Graceful Degradation of Control Device Operation Under Attack

Rainer Falk, Christian Feist, and Steffen Fries
Siemens AG
Foundational Technologies
Munich, Germany
e-mail: {rainer.falk|christian.feist|steffen.fries}@siemens.com

***Abstract*—Cybersecurity includes preventing, detecting, and reacting to cyber-security attacks. Cyber resilience goes one step further and aims to maintain essential functions even during ongoing attacks, allowing to deliver an intended service or to operate a technical process, and to recover quickly back to regular operation. During an ongoing attack, the impact on the overall system operation is limited if the attacked system stays operational, maybe with degraded performance or functionality. Control devices of a cyber physical system monitor and control a technical process. This paper describes a concept for a control device that reduces its operation depending on the current threat landscape, maintaining its basic and essential functionalities. If attacks have been detected, or if relevant vulnerabilities have been identified, the functionality is increasingly limited, thereby reducing the attack surface in risky situations, while allowing the device and the cyber physical system to stay operational.**

Keywords–cyber resilience; cyber physical system; industrial security; cybersecurity.

I. INTRODUCTION

A Cyber Physical System (CPS), e.g., an industrial automation and control system, contains control devices that interact with the real, physical world using sensors and actuators. They implement the functionality to control and monitor the operations in the physical world, e.g., a production system or a power automation system. A control device can be a physical device, e.g., an industrial Internet of Things (IoT) device, an electronic control unit, a Programmable Logic Controller (PLC), or a virtualized control device, e.g., a container or virtual machine executed on a compute platform. Control devices communicate via data networks to exchange control commands and to monitor the CPS operation to realize different automation use cases. These use cases may comprise predictive maintenance or the reconfiguration of control devices for flexible automation and for optimizing operational systems (Industry 4.0), or specific line protection features in power system operation. The connectivity of control devices is thereby increasingly extended towards enterprise networks and towards cloud-based services, increasing the exposure towards attacks originating from external networks or the Internet [2].

Being resilient means to be able to withstand or recover quickly from difficult conditions [3][4]. The Cybersecurity puts the focus on preventing, detecting, and reacting to cyber-security attacks. With cyber resilience, the scope is extended to the aspect to continue to deliver an intended outcome despite an ongoing cyber attack, and also to recover quickly back to regular operation. When an attack is carried out, the impact on the overall system operation is limited if the attacked system stays operational, even with degraded performance or functionality. Even during attacks, intended services can still be provided, at least in a limited way.

This paper, as an extended version of [1], describes a concept for a control device that can adapt to a changing threat landscape by adapting and limiting its provided functionality. If attacks have been detected, or if relevant vulnerabilities have been identified, devices can limit their functionality increasingly towards only basic and essential functions, thereby reducing their attack surface in risky situations. Basic and essential functions refer to the main functionality of a device that contribute to the intended operational use case and the embedding operational environment. This paper extends [1] by giving an overview on industrial CPS and their cybersecurity, and by describing the concept of a resilience engine, an isolated execution environment ensuring that the resilience functionality is executed in a trustworthy way even if the main functionality of the control device has been manipulated. Furthermore, the evaluation section has been extended.

The remainder of the paper is structured as follows: Section II gives an overview on related work, Section III on industrial CPS, and Section IV on their integrity protection. Section V describes the concept of graceful degradation under attack, and Section VII presents a usage example in industrial automation systems. Section VIII provides an evaluation of the presented approach from different perspectives relevant for an industrial application. Section IX concludes the paper and gives an outlook towards future work.

II. RELATED WORK

Cybersecurity requirements for Industrial Automation and Control Systems (IACS) are defined in the standard series IEC62443 [5]. This series provides a holistic security framework as a set of standards defining security requirements for the development process and the operation of IACS, as well as technical cybersecurity requirements on automation systems and the used components. IEC62443 requires that the IACS security measures do not cause a loss of essential services and functions, i.e., essential functions

