DOI 10.5162/iCCC2024/P10

Enhancing Cyber-Resilience in Cyber-Physical Systems of Systems: A Methodical Approach

Elisabeth Vogel[1], *Peter Langendörfer*[1,2]
[1] *Leibniz Institute for High Performance Microelectronics (IHP), 15236 Frankfurt (Oder), Germany*
[2] *Chair of Wireless Systems, BTU Cottbus-Senftenberg, 03046 Cottbus, Germany*
vogel@ihp-microelectronics.com

Summary:
This paper delves into the omnipresence of cyber-physical systems of systems (CPSoS) across diverse sectors, highlighting their critical role from Industry 4.0 to smart homes. Addressing the varied requirements and challenges faced by CPSoS, we propose a modified Cyber-Resilience Life-Cycle, offering a practical framework for sustainable disturbance mitigation. Our approach enhances the adaptability of CPSoS, ensuring resilience in the face of evolving complexities and potential disruptions. The paper concludes with insights into the modified life cycle's applications, emphasizing its role in fostering cyber resilience in active systems.

Keywords: Cyber-Physical Systems of Systems, Condition monitoring, Cyber-Resilience, IT-Security, Maintenance

1. Introduction

Cyber-physical systems of systems (CPSoS) can be found in almost all areas of human life, dominating the public sector, including Industry 4.0, autonomous driving, smart grids & energy, agriculture, aerospace, and telecommunications. CPSoS are also increasingly penetrating many private sectors, such as smart homes, smart wearables, intelligent household appliances, personal assistants, and smart speakers.

The requirements and challenges faced by CPSoS in various sectors are highly differentiated and necessitate a closer examination. These requirements include, for example, reliability, availability, security, interoperability, real-time capability, flexibility, and scalability. It should be noted that different requirements have different meanings for CPSoS in different sectors. For example, failing to meet requirements has different global and local consequences for a nuclear power plant or a large hospital than it does for smart homes.

The extensive and continually expanding pool of requirements and challenges for CPSoS can be attributed to the ubiquitous presence of such systems. With the constant progress and further development of CPSoS, their complexity is continuously increasing.

The concept of cyber resilience offers a holistic solution for overcoming these growing challenges. This article presents the basic conditions that CPSoS must fulfill to meet the concept of cyber resilience. From these conditions, a model-based approach can be derived for managing the mitigation of disruptions and risk factors of CPSoS in a cyclical manner. In Section 2, we introduce the Cyber-Resilience Life-Cycle as described in [1]. This involves a closer examination of the definition and characteristics of Cyber-Resilience. Section 3 presents our modified Cyber-Resilience Life-Cycle, providing detailed insights into the changes we implemented and the rationale behind them, emphasizing their significance in achieving a more practical and realistic representation.

This paper concludes with a summary outlining the potential applications of the modified Cyber-Resilience Life Cycle.

2. Background

CPSoS are susceptible to various risk factors, encompassing both internal factors (e.g., software or hardware errors) and external factors (e.g., human error or cyber attacks) affecting the physical system under consideration. As the complexity of a CPSoS increases, the diversity of associated risk factors also rises. The immediately observable effects of an occurred risk factor are disturbances.

Disturbances can be either visible or not directly visible. Examples of visible faults include (partial) hardware failures. Visible disruptions, therefore, involve all risk factors leading to the loss of

functionality (e.g., hardware failure). On the other hand, non-visible faults denote the compromise of the integrity of a CPSoS. This mainly encompasses cyber attacks that corrupt a system or aim to steal data.

For a cyber-resilient CPSoS, the capability to recognize and comprehend both types of disruptions, respond to them, and adapt accordingly is crucial. In accordance with these requirements, we have defined resilience in [1] as follows:

"A CPS (oS) is resilient if it has the ability to react to specified and unspecified disturbances in a way that preserves its function and reacts quickly. This reaction includes the early detection, minimization, prediction or even avoidance of disturbances. In addition, it needs to have the capability to anticipate future challenges and to prepare itself for those."

In line with that definition of the concept of cyber resilience, the core idea is not to prevent disruptions. The goal is to respond to disruptions in a way that, at best, preserves the function and integrity of the system. Disruptions to highly complex CPSoS cannot be prevented due to their enormous complexity, but their negative impact on the CPSoS should be minimized through appropriate preventive measures.

The definition of cyber resilience describes a set of characteristics or capabilities [1] that a CPSoS must possess to be considered (cyber) resilient. These characteristics, known as key actions [1, 3], are described in Tab. 1.

Tab. 1: Enumeration and description of the key actions.

Key action	Description
Anticipation	The ability to predict future events based on known information.
Error analysis	The ability to detect and comprehend disturbances.
Recovery	The ability to restore functionality after an incident within acceptable parameters.
Adaptation	The ability to implement available countermeasures to the extent that future responses to a disturbance can be functionally sustained.
Permanent resilience	Permanently active countermeasure for already known disturbances.
New (learned) Resilience	Non-permanently active countermeasures that can be activated based on the situation.

