Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 180 (2021) 301–307

Procedia Computer Science

www.elsevier.com/locate/procedia

International Conference on Industry 4.0 and Smart Manufacturing

Multi-mode Systems for Resilient Security in Industry 4.0

Michael Riegler*, Johannes Sametinger

LIT Secure and Correct Systems Lab and Dept. of Business Informatics - Software Engineering
Johannes Kepler University Linz, Altenberger Straße 69, 4040 Linz, Austria

Abstract

In the era of the Internet of Things and Industry 4.0, machines and devices are increasingly getting connected. These connections go hand in hand with security vulnerabilities and potential threats to these devices. In regular IT systems, we typically provide updates to eliminate vulnerabilities. In industrial automation and control systems, especially in mass production, legacy systems are widespread and installing updates causes downtime. Availability is one of the top goals; stopping a machine in case of a cyber-security threat is often too expensive. But, system integrators and asset owners should not have to wait until product or component suppliers release appropriate updates. Due to safety and warranty requirements, developing and distributing updates can take a long time. In the meantime, attackers can pose threats by taking advantage of devices' known vulnerabilities. In this paper, we propose the design of resilient systems based on multi-modal architectures with several operational modes. When vulnerabilities of systems become known, or when systems get even attacked at some point, mode switching can overcome the time between vulnerability disclosure or attack, and the availability of corresponding security patches. Therefore, system integrators and asset owners can actively protect themselves by implicitly or explicitly switching to modes with reduced attack surfaces and, thus, with limited ranges of activity for attackers.

Keywords: Multi-mode systems; Mode switching; Resilience; Security; Industry 4.0; Zero-day vulnerabilities

1. Introduction

Through recent innovations in electronics and communication, industrial automation and control systems (IACSs) increase availability and efficiency. The reduction of down times, lead times, waste and as well costs have long been targets of the industry. Batch size one, Industry 4.0, digital twin, big data analytics and predictive maintenance are today's buzz words [23]. Information technology pervades the industry and creates more transparency, increases flex-

* Corresponding author. Tel.: +43-732-2468-9540.
E-mail address: michael.riegler@jku.at

1877-0509
10.1016/j.procs.2021.01.167

ibility and adaptability. The Internet of Things (IoT) and especially the Industrial Internet of Things (IIoT) connects physical devices like machines, robots and sensors over various protocols like OPC UA, MQTT and others. Remote monitoring allows support and control across several locations.

Increased connectivity has its price. In 2019, about 2 billion IoT devices were affected by zero-day vulnerabilities which allowed remote code execution and bypassing firewalls and network address translation [8]. According to the Allianz Risk Barometer [1], cyber incidents are the biggest threat to companies after business interruptions in 2020. In addition to the Covid-19 lockdown, cyberattacks have also led to production downtimes. For example, the German car parts company Gedia and the Belgian loom manufacturer Picanol had to send over 1,500 people home after cyberattacks [9, 24]. Moreover, attackers have used Covid-19 for scam and phishing emails to distribute malware and exploit the new teleworking infrastructure [25].

Security has to be considered over the entire life-cycle of an IACS. In this idea paper we propose the development of resilient systems with several operational *modes* to mitigate threats in the long term based on ideas in [17, 18]. If malware is detected or if vulnerabilities are known to exist, we want to provide protection mechanisms for endangered systems. These systems should automatically switch or manually be switched to a mode with a reduced attack surface.

In Section 2, we describe opportunities and challenges of Industry 4.0 and Smart Manufacturing from a security perspective. The importance of resilient security will be discussed in Section 3. In Section 4, we will first demonstrate the idea and the use of multi-mode systems from other (non-security) domains, then present mode switching in general, introduce our proposed multi-modal architecture, and provide some sample mode-switch scenarios. We discuss the findings in Section 5 and draw our conclusions in Section 6.