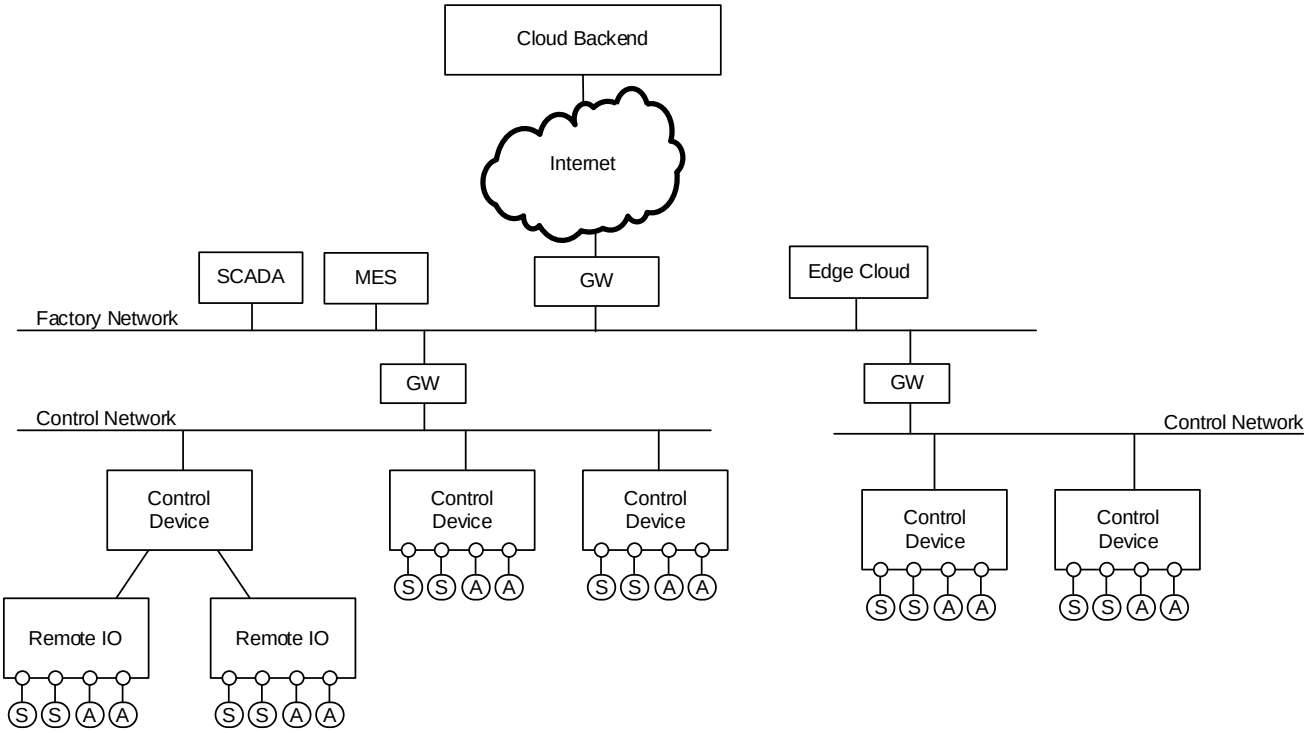

Figure 1. Industrial Cyber Physical System.

have to be kept operational in a degraded operation mode. A main objective is that deployed cybersecurity measures do not negatively impact the availability of the IACS operations. An essential function is defined as a "function or capability that is required to maintain health, safety, the environment and availability for the equipment under control". Essential functions have to be maintained also during denial-of-service attacks, or if a zone boundary protection, e.g., a network firewall, activates an island mode with limited or no connectivity. Further requirements address backups of the configuration of IACS devices, allowing to restore configurations, and the recovery and reconstitution to a known secure state after an incident.

Cyber resilience in the broader meaning to keep systems operational under attack and to recover quickly gets increasing attention, as can be seen by recent security standards and the regulation of the European Cyber Resilience Act (CRA) [6] and the Delegated Regulation for the Radio Equipment Directive (RED) [7]. The regulation of the Cyber Resilience Act (CRA) [6] includes in Annex I the requirement to maintain essential and basic functions under attack ("protect the availability of essential and basic functions, also after an incident, including through resilience and mitigation measures against denial-of-service attacks"). The development of corresponding standards addressing CRA regulative requirements has just started. The NIST Cybersecurity Framework (CSF) 2.0 [11] gives general guidance on managing risk, addresses resilience for normal and adverse situations. The standard NIST SP800-193 [8] describes technology-independent guidelines for resilience of platform firmware. Resilience-specific roots of trust are defined for update of platform firmware, for detection of a corrupted firmware, and for recovery from a compromised platform state. England et al. give a high-level overview of the Cyber Resilient Platforms Program (CyReP) [10], describing hardware and software components addressing NIST SP800-193 requirements. A working group on "cyber resilient technologies" of the Trusted Computing Group (TCG) is working on technologies to enhance cyber resilience of connected systems. Here, different building blocks for cyber resilient platforms have been described that allow to recover from a malfunction reliably back into a well-defined operational state [9]. Such building blocks support cyber resilience as they allow to recover quickly and with reasonable effort from a manipulated state. Basic building blocks are a secure execution environment for the resilience engine on a device, protection latches to protect access to persistent storage of the resilience engine even of a compromised device, and watchdog timers to ensure that the resilience engine can in fact perform a recovery. A further standard, ETSI EN 303 645 [12], describes specific security requirements for the consumer IoT device domain, addressing also resilience by the requirement to "remain operating and locally functional in the case of a loss of network access".

