resilience and mixed criticality framework becomes a promising research direction for future ICS.

The above discussion shows how the proposed mixed critical-aware resilience considerations link to advanced state-of-the-art paradigms as PM, PHM, FMEA, and HAZOP. While all these schemes, i.e., PM, PHM, FMEA, HAZOP, and mixed criticality and resilience contribute towards efficient, autonomous, and flexible ICS, the generality of the proposed mixed criticality and resilience framework underlines its broad applications to future ICS and its suitability to determine and perform countermeasures at runtime.

VIII. CHALLENGES AND FUTURE WORK

With the previous considerations at hand, a multi-disciplinary view on the joint benefits of resilience and mixed criticality for ICS is obtained. Initial ideas, concepts, and methods are discussed and case studies show initial proof-of-concepts. However, research in this domain is at an early stage at this point. Many open questions, challenges, and opportunities remain and we next provide aspects for future work from

the perspective of system design, communications, control systems, and security, respectively.

A. SYSTEM DESIGN

Detection of events is an interesting topic from multiple viewpoints. On the one hand, digital twins provide a suitable comparison to identify deviations from the expected behavior. On the other hand, a digital twin is only as good as the underlying model. This problem is exacerbated for security, where attackers actively try to find vulnerabilities that are undetectable. In addition, ICS generate vast amounts of data that could be analyzed to find abnormalities, yet, these devices are also resource-constrained. A major challenge of introducing resilience is the mechanism of decision making, that decides on the particular strategy that should be used in response to an event. In organizational or society models of resilience, humans play a major role in this. In ICS, the goal should be to eliminate the human from the process as much as possible to allow for a faster response. Yet, current algorithms are unable to provide the *creativity* necessary to come up with truly innovative strategies to respond to unpredictable events. Finally, any decision must be implemented in the hard- and software. The nature of ICS makes them inherently difficult to adapt, while guaranteeing consistency of the behavior. In addition, an interface to reconfigure a system is a potential vulnerability that can be exploited by an adversary.

B. COMMUNICATION

From a communications perspective, the proposed general idea of jointly considering resilience and mixed criticality in wireless communication systems offers plenty of research directions, areas of interest, and future perspectives. A case study presented initial insights into the key ideas of both aspects in a simple network. However, such concepts need to be applied to a variety of network setups under well-known, as well as future communication techniques to evaluate the overall performance. A variety of research opportunities rely on the concept of *large-scale* networks. Whereas the overall performance in small-scale networks heavily relies on individual connections, large-scale performance comes through the mass of connected devices. In this context, the resilience to wide-spread network outages is of special interest. How can a provider outage, cloud disruption, or the collapse of a data-highway be handled? Especially the concepts of multi-cloud networks and decentralized algorithms play a major role in resilient large-scale networks. In addition, key enablers of designing resilient communication system, how to optimize the resilience, what is the theoretical limit, and how to achieve practical implementations, are aspects to tackle in future works.

C. CONTROL

Recursive and other designs of adaptive controllers were recently applied in adaptive resilient control, i.e., in the case when a nonlinear system with unknown parameters is affected by false data injection attacks and actuator faults, e.g., see [100] and [101]. Since the designs of controllers in these and other related papers address the case of a single agent (node), it would be challenging to obtain constructive designs of adaptive and resilient decentralized and distributed controllers for large-scale and multi-agent networks along the same research lines as those considered in the above-mentioned papers [57], [58]. From this viewpoint, it is natural to raise the following questions: How can one update a distributed control algorithm (for example in [57]), if the communication channels between individual nodes of the network are affected by some external attacks, by time-delays, or by loss of information? This problem formulation can also be updated and extended in terms of mixed criticality and resilience requirements discussed in Section IV, assuming that such requirements can appear. Similarly, how can the control strategies of the agents be updated, if one of them is affected by instant variations of its internal dynamics? Recent work [72] tackles these problems and addresses recursive designs of decentralized adaptive fuzzy controllers for nonlinear interconnected systems affected by denial-of-service attacks. It would be promising to extend the methods from Section V to the case of resilient control systems systematically. For instance: Can recent work [59] be extended to the case of such problem formulation as in [100], [101], and [72]? Another promising direction in a multi-agent setting is the contract-based design of CPSs. Assume-guarantee contracts (AGCs) are used to break down global specifications in large-scale CPSs into specifications on subsystems. Also in complex large-scale CPSs not only a single specification is of interest, but a set of properties that originate from various distinct disciplines. Therefore ''design contracts'' are used to break down global design problems into smaller subproblems such as stability, schedulability when running on shared resources, and resilience when subject to an attack. Reference [102] uses for example the framework of parametric AGCs to compositionally verify and design decentralized controllers, guaranteeing a given specification for interconnected systems. An arising challenge in this context is to formulate an appropriate assume-guarantee reasoning framework and proper ''design contracts'' for a modular design of resilient mixed critical interconnected systems.

