Towards Increasing Safety in Collaborative CPS Environments

Marco Stadler[1] , Michael Riegler[1,2] , and Johannes Sametinger[1,2]

[1] LIT Secure and Correct Systems Lab
[2] Institute of Business Informatics – Software Engineering
Johannes Kepler University, Linz, Austria
{firstname.lastname}@jku.at
https://www.jku.at/en/lit-secure-and-correct-systems-lab
https://www.se.jku.at

Abstract. Cyber-Physical Systems (CPS) frequently operate in collaborative environments with other CPS and humans. This collaborative environment has the potential for situations in which CPS endanger humans. We argue that safety in such environments can be increased if the environment is aware of the safety-critical situation and can respond appropriately. In this paper, we describe our preliminary work on a collaborative CPS safety framework that combines distinct modes of operation with adaptive monitoring.

Keywords: Collaborative CPS · Adaptive Monitoring · Modes.

1 Introduction

Cyber-Physical Systems (CPS) frequently operate in safety-critical environments and domains due to their close interaction with humans [4]. While recent efforts in securing the collaboration seem promising [11], safety incidents jeopardizing human well-being still occur. Reasons for these safety incidents range from security breaches [7] to malfunctioning systems due to system design flaws and sensor failures [6].

Alongside other countermeasures, the concept of *Modes* has been introduced to address this issue. modes provide a set of functionalities to ensure a particular system behavior. We can switch modes based on certain circumstances. The trigger for switching between the modes depends on the context. From a functional standpoint, self-driving vehicles [3] use different modes to operate autonomously or manually. These triggers can also be based on safety risks; for instance, in the area of robotics, a manufacturing robot can switch between modes and adjust its movement speed based on the proximity of a human to avoid the risk of collision [14].

The detection of safety risks is not trivial. *Monitoring* certain properties of the CPS itself or the environment surrounding the CPS to detect potential safety risks as they occur is a crucial technique to accomplish this objective [9]. This

2   M. Stadler et al.

is, for instance, the distance value measured by a LiDAR unit or a temperature measurement that prevents overheating in the preceding robotic example.

Furthermore, multiple CPS often operate as part of a *collaborative CPS*, to complete a specific mission, making the process of ensuring safety even more complex [1]. Recent efforts, therefore, have expanded this mode concept by facilitating the sharing of mode-related data between multiple CPS [13].

Most of the related approaches consider modes either for single systems [14], target only certain aspects like multi-mode real-time monitoring [10], or focus on formal frameworks for the design of safety monitors for multi-functional robotic systems with modes [5]. However, none of these approaches completely consider the combination of mode switches and adaptive monitoring for enhancing safety in a collaborative CPS environment.

The concept has thus far been employed in both security and safety contexts. In this paper, we present our initial efforts to increase safety in a collaborative CPS environment by combining the sharing of mode-related data with adaptive monitoring, thereby concentrating on the safety aspect of modes.

In detail, we claim the following contributions: (*i*) We present a list of challenges (*c.f.* Section 3) associated with environmental safety risks caused by multiple CPS collaborating with humans and (*ii*) derive an initial framework architecture (*c.f.* Section 4) utilizing mode switching and adaptive monitoring for mitigating these risks. In addition, we (*iii*) provide a *Proof of Concept* (PoC) of the framework (*c.f.* Section 5) to demonstrate the viability of our approach.

2   Motivation

CPS and robotic systems frequently operate in hazardous environments. For instance, accidents involving jamming, cutting, and crushing continue to occur frequently in industrial settings where collaborative work between multiple CPS and humans is prevalent, making these environments hazardous. Studies [8] indicate that the majority of incidents occurred during non-routine work, such as inspections, cleanings, or repairs, i.e., when systems are not operating in their typical mode(s) of operation. Therefore, systems undergoing non-routine modes of operations, such as *Maintenance Mode*, represent a safety-sensitive time frame and can be considered *safety-critical modes*. Due to its complexity, uncertainty, and variability, the environment of a CPS poses unique safety risks [1]. These risks are exacerbated when the collaborative CPS are operating additionally in a safety-critical mode. Fatal incidents are caused by the environment of collaborative CPS operating in a safety-critical mode. During an incident on a manufacturing floor [2], for instance, a human conducting maintenance tasks was killed by a robotic CPS from the environment that entered the maintenance zone by mistake. However, the incident could have been avoided if the environment had responded appropriately to the ongoing maintenance by switching the CPS in the environment into respective restrictive modes (e.g., completely disabled certain unsafe movements) and intensifying movement monitoring around the maintenance zone to detect collisions/malfunctions early on (i.e., employed adaptive

monitoring). Therefore, we contend that the safety of such a collaborative CPS environment can be enhanced by leveraging appropriate mode switching and adaptive monitoring.