III. Industrial Cyber Physical Systems

An industrial CPS, i.e., an IACS, monitors and controls a technical system. Examples are process automation, factory automation, production machines, building automation, energy automation, and cloud robotics. Figure 1 shows an

example of an IACS, comprising different control networks connected to a factory network and a cloud backend system. Sensors (S) and actuators (A) of a technical system are connected with control devices directly or via remote input/output (IO) modules. The technical process is controlled by measuring its current state using the sensors, and by determining the corresponding actuator signals. Separation of the network by gateways (GW) is used to realize distinct control networks with strict real-time requirements for the interaction between sensors and actuators of a production cell, or to enforce a specific security policy within a production cell. A Supervisory Control and Data Acquisition (SCADA) system allows operators to monitor and influence the technical operation, and a Manufacturing Execution System (MES) can be used to plan, track, and document manufacturing steps.

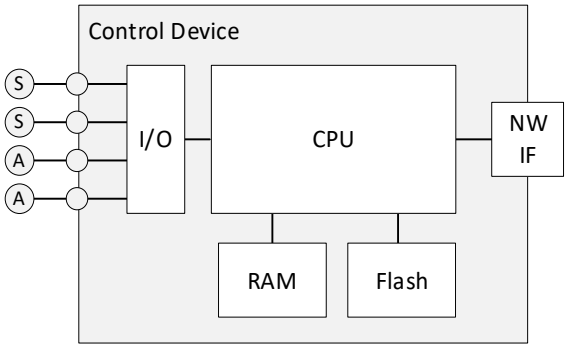

Figure 2. Control Device.

Figure 2 shows the typical structure of automation components that monitor and control the physical world using sensors and actuators. The monitoring and control functionality is defined by its firmware/software that is executed on a central processing unit (CPU) and the corresponding configuration data, both stored in non-volatile memory (Flash). A network interface (NW IF) allows communication with other devices, e.g., via Ethernet or via wireless communications as wireless local area network (WLAN) or a private 5th generation (5G) mobile communication system.

In a CPS, the impact of an attack in the OT system may not only affect data and data processing as in classical IT, but it may have an effect also on the physical world. For example, production equipment could be damaged, or the physical process may operate outside the designed physical boundaries, so that the produced goods may not have the expected quality, or even safety-related requirements could be affected.

IV. CPS CYBERSECURITY

Cybersecurity mechanisms have been known for many years and are applied in smart devices (Internet of Things, Cyber Physical Systems, industrial and energy automation systems, operation technology). Such mechanisms target source authentication, system and communication integrity, and confidentiality of data in transit or at rest.

A. Industrial Security

Protecting IACS against intentional attacks is demanded by operators to ensure a reliable operation, and also by regulation. The main relevant industrial security standard that describes security from a holistic perspective is IEC 62443 [3]. Security requirements defined by the industrial security standard IEC 62443 range from security processes during development and operation of devices and systems, personal and physical security, device security, network security, and application security, addressing the device manufacturer, the integrator as well as the operator of the IACS.

Industrial security is also called Operation Technology (OT) security, to distinguish it from general IT security. Industrial systems have different security priorities and requirements compared to common IT systems. Typically, availability and integrity of an automation system have higher priority than confidentiality. Specific requirements and side conditions of industrial automation systems like high availability, planned configuration (engineering info), scheduled maintenance windows, long life cycles, unattended operation, real-time operation, and communication, as well as safety requirements have to be considered when designing an OT security solution.

B. Control Device Integrity

The objective of device integrity is to ensure that a single device is not manipulated in an unauthorized way, ensuring that it operates as genuine device. Device integrity is highly relevant for industrial control devices to ensure their reliable operation.

Integrity protection includes the integrity of the device firmware, the integrity of the device configuration, but also its physical integrity. The main technologies to protect device integrity are:

- Secure boot: A device loads at start-up only unmodified, authorized firmware. Typically, a device verifies the digital signature of loaded firmware before executing it.
- Measured boot: The loaded software modules are checked at the time they are loaded. Usually, a cryptographic hash value is recorded in a platform configuration register of a hardware or firmware Trusted Platform Module (TPM). The configuration information can be used to grant access to keys, or it can be attested towards third parties.
- Protected firmware update: When the firmware of a device is updated, the integrity and authenticity of the firmware update is checked. The firmware update image can be digitally signed.
- Application whitelisting: Only allowed, known applications can be started on a device. A whitelist defines which application binaries can be started.
- Runtime integrity checks: During operation, the device performs a self-test of security functionality and integrity checks to verify whether it is operating as expected. Integrity checks can verify the integrity of files, configuration data, software modules, and runtime data

as the process list, i.e., the list of currently executed processes.