D. SECURITY

From a security perspective, the proposed general idea of jointly considering cyber resilience and mixed criticality in industrial control systems provides a wealth of research directions, and future opportunities. What is the best way to counteract a detected breach of security? How can these incidents be adverted in the future? Today, security measures need to be tuned individually to the respective use case. However, a desired goal is the application to a variety of known as well as future systems to maintain overall performance. In future work, adaptive learning, the development of a structured world model, and mechanisms for dealing with explicitly defined manipulations can be encouraged. Based

on this, a network of systems for tamper detection in critical infrastructure can be designed [84]. Resilience must be evaluated through design, appropriate optimization metrics, theoretical limits, and practical implementations that enable mixed critical resilience [85].

IX. CONCLUSION

To increase the overall system performance, flexibility, and autonomy of future ICS, especially under mixed criticality conditions, unforseeable events, and malicious attacks, this contribution considers the application of resilience and mixed criticality from a multi-domain perspective. Along with insights into the resilience and mixed criticality paradigms from a process industry point of view, the role of resilience during a system life cycle is discussed, especially focusing the design-time, and the MAPE cycle, i.e., monitoring, analysis, planning, and execution phases. Applying such cycle into a communication network controller shed lights onto lower layer resilience behavior in mixed critical networks, while a case study validates the considerations and provides promising results. Considerations from control ranged from model-based approaches to data-driven techniques and are envisioned to greatly enhance criticality-aware resilience behavior of future ICS. A security perspective, with a focus on detecting a compromise, emphasizes the necessity of a multi-disciplinary viewpoint. Joining the considered domains, namely, industry, system design, communication, control, and security and identifying synergies among them promises to be a crucial factor for resilience and mixed criticality in ICS. While many open questions, directions, opportunities, and challenges persist, this work is one step forward in establishing a baseline and finding qualitative enablers for mixed criticality-aware resilience in future ICS.

ACKNOWLEDGMENT

The authors would like to thank Hansjörg Mucke, Shaban Guma, and Kai Jansen for the many discussions and all the support during the preparation of this manuscript.