2. Industry 4.0 & Smart Manufacturing

According to Lasi et. al [11], the fourth industrial revolution will increase digitalization and networking of all manufacturing processes and transform industries from a product-oriented to service-orientated business. This is what we call Industry 4.0. It should provide high flexibility and individualization (batch size one) in product development and production and therefore decrease time to market. Smart Manufacturing is a fundamental concept and is defined by NIST [14] as ”fully-integrated, collaborative manufacturing systems that respond in real time to meet changing demands and conditions in the factory, in the supply network, and in customer needs”. Many sensors, actors and embedded systems need to be combined in one IACS that communicates with other systems and services and is either fully automated, semi-automated or operated manually.

IACSs have a typical life-cycle from 5 to 20 years. They need to work 24/7 and thereby master special security challenges. We have to consider many perspectives and issues: from organizational and regulatory challenges to resource constraints to non-technical aspects like security awareness. *Safety*, the protection of the environment, including staff, customers and assets, from the IACS and its components is always the most important goal. Manufacturers have to make sure that their systems do not harm people or damage anything. *Security* can be seen as the opposite of safety. It aims at protecting IACSs and their components from their environments, e.g., from attacks by hackers.

Safety is at stake when security is weak. For example, if attackers get access to an IACS, take over control of a robot and harm people or cause damage, a security issue also becomes a safety issue. Stopping an IACS in case of potential or real threats is seldom an option. Patches for critical vulnerabilities may not quickly be available. Before they can be installed, they must be tested extensively due to safety, certification and warranty requirements. This takes time. When an update or patch is eventually available, it should be installed as soon as possible, because hackers can use the information about the fixed vulnerabilities to write malware and attack unpatched systems.

3. Resilient Security

Threats refer to incidents with the potential to harm systems and are based on the exploit of vulnerabilities. They can be both intentional and unintentional. Vulnerabilities are mistakes in software or hardware that can be directly used by attackers to gain access to systems or networks [13]. The span is crucial between the time when a vulnerability becomes known to the public and the time when an update or patch to fix that vulnerability becomes available. As availability is one of the top goals of an IACS, stopping a machine is the worst-case scenario as it typically means losing money. Developing updates is needed, but that may take a comparably long time.

IACSs and their components need to be certified through quality assurance processes. Due to safety requirements, manufacturers have to get their formal approvals, e.g. European Machinery Directive [4]. System integrators and asset owners may have to wait until the product or component supplier releases updates. If the asset owner changes something in the hardware or software itself, the warranty may expire. If vulnerabilities are known to attackers, they can develop exploits to take advantage. The development of updates and their distribution has to be accelerated, especially to mitigate zero-day vulnerabilities. But this only helps in the short term. Threats and vulnerabilities must be addressed over the entire life-span of an IACS. A life-time of 20 years makes security by design and defense in depth challenging. Making predictions is quite difficult, especially about the future, as they say. State of the art authentication and cryptography methods, protocols and libraries may be out of date in a few years.

We have to consider the fact that product manufacturers and component suppliers may discontinue the support of devices. Some manufacturers may even go bankrupt. It is only a matter of time until connected systems get attacked. Even when IACSs are air-gapped, there can be attacks, like the computer worm Stuxnet spread via USB flash drives and caused wide-spread damage [5, 10].

Systems are considered to be resilient if they do their work despite adverse circumstances and if they recover rapidly from any harm [6]. No matter how well systems have been designed, unknown or unresolved vulnerabilities can become a risk in the future. Resilient systems protect their important assets by using methods to resist and detect adversities, to mitigate them and to recover. Due to location and time this is often done autonomously [7]. For resilient security of IACSs, exposure and authentication measures may be adapted depending on the security context by switching modes [21]. Reduced exposure can be a first step, e.g., to reduce the data transfer rate or to block communication temporarily. In addition, modes are not only useful from a security perspective. If there are external or internal disturbances, problems with a component, a restricted mode like vehicles' limp mode can provide at least the core functionality for mission-critical capabilities and therefore business continuity.