- Process isolation, kernel-based Mandatory Access Control (MAC): Hypervisors, OS-level virtualization such as containers, or kernel-based MAC systems can be used to isolate different classes of software (security domains). An attack or malfunction of one security domain does not affect other security domains on the same device.
- Tamper evidence, tamper protection: The physical integrity of a device can be protected, e.g., by security seals or by tamper sensors that detect opening or manipulation of the housing.
- Device integrity self-test: A device performs a self-test to detect failures. The self-test is performed typically during startup and is repeated regularly during operation.
- Operation integrity checks: Measurements on the device can be compared with the expected behavior in the operative environment. An example is the measurement of connection attempts to/from the device, based on parameters of a Management Information Base (MIB).

These technologies protect the device integrity, ensuring that the device's control functionality operates as designed, and to detect manipulations. Device resilience technologies are needed on top to support a reliable operation during attacks and to recover quickly.

C. Cyber Physical System Integrity Monitoring

Integrity does not only affect single devices, but also the overall system level comprising a set of interconnected devices. The main approaches to protect system integrity are collecting and analyzing information at system level:

- Centralized Logging: Devices provide log data, e.g., using Open Platform Communication Unified Architecture (OPC UA) protocol, Simple Network Management Protocol (SNMP), or syslog protocol, to a centralized logging system for further analysis. This may be done in a Security Information and Event Management (SIEM) System and lead to reactions on identified cybersecurity events.
- Runtime device integrity measurements: A device integrity agent provides information gathered during the operation of the device (see also subsection B above). It collects integrity information on the device and provides it for further analysis. Basic integrity information includes the results of a device self-test, and information on the current device configuration (firmware version, patches, installed applications, configuration). Furthermore, runtime information can be gathered and provided for analysis (e.g., process list, file system integrity check values, partial copy of memory).
- Network monitoring: The network communication is intercepted, e.g., using a network tap or a mirror port of a network switch.

The captured integrity information can be used for system runtime integrity monitoring to detect integrity violations in in a timely manner. Operators can be informed, or actions can be triggered automatically. Furthermore, the information is archived for later investigations. This allows that integrity violations can be detected also later with a high probability, so that corresponding countermeasures can be initiated (e.g., plan for an additional quality check of produced goods).

An intelligent analysis platform performs data analysis (e.g., statistical analysis, big data analysis, artificial intelligence) and triggers suitable respondence actions (e.g., alarm, remote wipe of a device, revocation of a device, stop of a production site, planning for additional test of manufactured goods).

D. Resilience Under Attack

In a cyber physical environment, a main objective is that the CPS stays operational and that its integrity is ensured. In the context of an industrial automation and control system, that means that intended actions of the system in the physical world continue to take place even when the automation and control system of the CPS is attacked successfully. Risk management, the established approach to cyber security, identifies threats and determines the risk depending on probability and impact of a potential attack. The objective is to put the focus of defined security measures on the most relevant risks, reducing the probability that a successful attack takes place, and reducing the impact of successful attacks, e.g., by detecting successful attacks by security monitoring allowing to react, e.g., by shutting down a CPS.

Resilience, however, puts the focus on a reduction of the impact of successful attacks, where the system can stay operational with a degraded performance or functionality, and to recover quickly from a successful attack.

Being resilient means to be able to withstand or recover quickly from difficult conditions [12]. It shifts the focus of "classical" IT and OT security, which put the focus on preventing, detecting, and reacting to cyber-security attacks, to the aspect to continue to deliver an intended outcome despite an adverse cyber attack taking place, and to recover quickly back to regular operation. More specifically, resilience of a system is the property to be resistant to a range of threats and withstand the effects of a partial loss of capability, and to recover and resume its provision of service with the minimum reasonable loss of performance.

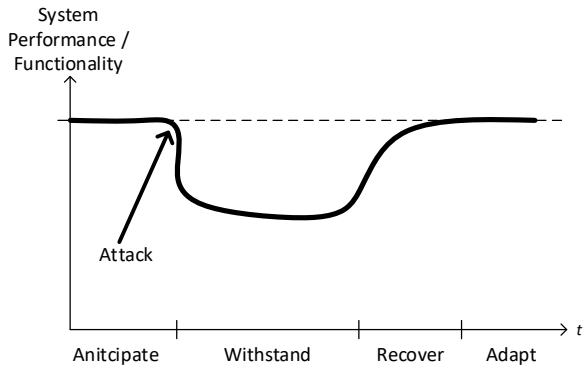

Figure 3. Concept of Cyber Resilience.