The key actions described in Tab. 1 are time-dependent and form an action cycle that provides a CPSoS with instructions on how to deal with the effects of a disruption. A mandatory prerequisite for this is that a CPSoS has recognized a malfunction. Fig. 1 illustrates this cycle of action, specifically referred to as the Cyber Resilience Life Cycle [1, 2].

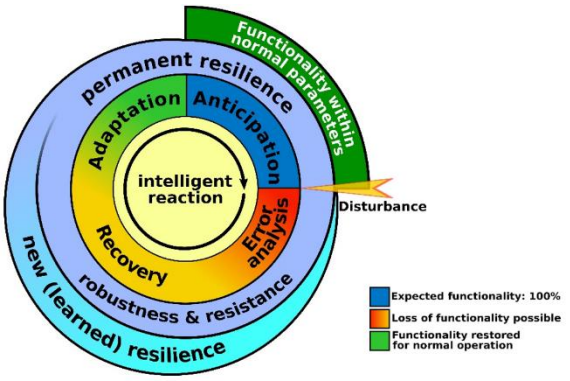

Fig. 1: Cyber-Resilience Life-Cycle [1, 2]

The Cyber-Resilience Life-Cycle shown in Fig. 1 depicts the key actions described in Tab. 1 in an interdependent cycle. In the broadest sense, these key actions can also be described as system states, as the various key actions provoke correspondingly different system behavior: By default, a CPSoS is in the Anticipate system state. In this state, the functionality and integrity corresponding to the specifications for the system are guaranteed. The system has the ability to predict any malfunctions that may occur in the future through various measures and the possibilities of self-observation and analysis, thus taking appropriate precautions to maintain functionality and integrity.

If a fault occurs that is either unknown to the system or for which no suitable course of action has yet been defined, the CPSoS enters the Error Analysis system state for this fault. Entry into this state requires the fault to be recognized. In the Error Analysis system state, the fault is analyzed, its negative effects on the system are evaluated, and the countermeasures available to the system are checked. In short, the fault and its negative effects on the CPSoS are understood.

In the Recovery system state, any lost system functionality is restored. When transitioning to the Adaptation system state, the modified countermeasures are integrated into the existing countermeasures:

robustness & resistance + new (learned) resilience → permanent resilience

to make the CPSoS more robust in the future against the disruption considered in this action cycle. In the future, the CPSoS will be able to anticipate the disruption being dealt with and minimize any loss of functionality that may occur. The more frequently this disruption occurs, the more efficiently this adaptation will take place.

3. Modified Cyber-Resilience Life-Cycle

In our comprehensive examination of cyber resilience in CPSoS, we advocate for a substantial revision of the cyber resilience life cycle outlined in Section 2. To commence this refinement, attention must be directed to the key actions outlined in Tab. 1.

While certain actions, such as anticipation, error analysis, recovery, and adaptation, remain untouched, there is an adjustment for the actions robustness & resistance and new (learned) resilience. These key actions will be combined into the new key action called "Resistance."

Another pivotal aspect of this evolution involves a reassessment of the chronological order of key actions. Drawing inspiration from the approach in [1], we posit that a CPSoS initially exists in a state allowing foresight into potential future faults. Upon fault recognition, the CPSoS transitions seamlessly into error analysis, retaining the essence of the prior Cyber-Resilience Life-Cycle (see Fig. 1). However, the stride in the revised model lies in the CPSoS initiating crucial modifications to active countermeasures before embarking on the restoration of functionality and/or integrity. This strategic shift is imperative to address potential damage at both hardware and software levels.

Efforts to ameliorate the damages must be undertaken comprehensively. In scenarios involving redundant system components, a viable recourse involves transitioning to unaffected components. However, when confronted with considerable damage surpassing the restorative capacities of the CPSoS, human intervention becomes imperative. It is paramount, particularly within the framework of a cyber-resilient system, to minimize reliance on human involvement. Consequently, the strategic integration of appropriate redundancies and the thoughtful coupling or segregation of system components emerges as a critical consideration from the nascent stages of the design phase.

The visual representation of this modifications is shown in Fig. 2, signaling a significant evolution in the Cyber-Resilience Life-Cycle.

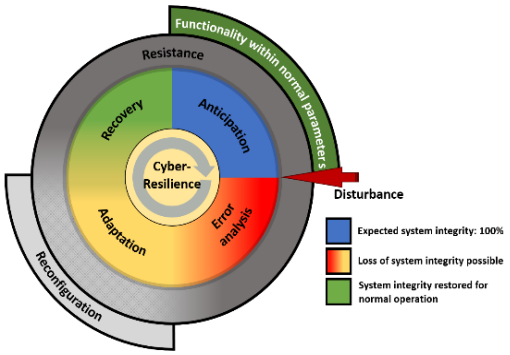

Fig. 2: Modified Cyber-Resilience Life-Cycle

In our view, the modification of the cyber-resilience life cycle described here is a necessary further development of the variants from [1, 3].