REFERENCES

[1] S. Hosseini, K. Barker, and J. E. Ramirez-Marquez, "A review of definitions and measures of system resilience," *Rel. Eng. Syst. Saf.*, vol. 145, pp. 47–61, Jan. 2016.
[2] E. Hollnagel, D. Woods, and N. Leveson, *Resilience Engineering: Concepts and Precepts*. Farnham, U.K.: Ashgate, Sep. 2006.
[3] S. Vestal, "Preemptive scheduling of multi-criticality systems with varying degrees of execution time assurance," in *Proc. IEEE 28th RTSS*, Dec. 2007, pp. 239–243.
[4] Ericsson. (Jun. 2022). *Ericsson Mobility Report June 2022*. [Online]. Available: https://www.ericsson.com/en/reports-and-papers/mobility-report/reports/june-2022
[5] A. Willig, "Recent and emerging topics in wireless industrial communications: A selection," *IEEE Trans. Ind. Informat.*, vol. 4, no. 2, pp. 102–124, May 2008.
[6] V. N. Swamy, P. Rigge, G. Ranade, B. Nikolić, and A. Sahai, "Wireless channel dynamics and robustness for ultra-reliable low-latency communications," *IEEE J. Sel. Areas Commun.*, vol. 37, no. 4, pp. 705–720, Apr. 2018.
[7] C. G. Rieger, D. I. Gertman, and M. A. McQueen, "Resilient control systems: Next generation design research," in *Proc. 2nd Conf. Hum. Syst. Interact.*, May 2009, pp. 632–636.
[8] C. Rieger, K. Schultz, T. Carroll, and T. McJunkin, "Resilient control systems—Basis, benchmarking and benefit," *IEEE Access*, vol. 9, pp. 57565–57577, 2021.
[9] M. Najarian and G. J. Lim, "Design and assessment methodology for system resilience metrics," *Risk Anal., Off. Publication Soc. Risk Anal.*, vol. 39, no. 9, pp. 1885–1898, Sep. 2019.
[10] M. Wied, J. Oehmen, and T. Welo, "Conceptualizing resilience in engineering systems: An analysis of the literature," *Syst. Eng.*, vol. 23, no. 1, pp. 3–13, Jan. 2020.
[11] G. Sansavini, "Engineering resilience in critical infrastructures," in *Resilience and Risk*. Amsterdam, The Netherlands: Springer, 2017, pp. 189–203.
[12] M.-V. Florin and I. Linkov, *IRGC Resource Guide on Resilience*. Lausanne, Switzerland: EPFL International Risk Governance Center, 2016. [Online]. Available: http://infoscience.epfl.ch/record/228206, doi: 10.5075/epfl-irgc-228206.
[13] J. Fiksel, "The new resilience paradigm-essential strategies for a changing risk landscape," *Resour. Guide Resilience*, vol. 29, no. 7, pp. 1–5, 2016.
[14] E. Zio, "Challenges in the vulnerability and risk analysis of critical infrastructures," *Reliab. Eng. Syst. Saf.*, vol. 152, pp. 137–150, Aug. 2016.
[15] K. A. Delic, "On resilience of IoT systems: The Internet of Things (ubiquity symposium)," in *Proc. Ubiquity*, Feb. 2016, pp. 1–7.
[16] J. P. G. Sterbenz, "Smart city and IoT resilience, survivability, and disruption tolerance: Challenges, modelling, and a survey of research opportunities," in *Proc. 9th RNDM*, Sep. 2017, pp. 1–6.
[17] L. Xing, "Cascading failures in Internet of Things: Review and perspectives on reliability and resilience," *IEEE Internet Things J.*, vol. 8, no. 1, pp. 44–64, Jan. 2021.
[18] A. Burns and R. Davis, "Mixed criticality systems—A review," Dept. Comput. Sci., Univ. York, Heslington, U.K., Tech. Rep., 2013, pp. 1–69.
[19] A. Burns and R. I. Davis, "A survey of research into mixed criticality systems," *ACM Comput. Surv.*, vol. 50, no. 6, pp. 1–37, Nov. 2018.
[20] H. Lasi, P. Fettke, H. G. Kemper, T. Feld, and M. Hoffmann, "Industry 4.0," *Bus. Inf. Syst. Eng.*, vol. 6, no. 4, pp. 239–242, 2014, doi: 10.1007/s12599-014-0334-4.
[21] M. Hankel and B. Rexroth, "The reference architectural model industrie 4.0 (RAMI 4.0)," *ZVEI*, vol. 2, no. 2, pp. 4–9, Apr. 2015.
[22] T. Kletz, *HAZOP and HAZAN: Identifying and Assessing Process Industry Hazards*. Boca Raton, FL, USA: CRC Press, 2018.
[23] N. Kockmann, P. Thenée, C. Fleischer-Trebes, G. Laudadio, and T. Noël, "Safety assessment in development and operation of modular continuous-flow processes," *Reaction Chem. Eng.*, vol. 2, no. 3, pp. 258–280, 2017.
[24] J. O. Kephart and D. M. Chess, "The vision of autonomic computing," *Computer*, vol. 36, no. 1, pp. 41–50, Jan. 2003.
[25] P. Arcaini, E. Riccobene, and P. Scandurra, "Modeling and analyzing MAPE-K feedback loops for self-adaptation," in *Proc. IEEE/ACM 10th SEAMS*, May 2015, pp. 13–23.
[26] D. Weyns, B. Schmerl, V. Grassi, S. Malek, R. Mirandola, C. Prehofer, J. Wuttke, J. Andersson, H. Giese, and K. M. Göschka, "On patterns for decentralized control in self-adaptive systems," in *Software Engineering for Self-Adaptive Systems II* (Lecture Notes in Computer Science), vol. 7475, R. de Lemos, H. Giese, H. A. Müller, and M. Shaw, Eds. Berlin, Germany: Springer, 2013, pp. 76–107.
[27] L. Prenzel and S. Steinhorst, "Decentralized autonomous architecture for resilient cyber-physical production systems," in *Proc. IEEE DATE*, Feb. 2021, pp. 1300–1303.
[28] L. Prenzel and S. Steinhorst, "Automated dependency resolution for dynamic reconfiguration of IEC 61499," in *Proc. IEEE ETFA*, Sep. 2021, pp. 1–8.
[29] L. Prenzel, S. Hofmann, and S. Steinhorst, "Real-time dynamic reconfiguration for IEC 61499," in *Proc. IEEE ICPS*, May 2022, pp. 1–6.
[30] J. Rohrer, J. Sterbenz, and D. Hutchison. *ResiliNets: Resilient and Survivable Networks*. Accessed: Feb. 8, 2022. [Online]. Available: https://resilinets.org/
[31] J. P. Sterbenz, D. Hutchison, E. K. Çetinkaya, A. Jabbar, J. P. Rohrer, M. Schöller, and P. Smith, "Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines," *Comput. Netw.*, vol. 54, no. 8, pp. 1245–1265, 2010.
[32] J. Rak and D. Hutchison, *Guide to Disaster-Resilient Communication Networks*. Cham, Switzerland: Springer, 2020.
[33] H. Farag, E. Sisinni, M. Gidlund, and P. Österberg, "Priority-aware wireless fieldbus protocol for mixed-criticality industrial wireless sensor networks," *IEEE Sensors J.*, vol. 19, no. 7, pp. 2767–2780, Apr. 2019.