3   Challenges

Given a scenario in which multiple robotic manipulators are working in close proximity, one enters a *Maintenance Mode* as a worker proceeds to perform certain tasks on/near one of the manipulators. This condition comes along with a series of risks. The safety zones of the *System under Maintenance* (SuM) itself are violated, making a human operate within the operating zone of the robot and therefore susceptible to collisions. Monitoring properties that adhere to the detection of a potential collision has the utmost priority at this time. Therefore, the framework must be able to **adapt monitoring of the SuM alongside the mode switch (C1)** to ensure the prompt detection of potential collisions. Humans often disregard safety rules and systems malfunction. As a result, they may operate outside the safe range, endangering other systems (in this case, other manipulators or passing autonomous vehicles) or even themselves. The **environment must therefore transition to precautionary modes (C2)** that disable unsafe CPS behavior. The environment and the CPS themselves evolve (e.g., the manipulators receive new sensors, a new CPS is added to the factory floor, or a CPS is capable of driving into the safety-critical zone). Therefore, the framework must be **capable of adjusting to changes and co-evolve with the monitored systems (C3)**. The detection of environment-wide patterns is essential for environmental safety. Consequently, **data on changes in modes and monitoring of a CPS must be aggregated (C4)** to derive additional insights on the monitored environment, as certain patterns can only be detected at a higher level of abstraction (e.g., a system-wide failure due to power outages). Since safety incidents continue to occur, it is essential to **preserve data for post-mortem examination (C5)**. Based on the persisted data, incident scenarios must be revisited to derive alterations to the mode switching logic configuration and adaptive monitoring.

4   Framework Architecture

To address the aforementioned challenges, we present our preliminary work on a framework capable of adaptively monitoring CPS and switching modes in a collaborative CPS environment. An overview of the framework can be found in Fig. 1. The framework architecture was conceived based on the identified challenges (**C1**–**C5**). The correspondence between a specific challenge and a framework component is indicated with the blue ellipses.

The framework consists of five main components: `Environment`, `Registry`, `Communication Broker`, `Adaption Controller`, and `Services`. The `Environment` consists of all the CPS that might influence each other's safety. The `Communication Broker` is intended to use a topic-based protocol providing a standardized interface capable of handling diverse systems. The topic-based architecture enables

CPS to dynamically (un-) subscribe to changes in the `Environment`, therefore enabling a co-evolving framework (*c.f.* **C3**). The topics are assigned by a `Registry` that keeps track of where CPS are (physically) located (*c.f.* `Zone Registry`) and which CPS poses certain features (*c.f.* `CPS Registry`) that might influence the safety of an environment (e.g., a property indicating that a vehicle is capable of moving freely in the factory floor). Once a CPS enters a safety-critical mode (*c.f.* `CPS#2`) the information regarding the mode switch and metadata corresponding to the switch are published via the `Communication Broker`. Based on the previously assigned topics, the respective CPS in the environment are notified via topic subscriptions (e.g., `CPS#1` and `CPS#3` are notified as they are nearby and `CPS#4` is notified as it might move into the safety-critical zone). CPS that are irrelevant (*c.f.* `CPS#5` and `CPS#6`) are neglected and operations continue as usual. The influential CPS in the environment and the CPS in the safety-critical mode then request an adaptation from the `Adaptation Controller`. Mode switches (*c.f.* **C2**) and a new monitoring configuration (*c.f.* **C1**) are provided by the `Mode Manager` and the `Monitoring Manager`. This information is consolidated by the `Core` and forwarded back to the respective CPS that can adapt accordingly. In parallel to this process, data collected by the `Environment` is aggregated at the `Aggregator` and the insights are fed into the `Adaptation Controller` to react accordingly (*c.f.* **C4**). Finally, all the gathered data concerning the mode switches and the CPS sensor data is persisted at the `Persistor` (*c.f.* **C5**).
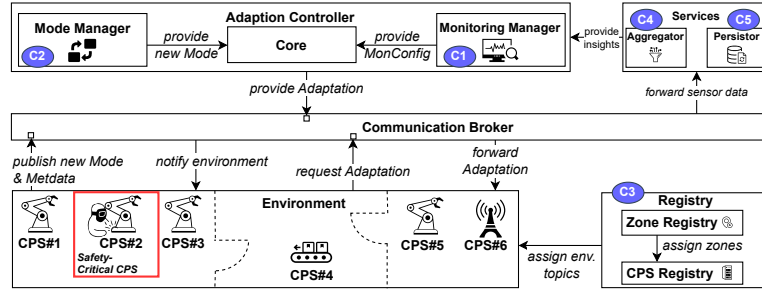