4. Multi-Mode Systems

The idea of *multiple modes* and *mode switching* is well known from domains like, for example, aviation and automobiles. Airplanes have a parking mode, a taxiing mode, a take-off mode, manual and automatic flying mode, landing mode and perhaps an emergency mode. Such multi-mode systems are also used to manage complexity and to divide systems into modes of operation in the automotive domain. Self-driving cars may use a manual mode, an adaptive cruise control mode, a lane keeping assistant mode, an emergency braking mode or a parking mode [15, 2]. Each mode consists of a set of functionalities and a system configuration as well as different control goals. Modes can be represented by finite state machines [15]. Most vehicles also have a self-protection feature called limp mode. This mode is activated when abnormal behavior is detected to protect engine and transmission from major damage. The car's speed and performance are limited, but it can still be used to drive to a nearby service station or to a safe location at the roadside to wait for assistance.

Nuclear power plants have also systems with multiple operating modes like power operation, startup, hot standby, hot shutdown, cold shutdown and refueling [26]. There are special emergency and accident systems to change modes. If there is a malfunction or parameters are exceeding or falling below critical values, the reactor is immediately switched off automatically [22]. Such an emergency shutdown, called SCRAM, can also be triggered manually by a kill switch. These emergency stop buttons are used on railways, industrial machines, etc. to abort the current operation mode as quickly as possible in order to prevent damages, injuries and deaths. Dead man's switch is a similar fail-safe system at vehicles like motorcycles, snowmobiles and locomotives, which stop (or start) a machine if the human operator becomes unconscious or is removed from control.

In wireless networks, we know the infrastructure mode and the ad-hoc mode. Unix operating systems support a user-mode, a kernel-mode and if something goes wrong a rescue mode. Portable devices typically support a power saving mode that is turned on when the battery is running low.

From a security perspective, we imagine the use of several modes with different attack surfaces, e.g., secure (offline) modes for critical operations, modes with wired connection and modes with wireless connection like NFC, Bluetooth or Wi-Fi and modes for configurations. For IACSs, similar to most operational technology, availability and a fail-safe state are more important than confidentiality and integrity. Mode switching can provide an option to achieve both. We may even decide to tolerate restricted availability in order to stay secure and safe.

4.1. Mode Switching

A mode switch, or mode change, can be triggered by a *timer* or by a specific *event*. In real-time operating systems, modes are used for the efficient usage of resources and real-time adaptation. For instance, smart phones poll mail servers every 15 minutes (*timer*) and go into an idle or sleeping mode to save battery thereafter. When a phone call comes in (*event*), an active mode takes over from the idle mode.

As mentioned above, mode switching is used in many domains. Other than the use of different modes in digital twins [3] to detect, simulate and analyze attacks, as of our knowledge, there is no application of different modes in the security context of IACSs. We suggest to switch among modes with different attack surfaces, e.g., a secure mode for critical operations without outside connections, a mode with more or less reduced communication functionality. In the security context, a mode switch can be triggered from outside, for example, if a vulnerability becomes known or if it becomes known that attackers start exploiting a vulnerability. A mode switch should also be triggerable by the system itself, for example, if it has the capability to detect threats [12, 16].

4.2. Multi-modal Architecture

A multi-modal architecture with several operational modes needs to have secure and safe transitions between these modes. We have to define conditions when and how mode switches can be performed. We have to decide how to handle unfinished tasks and how to release new tasks of future modes. The number of tasks can lead to potential overloads and deadline misses. Some tasks of the old mode may have to be finished in order to keep patients safe. But we may want to abort non-safety-critical tasks, not only for performance but also for security reasons. To protect IACSs against threats, a risk-based framework that continually manages and assesses security risks along with their proactive addressing has been proposed in [18]. A multi-modal design approach is used for risk assessment and an adaptive remediation scheme to mitigate security threats.

Our research objective is to practically demonstrate a holistic approach based on [17, 18]. We plan to develop a software prototype to demonstrate how mode switching can resiliently respond to threats and even to zero-day attacks. Several mode change protocols exist to ensure task schedulability, resource management and quality of service [19, 2]. Modes can be switched based on specific conditions, e.g., safety or limited resources. These protocols need to be reviewed from a security perspective and analyzed for adaptation to mode switching in case of security threats.