[34] A. Burns, J. Harbin, L. Indrusiak, I. Bate, R. Davis, and D. Griffin, "AirTight: A resilient wireless communication protocol for mixed-criticality systems," in *Proc. IEEE 24th RTCSA*, Aug. 2018, pp. 65–75.

[35] J. Harbin, A. Burns, R. I. Davis, L. S. Indrusiak, I. Bate, and D. Griffin, "The AirTight protocol for mixed criticality wireless CPS," *ACM Trans. Cyber-Phys. Syst.*, vol. 4, no. 2, pp. 1–28, Apr. 2020, doi: 10.1145/3362987.

[36] J. Vestin, A. Kassler, and J. Akerberg, "Resilient software defined networking for industrial control networks," in *Proc. 10th ICICS*, Dec. 2015, pp. 1–5.

[37] P. Dini, A. Begni, S. Ciavarella, E. De Paoli, G. Fiorelli, C. Silvestro, and S. Saponara, "Design and testing novel one-class classifier based on polynomial interpolation with application to networking security," *IEEE Access*, vol. 10, pp. 67910–67924, 2022.

[38] P. Dini and S. Saponara, "Analysis, design, and comparison of machine-learning techniques for networking intrusion detection," *Designs*, vol. 5, no. 1, p. 9, Feb. 2021.

[39] T. Cinkler, A. Ladanyi, J. Rak, C. Esposito, and G. Rizzo, *Resilience of 5G Mobile Communication Systems to Massive Disruptions*. Cham, Switzerland: Springer, 2020, pp. 699–719, doi: 10.1007/978-3-030-44685-7_28.

[40] R. Bruzgiene et al., *Quality-Driven Schemes Enhancing Resilience of Wireless Networks under Weather Disruptions*. Cham, Switzerland: Springer, 2020, pp. 299–326, doi: 10.1007/978-3-030-44685-7_12.

[41] A. A. Ahmad, J. Kakar, R.-J. Reifert, and A. Sezgin, "UAV-assisted C-RAN with rate splitting under base station breakdown scenarios," in *Proc. IEEE ICC Workshops*, May 2019, pp. 1–6.

[42] A. A. Ahmad, H. Dahrouj, A. Chaaban, A. Sezgin, T. Y. Al-Naffouri, and M.-S. Alouini, "Power minimization via rate splitting in downlink cloud-radio access networks," in *Proc. IEEE ICC Workshops*, Jun. 2020, pp. 1–6.

[43] R.-J. Reifert, S. Roth, A. A. Ahmad, and A. Sezgin, "Energy efficiency in rate-splitting multiple access with mixed criticality," in *Proc. IEEE ICC Workshops*, May 2022, pp. 681–686.

[44] R.-J. Reifert, S. Roth, A. Alameer Ahmad, and A. Sezgin, "Comeback kid: Resilience for mixed-critical wireless network resource management," 2022, *arXiv:2204.11878*.

[45] J. Kakar and A. Sezgin, "A survey on robust interference management in wireless networks," *Entropy*, vol. 19, no. 7, p. 362, Jul. 2017. [Online]. Available: https://www.mdpi.com/1099-4300/19/7/362

[46] R.-J. Reifert, A. A. Ahmad, H. Dahrouj, A. Chaaban, A. Sezgin, T. Y. Al-Naffouri, and M.-S. Alouini, "Joint beamforming and clustering for energy efficient multi-cloud radio access networks," in *Proc. IEEE WCNC*, Apr. 2022, pp. 608–613.

[47] R.-J. Reifert, A. A. Ahmad, H. Dahrouj, A. Chaaban, A. Sezgin, T. Y. Al-Naffouri, and M.-S. Alouini, "Distributed resource management in downlink cache-enabled multi-cloud radio access networks," *IEEE Trans. Veh. Technol.*, early access, Aug. 1, 2022, doi: 10.1109/TVT.2022.3195342.

[48] F. Pierri, G. Muscio, and F. Caccavale, "An adaptive hierarchical control for aerial manipulators," *Robotica*, vol. 36, no. 10, pp. 1527–1550, Oct. 2018.

[49] S. Sui and C. L. P. Chen, "Adaptive output-feedback finite-time stabilisation of stochastic non-linear systems with application to a two-stage chemical reactor," *IET Control Theory Appl.*, vol. 13, no. 4, pp. 534–542, Mar. 2019.

[50] S. Mehraeen, S. Jagannathan, and M. L. Crow, "Power system stabilization using adaptive neural network-based dynamic surface control," *IEEE Trans. Power Syst.*, vol. 26, no. 2, pp. 669–680, May 2011.

[51] I. Kanellakopoulos, P. V. Kokotovic, and A. S. Morse, "Systematic design of adaptive controllers for feedback linearizable systems," in *Proc. ACC*, Jun. 1991, pp. 649–654.