Fig. 1. High-level overview of the architecture

5   Proof of Concept

To demonstrate the viability of the approach, we incorporated the proposed framework into a prototype PoC containing the core functionalities (i.e., the outlined core components, communication flows, mode switching logic, and adaptive monitoring). We used CPS employing the Robot Operating System (ROS) for the Python-based prototype and simulated a safety-critical mode transition in one of the CPS using TurtleBots [12] in a test scenario. The CPS in the environment then switched modes and adapted their monitoring behavior to reduce the time required to detect collisions in safety-critical zones. The source code is incorporated within a ready-to-use ROS package and available on GitHub[3].

---

[3] `https://github.com/jku-lit-scsl/mode-mon`

6 Conclusion

In this paper, we describe our initial efforts to increase safety in a collaborative CPS environment by employing mode switching and adaptive monitoring. We develop a general framework based on the challenges of such a safety-critical environment. A PoC is utilized to validate the viability of the proposed approach. Future efforts concentrate on the complete implementation of the framework and a case-study evaluation.

References

1. Ali, N., Hussain, M., Hong, J.E.: Analyzing safety of collaborative cyber-physical systems considering variability. IEEE Access **8**, 162701–162713 (2020)
2. Baldas, T.: Lawsuit: Defective robot killed factory worker; human error to blame (2017), `https://eu.freep.com/story/news/local/michigan/2017/03/14/lawsuit-defective-robot-killed-factory-worker-human-error-blame/99173888/`, Accessed May 3, 2023.
3. Chen, T., Phan, L.T.X.: SafeMC: A system for the design and evaluation of mode-change protocols. Proc. of the IEEE Real-Time and Embedded Technology and Applications Symposium, RTAS pp. 105–116 (2018)
4. Dibaji, S.M., Pirani, M., Flamholz, D.B., Annaswamy, A.M., Johansson, K.H., Chakrabortty, A.: A systems and control perspective of CPS security. Annual Reviews in Control **47**, 394–411 (2019)
5. Guiochet, J., Powell, D., Baudin, É., Blanquart, J.P.: Online Safety Monitoring Using Safety Modes. In: Workshop on Technical Challenges for Dependable Robots in Human Environments. pp. 1–13 (2008)
6. Herkert, J., Borenstein, J., Miller, K.: The Boeing 737 MAX: Lessons for Engineering Ethics. Science and Engineering Ethics **26**(6), 2957–2974 (2020)
7. Inayat, I., Farooq, M., Inayat, Z., Abbas, M.: Security-Based Safety Hazard Analysis Using FMEA: A DAM Case Study. Communications in Computer and Information Science **1479 CCIS**, 18–30 (2021)
8. Kim, S., Lee, J., Kang, C.: Analysis of industrial accidents causing through jamming or crushing accidental deaths in the manufacturing industry in South Korea: Focus on non-routine work on machinery. Safety Science **133** (2021)
9. Lyu, X., Ding, Y., Yang, S.H.: Safety and security risk assessment in cyberphysical systems. IET Cyber-Physical Systems: Theory and Applications **4**(3), 221–232 (2019)
10. Neukirchner, M., Quinton, S., Ernst, R., Lampka, K.: Multi-mode monitoring for mixed-criticality real-time systems. 2013 Intl. Conf. on Hardware/Software Codesign and System Synthesis, CODES+ISSS 2013 (2013)
11. Nikolakis, N., Maratos, V., Makris, S.: A cyber physical system (CPS) approach for safe human-robot collaboration in a shared workplace. Robotics and Computer-Integrated Manufacturing **56**, 233–243 (2019)
12. Open Source Robotics Foundation, I.: TurtleBot (2023), `https://www.turtlebot.com/`, Accessed May 3, 2023.
13. Riegler, M., Sametinger, J., Vierhauser, M.: A Distributed MAPE-K Framework for Self-Protective IoT Devices. In: IEEE (ed.) Proc. of the 18th Symposium on Software Engineering for Adaptive and Self-Managing Systems. SEAMS '23 (2023)
14. Villani, V., Pini, F., Leali, F., Secchi, C.: Survey on human–robot collaboration in industrial settings: Safety, intuitive interfaces and applications. Mechatronics **55**, 248–266 (2018)