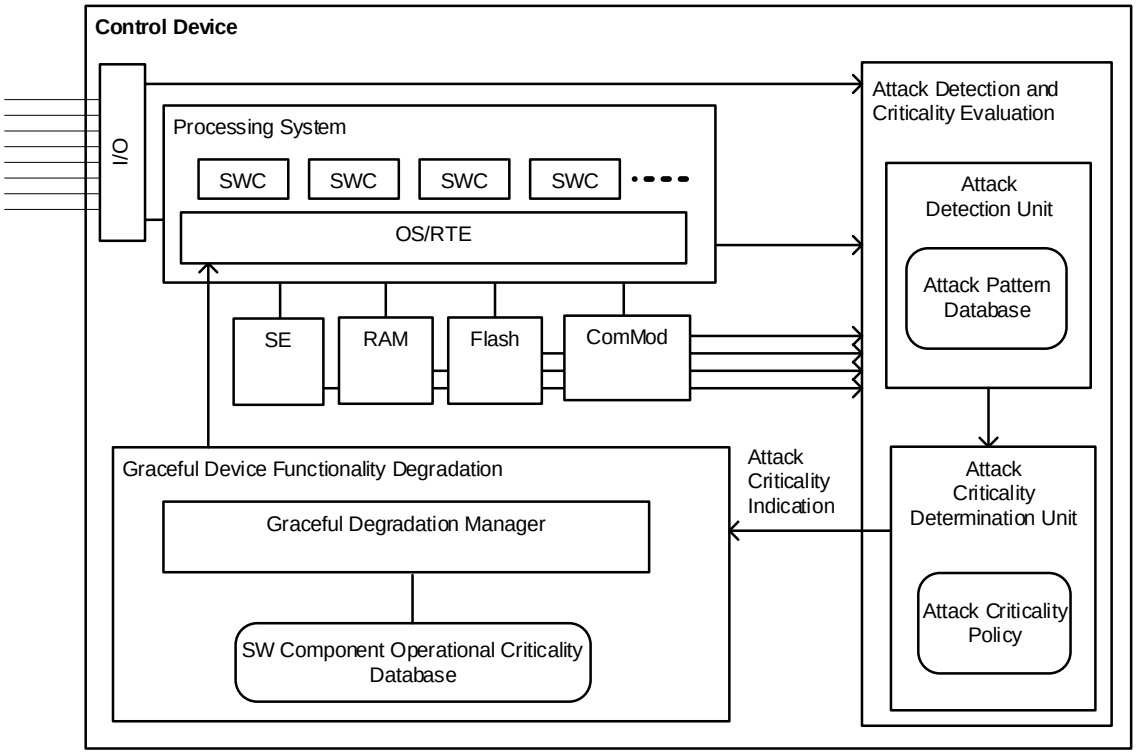

Figure 4. Control Device with graceful degradation under attack.

Figure 3 illustrates the concept of cyber resilience: When an attack is ongoing, the impact on the CPS operation is limited as basic and essential functionality is maintained in a reliable way. The effects of an attack on the CPS operation are "absorbed", so that the CPS can stay operational, but with limited performance or functionality. In particular, it can be avoided that the CPS has to be shut down completely. A recovery takes place to bring the system up to the regular operation in a fast and trustworthy way.

V. CONTROL DEVICE WITH GRACEFUL DEGRADATION UNDER ATTACK

Control devices of a cyber physical system monitor and control a technical process via sensors and actuators. The proposed enhanced control device can adapt to a changing threat landscape by adapting and limiting its functionality depending on the current threat landscape. If attacks have been detected, or if relevant vulnerabilities have been identified, the functionality of the device is increasingly limited towards essential functions. This graceful degradation under attack reduces the attack surface in risky situations, while maintaining essential functions of the device. This allows the cyber physical system, in which the control device is deployed, to stay operational even during attack.

Figure 4 shows the concept of a control device that is designed for graceful degradation under attack. The main functionality of the device is realized on its processing system by multiple SoftWare Components (SWC) that are executed by an Operating System (OS) and/or an app RunTime Environment (RTE). Software components may, e.g., implement the control function and diagnostic functions. The components interact with the physical world via sensors and actuators that are connected via an Input/Output (I/O) interface. The processing system uses a Secure Element (SE) for secure key storage and cryptographic operations, a Random Access Memory (RAM), a flash memory, and a Communication Module (ComMod).