[52] M. Krstić, I. Kanellakopoulos, and P. V. Kokotović, "Adaptive nonlinear control without overparametrization," *Syst. Control Lett.*, vol. 19, no. 3, pp. 177–185, 1992, doi: 10.1016/0167-6911(92)90111-5.

[53] X. Hu, X. Wei, H. Zhang, and J. Han, "Adaptive saturation compensation for strict-feedback systems with unknown control coefficient and input saturation," *Int. J. Adapt. Control Signal Process.*, vol. 35, no. 6, pp. 1083–1098, Jun. 2021.

[54] H. Wang and Q. Zhu, "Adaptive state feedback stabilisation for more general switched stochastic non-linear systems under arbitrary switchings," *IET Control Theory Appl.*, vol. 14, no. 6, pp. 878–886, Apr. 2020, doi: 10.1049/iet-cta.2019.0976.

[55] Z. P. Jiang, A. R. Teel, and L. Praly, "Small-gain theorem for ISS systems and applications," *Math. Control, Signals, Syst.*, vol. 7, no. 2, pp. 95–120, 1994, doi: 10.1007/BF01211469.

[56] Z.-P. Jiang, "A combined backstepping and small-gain approach to adaptive output feedback control," *Automatica*, vol. 35, no. 6, pp. 1131–1139, 1999, doi: 10.1016/S0005-1098(99)00015-1.

[57] T. Liu and Z.-P. Jiang, "Distributed output-feedback control of nonlinear multi-agent systems," *IEEE Trans. Autom. Control*, vol. 58, no. 11, pp. 2912–2917, Nov. 2013.

[58] S. Dashkovskiy and S. Pavlichkov, "Stability conditions for infinite networks of nonlinear systems and their application for stabilization," *Automatica*, vol. 112, Feb. 2020, Art. no. 108643, doi: 10.1016/j.automatica.2019.108643.

[59] S. Pavlichkov and N. Bajcinca, "Decentralized adaptive stabilization of infinite networks of switched nonlinear systems with unknown control directions," presented at the 61st IEEE Conf. Decis. Control, Cancún, Mexico, Dec. 6–9, 2022. [Online]. Available: https://cdc2022.ieeecss.org/

[60] B. Zhu and X. Xia, "Lyapunov-based adaptive model predictive control for unconstrained non-linear systems with parametric uncertainties," *IET Control Theory Appl.*, vol. 10, no. 15, pp. 1937–1943, Oct. 2016, doi: 10.1049/iet-cta.2016.0203.

[61] P. Dini and S. Saponara, "Processor-in-the-Loop validation of a gradient descent-based model predictive control for assisted driving and obstacles avoidance applications," *IEEE Access*, vol. 10, pp. 67958–67975, 2022.

[62] Z.-P. Jiang et al., "Learning-based control: A tutorial and some recent results," *Found. Trends Syst. Control*, vol. 8, no. 3, pp. 176–284, 2020.

[63] J. Hornegger and H. Niemann, "Statistical learning, localization, and identification of objects," in *Proc. ICCV*, 1995, pp. 914–919.

[64] J. Chai, H. Zeng, A. Li, and E. W. T. Ngai, "Deep learning in computer vision: A critical review of emerging techniques and application scenarios," *Mach. Learn. Appl.*, vol. 6, Dec. 2021, Art. no. 100134.

[65] V. Mnih, K. Kavukcuoglu, D. Silver, A. Graves, I. Antonoglou, D. Wierstra, and M. Riedmiller, "Playing Atari with deep reinforcement learning," 2013, *arXiv:1312.5602*.

[66] M. Hausknecht and P. Stone, "Deep recurrent *Q*-learning for partially observable MDPs," in *Proc. AAAI Fall Symp. Ser.*, 2015, pp. 1–9.

[67] V. Singh and H. Kodamana, "Reinforcement learning based control of batch polymerisation processes," *IFAC-PapersOnLine*, vol. 53, no. 1, pp. 667–672, 2020.

[68] M. Wang, S. S. Ge, and K.-S. Hong, "Approximation-based adaptive tracking control of pure-feedback nonlinear systems with multiple unknown time-varying delays," *IEEE Trans. Neural Netw.*, vol. 21, no. 11, pp. 1804–1816, Nov. 2010.

[69] Y. Yang, G. Feng, and J. Ren, "A combined backstepping and small-gain approach to robust adaptive fuzzy control for strict-feedback nonlinear systems," *IEEE Trans. Syst., Man, Cybern. A, Syst., Humans*, vol. 34, no. 3, pp. 406–420, May 2004.

[70] P. Dini and S. Saponara, "Design of adaptive controller exploiting learning concepts applied to a BLDC-based drive system," *Energies*, vol. 13, no. 10, p. 2512, May 2020.

[71] W. He, Z. Yan, Y. Sun, Y. Ou, and C. Sun, "Neural-learning-based control for a constrained robotic manipulator with flexible joints," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 29, no. 12, pp. 5993–6003, Dec. 2018.