We imagine the use of a middleware to provide core functionality for a variety of IACSs and maybe also for devices in other domains. Figure 1 gives an impression about the multi-modal software architecture. Example modes provide different features and attack surfaces and include a secure pre-configured mode (mode 0) for critical operations without outside connections, an emergency or limp mode to control the machine manually, e.g., to free a trapped person, a mode to initialize communication, e.g., NFC to transmit data only over a short distance, a communication mode with higher data transfer rate and more range, e.g., Bluetooth or Wi-Fi and a configuration mode where authorized persons can adapt settings. In a real system design, these modes may be more complex and overlap each other, e.g. some functionalities will be part of several modes. Specific core functionality could be implemented mode independent and work during all modes and switches.

4.3. Sample Mode-Switch Scenarios

A scheduler has to ensure the optimal utilization of resources and a proper and smooth change between individual modes. As mentioned in [17], real-time monitoring, threat detection and adaptive risk mitigation can be triggers for mode switches. If sensors detect a threatening situation, a multi-modal system can switch to another mode where further communication is restricted. With such a multi-mode system, system integrators or even operating staff will be able to reduce the attack surface, even if there is an inability to install security patches, even if a manufacturer has discontinued support, and even if a manufacturer no longer exists.

In case of a denial-of-service attack, e.g., to brute force authentication, systems should switch modes after a certain count of access attempts and deny further access for a specific period of time. Notifications to asset owners and device manufacturers about mode switches can help to detect problems early and to react in time. Such notifications will not prevent attacks, but they will make them more transparent and may prevent further damage.

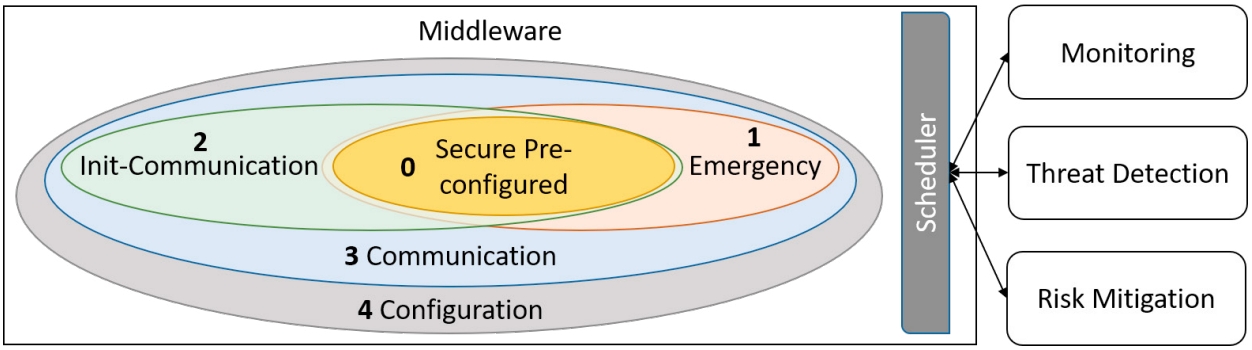

Fig. 1. Multi-modal software architecture

A limited attack surface resulting from a mode switch may allow one-way communication only, where collected data from the IACS can still be transmitted to the asset owner, but configuration changes are not allowed/possible anymore. This would require configuration changes to be done only by the system integrator or service personal, where systems may get changed back to a more flexible programming or configuration mode again. Minor remote changes may also be an option, for example, with a release mechanism that has to be activated manually by pressing a button on an IACS or in some other form. If the IACS is sold or decommissioned, asset owners can switch respectively reset it to the factory mode. Thereby internal passwords, system configuration and intellectual property can't be accessed by anyone.

5. Discussion

Mode switching will not provide a silver bullet to solve security problems. IACSs need an overall concept with several security layers (defense in depth), which considers the entire life-cycle from architecture, design and implementation up to eventual decommission. According to the principles for resilient systems listed in [7] the focus should be on mission-critical capabilities. All type of threats should be considered, not only security. Robustness, safety, interoperability and others are as well important. In fact, mode switching is an approach to provide security by design. Security needs to be considered in the product development from the very beginning. Adversities need to be detected early, and protection needs have to be identified and countermeasures taken. Fundamental security flaws in the architecture should be avoided and the architecture should resistant against security threats and recovers fast from harm.