An attack detection and criticality evaluation module monitors the operation of these device components to detect unexpected device behavior, here by matching the detected monitoring events with an attack pattern database. It would also be possible to check the device monitoring data against reference states providing the expected behavior. Such a check could be done against static reference data, but could also be done in conjunction with a digital twin, providing a simulation of the ongoing process. If a suspicious device behavior is detected, a criticality is determined, and depending on that, the functionality of the device is adapted by the Graceful device functionality Degradation Manager (GDM). For example, a SWC implementing a simplified control function with reduced functionality can be activated instead of the regular control function, reducing the threat exposure.

This example shows a self-contained realization in which the attack detection and graceful degradation functionality is realized as part of the device. A distributed implementation involving also device-external components would be possible as well, but would require tight protection of all external

interfaces to ensure a reliable operation even during ongoing attacks.

In industrial automation, the control functionality is usually not fixed, but is commissioned by the automation system operator, a machine builder, or an integrator. For this application domain, the need is therefore foreseen to allow also commissioning of the graceful degradation functionality of a control devices, allowing to define the device resilience behavior under attack. This specifically relates to the definition of essential functions, depending on the application use case.

VI. RESILIENCE ENGINE

An isolated execution environment, a resilience engine, is needed to ensure that resilience functionality is executed in a trustworthy way even if the main functionality of the control device is manipulated.

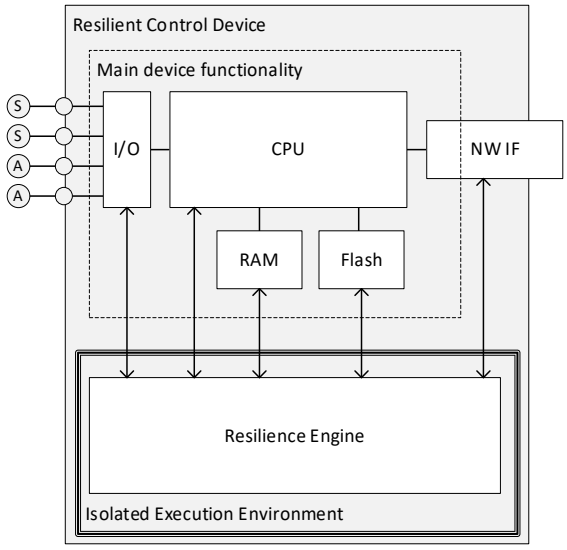

Figure 5. Control Device with Resilience Engine

Figure 5 shows a resilient control device that includes a resilience engine for the resilience functionality. The resilience engine can monitor and restrict the control device operation, in particular the processing unit (CPU), the IO operations, and the network communications. The resilience engine is isolated from the regular control function of the control device to ensure that is in a trustworthy state even if the main device functionality has been attacked successfully. Various realization options can be followed:

- Separate security chip or crypto controller with tamper protection.
- Integrated circuit (system on chip) with separate security core. The security core may implement specific tamper protection measures.
- Isolation on a regular processing core using hardware-support, e.g., by a trusted execution environment (TEE).
- Isolation using a software-based hypervisor executed below the operating system on the main processor.
- Isolation using operating systems means.

These approaches differ concerning the robustness of isolation, but also concerning their implementation overhead. It is a design decision, based on threat and risk analysis, to balance implementation robustness with implementation effort. Besides isolation, the resilience engine has to be protected by cybersecurity measures, e.g., secure firmware update and remote integrity attestation. Dedicated cryptographic keys for protecting the resilience engine can be used, to ensure that the cryptographic protection measures of the resilience engine are independent of the protection measures of the main device functionality.

VII. USAGE EXAMPLE

This section describes the usage in an exemplary way, distinguishing software components of varying criticality from the perspective of maintaining the CPS operation under attack.

Figure 6 shows example software components that are grouped according to the operational criticality. The graceful degradation manager activates the software components of the respective functionality group depending on the current attack scenario. In this example, three sets of software components are defined, defining the software components that are active in full, reduced, and in minimum functionality mode.

To ensure cyber resilience, the functionality is reduced to a limited control functionality that can be less optimized and lead to reduced CPS performance, and to keep limited remote access. In more critical attack scenarios, a fail-safe operation mode is activated, i.e., if even the reduced functionality operation cannot be ensured reliably.