[72] L. An and G.-H. Yang, "Decentralized adaptive fuzzy secure control for nonlinear uncertain interconnected systems against intermittent DoS attacks," *IEEE Trans. Cybern.*, vol. 49, no. 3, pp. 827–838, Mar. 2019.

[73] S. G. Khan, G. Herrmann, F. L. Lewis, T. Pipe, and C. Melhuish, "Reinforcement learning and optimal adaptive control: An overview and implementation examples," *Annu. Rev. Control*, vol. 36, no. 1, pp. 42–59, Apr. 2012.

[74] L. Brunke, M. Greeff, A. W. Hall, Z. Yuan, S. Zhou, J. Panerati, and A. P. Schoellig, "Safe learning in robotics: From learning-based control to safe reinforcement learning," *Annu. Rev. Control, Robot., Auto. Syst.*, vol. 5, no. 1, pp. 411–444, May 2022, doi: 10.1146/annurev-control-042920-020211.

[75] J. C. Willems, P. Rapisarda, I. Markovsky, and B. L. M. De Moor, "A note on persistency of excitation," *Syst. Control Lett.*, vol. 54, no. 4, pp. 325–329, Apr. 2005.

[76] J. Coulson, J. Lygeros, and F. Dörfler, "Data-enabled predictive control: In the shallows of the DeePC," in *Proc. 18th ECC*, Jun. 2019, pp. 307–312.

[77] C. De Persis and P. Tesi, "Formulas for data-driven control: Stabilization, optimality, and robustness," *IEEE Trans. Autom. Control*, vol. 65, no. 3, pp. 909–924, Mar. 2020.

[78] A. Aminifar, P. Tabuada, P. Eles, and Z. Peng, "Self-triggered controllers and hard real-time guarantees," in *Proc. IEEE DATE*, Mar. 2016, pp. 636–641.
[79] Q. Sun, K. Zhang, and Y. Shi, "Resilient model predictive control of cyber–physical systems under DoS attacks," *IEEE Trans. Ind. Informat.*, vol. 16, no. 7, pp. 4920–4927, Jul. 2020.
[80] M. Al Khatib and N. Bajcinca, "Resilient scheduler and controller codesign for mixed-critical embedded control systems," presented at the 12th IFAC NOLCOS, 2022.
[81] R. Ross, R. Graubart, D. Bodeau, and R. McQuaid, "Systems security engineering: Cyber resiliency considerations for the engineering of trustworthy secure systems," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. NIST SP 800-160, 2018.
[82] N. C. Rowe and J. Rrushi, *Introduction to Cyberdeception*. Berlin, Germany: Springer, 2016.
[83] M. Pomerleau, *ONR Moves to Protect Ships' Systems From Cyberattacks*. Falls Church, VA, USA: Government Comput. News, 2015.
[84] A. Kott, L. Mancini, P. Theron, M. Drašar, E. Dushku, H. Günther, M. Kont, B. LeBlanc, A. Panico, M. Pihelgas, and K. Rzadca, "Initial reference architecture of an intelligent autonomous agent for cyber defense," U.S. Army Res. Lab., Adelphi, MD, USA, Release 2.0, Tech. Rep. ARL-SR-0421, 2018. [Online]. Available: https://apps.dtic.mil/sti/pdfs/AD1080471.pdf
[85] A. Kott and I. Linkov, "To improve cyber resilience, measure it," *Computer*, vol. 54, no. 2, pp. 80–85, 2021, doi: 10.1109/MC.2020.3038411.
[86] U.S. Department of Defense Instruction. (2014). *Cybersecurity*. [Online]. Available: https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodi/850001_2014.pdf
[87] B. Trump and I. Linkov, *The Science and Practice of Resilience*. Cham, Switzerland: Springer, Feb. 2019.
[88] A. Kott and I. Linkov, *Cyber Resilience of Systems and Networks*, 1st ed. New York, NY, USA: Springer, 2018.
[89] I. Linkov, D. A. Eisenberg, K. Plourde, T. P. Seager, J. Allen, and A. Kott, "Resilience metrics for cyber systems," *Environ. Syst. Decisions*, vol. 33, no. 4, pp. 471–476, Dec. 2013.
[90] A. Waldman. (2020). After a brief pause, trickbot rebounds from takedown efforts. TechTarget. [Online]. Available: https://searchsecurity.techtarget.com/news/252490814/After-a-brief-pause-Trickbot-rebounds-from-takedown-efforts
[91] T. Ring, "Connected cars—The next target for hackers," *Netw. Secur.*, vol. 2015, no. 11, pp. 11–16, 2015.
[92] M. Krotofil and J. W. Larsen, "Rocking the pocket book: Hacking chemical plants for competition and extortion," 2015.
[93] C. Zenger, H. Vogt, J. Zimmer, A. Sezgin, and C. Paar, "The passive eavesdropper affects my channel: Secret-key rates under real-world conditions," in *Proc. IEEE Globecom Workshops*, Dec. 2016, pp. 1–6.
[94] W. Wang and E. W. Gill, "Comparison of a modified periodogram and standard periodogram for current estimation by an HF surface radar," in *Proc. OCEANS TAIPEI*, Apr. 2014, pp. 1–7.
[95] L. Biggio and I. Kastanis, "Prognostics and health management of industrial assets: Current progress and road ahead," *Frontiers Artif. Intell.*, vol. 3, Nov. 2020, Art. no. 578613.
[96] T. Zonta, C. A. da Costa, R. da Rosa Righi, M. J. de Lima, E. S. da Trindade, and G. P. Li, "Predictive maintenance in the industry 4.0: A systematic literature review," *Comput. Ind. Eng.*, vol. 150, Dec. 2020, Art. no. 106889.
[97] C. Spreafico, D. Russo, and C. Rizzi, "A state-of-the-art review of FMEA/FMECA including patents," *Comput. Sci. Rev.*, vol. 25, pp. 19–28, Aug. 2017.
[98] F. Crawley and B. Tyler, *HAZOP: Guide to Best Practice*, 3rd ed., F. Crawley and B. Tyler, Eds. Amsterdam, The Netherlands: Elsevier, 2015.
[99] J. I. Single, "Automation of the hazard and operability method using ontology-based scenario causation models," Ph.D. thesis, Dept. Mech. Process Eng., Technische Universität Kaiserslautern, Kaiserslautern, Germany, 2022. [Online]. Available: http://nbn-resolving.de/urn:nbn:de:hbz:386-kluedo-67413
[100] S. Song, J. H. Park, B. Zhang, and X. Song, "Adaptive NN finite-time resilient control for nonlinear time-delay systems with unknown false data injection and actuator faults," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 33, no. 10, pp. 5416–5428, Oct. 2022.
[101] X. Jin, W. M. Haddad, and T. Yucelen, "An adaptive control architecture for mitigating sensor and actuator attacks in cyber-physical systems," *IEEE Trans. Autom. Control*, vol. 62, no. 11, pp. 6058–6064, Nov. 2017.
[102] M. Al Khatib and M. Zamani, "Controller synthesis for interconnected systems using parametric assume-guarantee contracts," in *Proc. IEEE ACC*, Jul. 2020, pp. 5419–5424.