The cycle of key actions described in [3] addresses the transition from risk management to disaster resilience and relates to the management of water resource infrastructure in the United States. Factors such as changes in climate patterns, increased environmental concerns, higher population densities in coastal areas, associated infrastructure, limited budget, and aging infrastructure were considered as risk factors.

[3] points out that as a dominant assessment strategy for engineering systems, risk management aims to provide solutions to known hazards in anticipation of continued normal operations. When uncertainties arise in engineering systems, risk management assumes that they can be quantified and mitigated [4]. However, the more complex a system becomes, the more influential factors such as feedback loops, interactions, (future) unknowns, and variable spatial or temporal scales for hazards become. Many of these factors are also unpredictable [3].

For this reason, [3] proposed a solution for the transition from risk management to a resilience approach as an alternative, since resilience pursues the handling and processing of the unknown and unpredictable as a guiding principle.

For the design of the Cyber-Resilience Life-Cycle [1], we have adopted the approach from [3] and initially adapted it for cyber-physical systems (see Fig. 1). Similar to the transition from risk management to disaster resilience, we believe that a shift from conventional fault tolerance to a resilience approach is necessary.

The increasing complexity of cyber-physical systems is another factor that needs to be taken into account. Conventional techniques from fault tolerance [5] may no longer be sufficient. The risk factors described in [3] are very wide-ranging and come from the most diverse areas. A

CPSoS is exposed to a similar range of risk factors.

With an increasing understanding of resilience approaches in CPSoS, we have now modified our Cyber-Resilience Life-Cycle from [1] in accordance with Fig. 2. The Cyber-Resilience Life-Cycle has been reorganized by swapping the recovery and adaptation phases.

From our perspective, in the context of CPSoS, it is imperative that a system must modify the countermeasures in accordance with the error analysis, after the error analysis has been performed and before the functionality or integrity can be restored. This prevents the CPSoS from being in a weakened state during recovery, making it more vulnerable to faults. With the modification of the Cyber-Resilience Life-Cycle from [1], the CPSoS can make all necessary adjustments and utilize improvements to restore functionality and integrity without an increased risk of a renewed failure.

4. Conclusion

The modified Cyber-Resilience Life-Cycle, elucidated in Section 3, stands as a methodological cornerstone facilitating both the conception and maintenance of CPSoS. This approach not only permits the early-stage evaluation of cyber-resilience during the developmental phase of a CPSoS but also opens avenues for simulated scenarios. These scenarios serve the purpose of scrutinizing the CPSoS' s response mechanisms under diverse conditions, affirming its capacity to react while preserving functionality.

Beyond the developmental phase, the application of this methodological approach finds resonance in the operational landscape of CPSoS. Contemplating instances such as planned maintenance cycles or the introduction of new components, simulations become instrumental. Conducting simulations in these scenarios allows for a meticulous assessment of their impact on the CPSoS. Consequently, it becomes feasible to proactively gauge and enhance cyber-resilience, ensuring preparedness for evolving conditions or potential disruptions.

In essence, the modified Cyber-Resilience Life-Cycle emerges not only as a comprehensive framework for resilient CPSoS design but also as a robust instrument for the in-depth evaluation of resilience characteristics within active systems. This strategic utilization empowers stakeholders to fortify CPSoS against potential vulnerabilities and reinforces their adaptive capacity in the face of dynamic challenges.

References

[1] E. Vogel, Z. Dyka, D. Klann, and P. Langendörfer, “Resilience in the Cyberworld: Definitions, Features and Models,” *Future Internet*, vol. 13, no. 11, 2021, doi: 10.3390/fi13110293.

[2] Z. Dyka, E. Vogel, I. Kabin, D. Klann, O. Shamilyan, and P. Langendörfer, “No Resilience without Security,” in *2020 9th Mediterranean Conference on Embedded Computing (MECO)*, 2020, pp. 1–5.

[3] J. D. Rosati, K. F. Touzinsky, and W. J. Lillycrop, “Quantifying coastal system resilience for the US Army Corps of Engineers,” *Environ Syst Decis*, vol. 35, no. 2, pp. 196–208, 2015, doi: 10.1007/s10669-015-9548-3.

[4] J. Park, T. P. Seager, P. S. C. Rao, M. Convertino, and I. Linkov, “Integrating risk and resilience approaches to catastrophe management in engineering systems,” *Risk analysis : an official publication of the Society for Risk Analysis*, vol. 33, no. 3, pp. 356–367, 2013, doi: 10.1111/j.1539-6924.2012.01885.x.

[5] S. Bharany *et al.,* “Energy efficient fault tolerance techniques in green cloud computing: A systematic survey and taxonomy,” *Sustainable Energy Technologies and Assessments*, vol. 53, p. 102613, 2022, doi: 10.1016/j.seta.2022.102613.