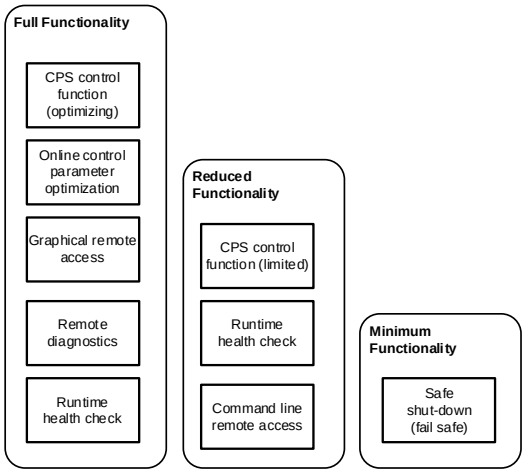

Figure 6. Software components with different operational criticality.

As an example from an industrial application use case, a protection device of a substation of an energy automation system may be considered as control device. Protection devices are applied within electric power systems to detect abnormal and intolerable electrical conditions and to initiate appropriate corrective actions, e.g., to interrupt a power line. The software executed on the protection device that implements the control functionality could be attacked via the network interface. In the extreme case, the network interface may be switched off for a limited time by the GDM, keeping

the protection functionality based on local sensor readings and connected actuators. That way, the protection device will not communicate its measurements to other substation devices in the substation anymore, but it would retain the local protection functionality and thus the safety of the connected power line.

VIII. EVALUATION

This section gives a preliminary evaluation of the presented concept from different perspectives.

CPS availability perspective: Availability and the flexibility to adapt to changing production requirements are important requirements for OT operators [6]. The proposed approach allows to maintain CPS operation in a limited way even under ongoing attacks or in specific failure situations. A reliable CPS operation can be maintained, avoiding the need to shutdown the CPS operation completely. This is considered to be the main advantage of enhanced control device resiliency with graceful degradation under attack, as the availability of the CPS is improved.

CPS operational performance perspective: The limited function mode may lead to a reduced productivity and less efficiency of the CPS. The exact impact depends on the limitations of the limited control operation functionality.

CPS management perspective: The operator of the CPS has to be aware about the resilience functionality supported by the CPS control devices. The CPS operator has to be made aware if some control devices have activated a restricted resilience operation mode, so that the overall CPS operation and the production planning can be adapted accordingly. The CPS' operation concept has to be defined accordingly to address restricted resilience operation modes, and the operating personnel has to be trained for the resilience functionality.

Implementation perspective: Control devices have to implement the functionality for attack detection and resilience management / graceful degradation in a highly protected execution environment that can be relied upon even if the main processing system of the control device should be attacked. The overhead depends on the specific technical implementation approach, e.g., requiring an additional protected hardware component, e.g., a secure microcontroller or a secured Field Programmable Logic Controller (FPGA). Both development effort and hardware costs are increased, which would have an impact in particular for cost-optimized control devices. Also, SCADA and MES systems have likely to be extended to allow operational personnel and production processes to be adapted if a control device activates a restricted resilience mode.

Engineering perspective: The graceful degradation functionality (attack criticality determination, as well as the definition of use case specific essential functions) has to be planned and defined so that it can be commissioned on the control device, leading to additional commissioning effort. It may be required that the same functionality has to be realized in different versions, e.g., in fully flexible, optimized operation mode and a limited operation mode. These modes have to be tested and validated, e.g., using simulations. Blueprints that give practice-proven engineering examples can limit the required additional engineering effort.

Testing perspective: The graceful degradation functionality has to be tested carefully to ensure that relevant attack scenarios are reliably detected, and also to validate that the limited control operation mode is reliably activated and performs reliably even under the detected attack scenarios. Testing has to be performed both on device-level for a single control device, as well as on system level for a CPS that uses multiple control devices, where some may be enhanced with graceful degradation under attack. As testing attack scenarios in real-world operational systems is often not possible, simulation tools are essential that allow simulating the CPS operation realistically under various attack scenarios when the engineered graceful degradation functionality is in place. Testing can be performed not only during the planning and engineering phase, but also during regular CPS operation to test the impact of recent attacks. Simulation may be useful also for training operational personnel.

Overall, implementing, engineering, and testing graceful degradation under attack implies additional effort that has to be justified by the increased availability of the CPS. The benefit depends on the attacks observed in real-world operations. Simulation tools (like digital twins) can be used also for this purpose to determine key performance indicators of the real-world CPS for which resilience under attack is protected with control devices implementing the engineered graceful degradation functionality and comparing it with a simulated CPS using control devices *not* implementing the engineered graceful degradation functionality.