ROBERT-JERON REIFERT (Graduate Student Member, IEEE) received the B.Sc. and M.Sc. degrees in electrical engineering and information technology from Ruhr University Bochum, Germany, in 2019 and 2021, respectively, where he is currently pursuing the Ph.D. degree with the Institute of Digital Communication Systems. His research interests include wireless communication systems, mixed criticality, and resilience in 6G communication networks and beyond. He was one of the recipient of the Association for Electrical, Electronic and Information Technologies (VDE) Rhein-Ruhr Graduate Student Award, in 2021.

MARTIN KRAWCZYK-BECKER received the Dipl.-Ing. degree in electrical engineering and information sciences from Ruhr University Bochum, Germany, in 2011, and the Dr.-Ing. degree from the Faculty of Medicine and Health Sciences, Universität Oldenburg, Germany, in 2016. From 2016 to 2018, he was a Postdoctoral Researcher at the University of Hamburg, Germany. He is currently with KROHNE Innovation GmbH, where he leads the Corporate Research Group. His research interests include digital signal processing and process automation technology.

LAURIN PRENZEL received the M.Sc. degree in mechanical engineering from the Technical University of Munich (TUM), Munich, Germany, in 2017. He has been a Research Associate at the Embedded Systems and the Internet of Things Group, Department of Electrical and Computer Engineering, TUM, since 2019. He was a Research Associate at the Safe Embedded Systems Group, Department of Mechanical Engineering, TUM, from 2017 to 2019. His research interests include dynamic reconfiguration of industrial control systems and resilient system architectures.

SVYATOSLAV PAVLICHKOV received the M.Sc. (Hons.) and Ph.D. degrees in mathematics from V. N. Karazin Kharkiv National University, Ukraine, in 1997 and 2002, respectively. He served as an Assistant Lecturer, a Senior Lecturer, and a Docent at the Faculty of Mechanical Engineering and Mathematics, V. N. Karazin Kharkiv National University; and the Faculty of Computer Science and Mathematics, V. I. Vernadsky Taurida National University. He was a Postdoctoral Research Fellow at the Center of Industrial Mathematics, University of Bremen; University of Applied Sciences Erfurt; Institute of Computer Science and Mathematics, University of Passau; Institute of Mathematics, University of Wuerzburg; Faculty of Science and Engineering, University of Groningen; and Department of Electrical and Computer Engineering, National University of Singapore. He was also visiting the Department of Mathematics, Louisiana State University, in 2005; and the Institute of Mathematics and Computer Science, University of Greifswald, in 2004 and 2008, as a Visiting Researcher. Since October 2021, he has been a Postdoctoral Researcher at the Department of Mechanical and Process Engineering, Technical University of Kaiserslautern. His research interests include nonlinear control and systems theory.