IX. CONCLUSION AND FUTURE WORK

The proposed concept for cyber resilient control devices can enhance CPS availability even under ongoing attack scenarios. However, it comes with relevant additional effort for implementation, engineering, testing, training, and with overhead for the trusted execution environment required for resilience functionality that requires besides hardware support also specific security-focused implementation effort. However, cyber resilience requirements and technologies are increasingly defined in cybersecurity standards and regulations, and are adopted in real-world solutions, e.g., for server systems in data centers [13]. The specific robustness properties and the implementation effort of different technical approaches to implement a resilience engine on embedded control devices have still to be investigated.

The additional effort needed for implementing cyber resilience for control devices has to be justified by the positive impact on CPS operation, allowing to maintain a reliable CPS operation during ongoing attacks. The CPS operation may relate to a business model focusing on providing a continuous service like energy provisioning or may focus on the preservation of a safety function, like the availability of a protection system. Simulation tools for CPS and their control devices allow investigating cyber resilience for CPS in both the planning and operation phases, reducing in particular the testing effort, and allowing to analyze the effectiveness for different types of attack. A further direction addresses robustness under attack that tries to keep the CPS operational under attack with minimal or even no reduction of the systems operational performance, i.e., to withstand attacks.

REFERENCES

[1] R. Falk, C. P. Feist, and S. Fries, "Graceful Degradation under Attack: Adapting Control Device Operation Depending on the Current Threat Exposure", International Conference on Cyber-Technologies and Cyber-Systems, CYBER2024, September 29, 2024 to October 3, 2024, Venice, Italy, pp. 9-12, 2024. [Online]. Available from: https://www.thinkmind.org/library/CYBER/CYBER_2024/cyber_2024_1_20_80023.html 2025.05.05

[2] Platform Industrie 4.0, "Resilience in the Context of Industrie 4.0", Whitepaper, April 2022. [Online]. Available from: https://www.plattform-i40.de/IP/Redaktion/EN/Downloads/Publikation/Resilience.html 2025.05.05

[3] R. Falk and S. Fries, "Enhanced Attack Resilience within Cyber Physical Systems", Journal on Advances in Security, vol 16, no 1&2, pp. 1-11, 2023. [Online]. Available from: https://www.iariajournals.org/security/sec_v16_n12_2023_paged.pdf 2025.05.05

[4] R. Falk and S. Fries, "System Integrity Monitoring for Industrial Cyber Physical Systems", Journal on Advances in Security, vol 11, no 1&2, July 2018, pp. 170-179. [Online]. Available from: www.iariajournals.org/security/sec_v11_n12_2018_paged.pdf 2025.05.05

[5] IEC 62443, "Industrial Automation and Control System Security" (formerly ISA99). [Online]. Available from: http://isa99.isa.org/Documents/Forms/AllItems.aspx 2025.05.05

[6] "Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act), Document 32024R2847, November 2024. [Online]. Available from: http://data.europa.eu/eli/reg/2024/2847/oj 2025.05.05

[7] "Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC Text with EEA relevance", 10/2023. [Online]. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0053 2025.05.05

[8] A. Regenscheid, "Platform Firmware Resiliency Guidelines", NIST SP 800-193, May, 2018. [Online]. Available from: https://csrc.nist.gov/publications/detail/sp/800-193/final 2025.05.05

[9] TCG, "Cyber Resilient Module and Building Block Requirements", V1.0, October 19, 2021. [Online]. Available from: https://trustedcomputinggroup.org/wp-content/uploads/TCG_CyRes_CRMBBReqs_v1_r08_13jan2021.pdf 2025.05.05

[10] P. England et al., "Cyber resilient platforms", Microsoft Technical Report MSR-TR-2017-40, September, 2017. [Online]. Available from: https://www.microsoft.com/en-us/research/publication/cyber-resilient-platforms-overview/ 2025.05.05

[11] NIST CSF, "The NIST Cybersecurity Framework (CSF) 2.0", February, 2024. [Online]. Available from: https://doi.org/10.6028/NIST.CSWP.29 2025.05.05

[12] EN 303 645, "Cyber Security for Consumer Internet of Things: Baseline Requirements", ETSI, V3.1.3 (2024-09), September, 2024. [Online]. Available from: https://www.etsi.org/deliver/etsi_en/303600_303699/303645/03.01.03_60/en_303645v030103p.pdf 2025.05.05

[13] Intel Data Center Block with Firmware Resilience, Solution Brief. [Online]. Available from: https://www.intel.com/content/dam/www/public/us/en/documents/solution-briefs/firmware-resilience-blocks-solution-brief.pdf 2025.05.05

[14] D. Bodeau and R. Graubart, "Cyber resiliency design principles", MITRE Technical Report, January 2017, [Online]. Available from: https://www.mitre.org/sites/default/files/publications/PR%2017-0103%20Cyber%20Resiliency%20Design%20Principles%20MTR17001.pdf 2025.05.05