MOHAMMAD AL KHATIB received the Electrical Engineering degree from Lebanese University, Lebanon, in 2014, the M.Sc. degree in systems and control from the University of Joseph Fourier, France, in 2014, and the Ph.D. degree in applied mathematics from the University of Grenoble Alpes, France, in 2017. He has been a Postdoctoral Researcher with the Department of Mechanical Engineering, Technical University of Kaiserslautern (TUK), since January 2022. Prior to that, he held a postdoctoral position at the Technical University of Chemnitz, from 2020 to 2022, and the Technical University of Munich (TUM) from 2018 to 2020. His research interests include large-scale embedded control systems, network control systems, and data-driven control.

SANDESH ATHNI HIREMATH received the master's degree in computer science and the Ph.D. degree in mathematics from TU Kaiserslautern, in 2013 and 2017, respectively. During this time, he worked on modeling, analysis, and simulation of multiscale nonlinear stochastic systems. From 2018 to 2021, he worked with Valeo Schalter und Sensoren as an Algorithm Developer, for developing vision based automated parking functionality for BMW. Since April 2021, he has been working as a Postdoctoral Researcher at the Mechatronics Department, TU Kaiserslautern, where he is currently working on implementing perception and control algorithms for autonomous vehicles. His research interests include learning based controllers, reinforcement learning, and modeling and analysis of random dynamical systems, especially the pattern forming and self-organizing behaviors of such systems.

MANAR AL-ASKARY received the Master of Science degree in electrical engineering and information sciences from the TU Dortmund, Germany, in 2016. He is currently employed at PHYSEC GmbH, where he works as a Product Manager and a Field Application Engineer. His research interests include secure communication, tamper detection, and digital signal processing.

NAIM BAJCINCA graduated the degree in theoretical physics and electrical engineering from the University of Prishtina, Kosova. He received the Ph.D. degree in robust control from the Institute of Robotics and Mechatronics, Technical University of Berlin; and the German Aerospace Research Center (DLR), Oberpfaffenhofen, Germany. He worked as a Research Associate with the Max–Planck Institute for Dynamics of Complex Technical Systems (Magdeburg), prior to accepting a Full Professor position at the Department of Mechanical and Process Engineering, University of Kaiserslautern, Germany. His research interests include control theory, stability analysis and control design in robust and optimal control, hybrid dynamical systems, networked control systems, stochastic control, and data-driven and learning-based control. His work on applied control comprises various domains of engineering and life sciences, including robotics, human–machine interaction, embedded and cyber-physical systems, autonomous systems, power systems, production systems, process engineering, and systems biology.

SEBASTIAN STEINHORST (Senior Member, IEEE) received the M.Sc. (Dipl.-Inf.) and Ph.D. (Dr.Phil.Nat.) degrees in computer science from Goethe University, Frankfurt, Germany, in 2005 and 2011, respectively. He is currently an Associate Professor at the Technical University of Munich (TUM), Germany, where he leads the Embedded Systems and the Internet of Things Group, Department of Electrical and Computer Engineering. He was also a Co-Program PI with the Electrification Suite and Test Laboratory, Research Center TUMCREATE, Singapore. His research interests include design methodology and hardware/software architecture co-design of secure distributed embedded systems for use in the IoT, automotive, and smart energy applications.

AYDIN SEZGIN (Senior Member, IEEE) received the Dr.-Ing. (Ph.D.) degree in electrical engineering from TU Berlin, in 2005. From 2001 to 2006, he was with the Heinrich-Hertz-Institute, Berlin. From 2006 to 2008, he held a postdoctoral position and a Lecturer with the Information Systems Laboratory, Department of Electrical Engineering, Stanford University, Stanford, CA, USA. From 2008 to 2009, he held a postdoctoral position with the Department of Electrical Engineering and Computer Science, University of California, Irvine, CA. From 2009 to 2011, he was the Head of the Emmy-Noether-Research Group on Wireless Networks, Ulm University. In 2011, he joined TU Darmstadt, Germany, as a Professor. He is currently a Professor with the Ruhr University Bochum, Germany. He has published several book chapters and more than 60 journals and 180 conference papers. He was a winner of the ITG-Sponsorship Award, in 2006. He was a first recipient of the prestigious Emmy-Noether Grant by the German Research Foundation in communication engineering, in 2009. He has coauthored papers that received the Best Poster Award at the IEEE Communication Theory Workshop, in 2011; the Best Paper Award at ICCSPA, in 2015; and the Best Paper Award at ICC, in 2019.