It will be crucial how these ideas can be combined and merged with already existing operation modes of IACSs. Do the new modes increase the system's complexity and the risk of unintended interactions or negative side-effects? How does the transition from one mode to another work? Moreover, the multi-modal architecture should not become the new Achilles' heel or a new attack surface. Attackers could misuse the mode-switching mechanism in order to reduce functionality and availability. Table 1 summarizes benefits and drawbacks of a multi-modal architecture from a security point of view.

Table 1. Benefits and drawbacks of a multi-modal architecture from a security point of view

Benefits	Drawbacks
Secure the time between vulnerability disclosure and the availability of security patches	Potential misuse of mode-switching mechanism to reduce functionality and availability
Context-specific reduction of attack surface	Increased system complexity
More resilience to existing vulnerabilities	More extensive and more expensive design and development phase
Means of risk reduction for system operator (also for unpatched systems and even if manufacturer has stopped service)	Potential unintended negative side-effects due to multi-modal architecture
Reduced machine down-times due to cyber-attacks	

We can also see modes more comprehensively. An individual IACS, a class of machines, the production line, or a factory can each have a separate mode, not only from a technical but also from an organizational perspective. Modes of several IACSs can have an effect on the factory or global mode and vice versa. If a number of machines are attacked and they therefore switch to a different mode, this could result in further actions by the operator or manufacturer after a certain threshold value has been exceeded.

6. Conclusion

We have argued that a *multi-modal architecture* and *mode switching* will make connected industrial control and automation systems more secure and resilient against cyber-attacks. On the one hand, system integrators or asset owners will have the opportunity to reduce the attack surface by themselves without any updates. On the other hand, devices can be equipped with intrusion detection systems to automatically detect and ward off attacks by switching modes. Thus, the likelihood of being attacked can be reduced by limiting an attackers' range of activity. Our future work includes systematic analysis and evaluation of mode switching protocols and an investigation of how to apply them to security, especially in the context of IACSs. First findings of a systematic literature review on mode switching from a security perspective are presented in [20]. In addition, we plan a prototypical implementation for further evaluation and to demonstrate the effectiveness of mode switching for increased security.

Acknowledgements

This work has partially been supported by the LIT Secure and Correct Systems Lab funded by the State of Upper Austria.

References

[1] Allianz Global Corporate & Specialty SE, 2020. Allianz Risk Barometer. URL: https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2020-Appendix.pdf.

[2] Chen, T., Phan, L.T., 2018. SafeMC: A System for the Design and Evaluation of Mode-Change Protocols, in: 2018 IEEE Real-Time and Embedded Technology and Applications Symposium (RTAS), pp. 105–116. doi:10.1109/RTAS.2018.00021.

[3] Dietz, M., Pernul, G., 2020. Unleashing the Digital Twin's Potential for ICS Security. IEEE Security and Privacy Magazine 18, 20–27. doi:10.1109/MSEC.2019.2961650.

[4] European Union, 2006. Directive 2006/42/EC of the European Parliament and of the Council. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32006L0042&from=EN.

[5] Falliere, N., O Murchu, L., Chien, E., 2010. W32.stuxnet dossier. Symantec URL: https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf.

[6] Firesmith, D., 2019. System Resilience: What Exactly is it? URL: https://insights.sei.cmu.edu/sei_blog/2019/11/system-resilience-what-exactly-is-it.html.

[7] Firesmith, D., 2020. System Resilience Part 7: 16 Guiding Principles for System Resilience. URL: https://insights.sei.cmu.edu/sei_blog/2020/04/part-7-16-guiding-principles-for-system-resilience.html.

[8] Forbes, 2019. Critical 'Update Now' Warning Issued For VxWorks OS Inside 2 Billion IoT Devices. URL: https://www.forbes.com/sites/zakdoffman/2019/07/29/warning-as-2-billion-medical-industrial-and-enterprise-iot-devices-at-risk-of-attack/.

[9] Goodwin, B., 2020. Travelex hackers shut down German car parts company Gedia in massive 'cyber attack'. URL: https://www.computerweekly.com/news/252477247/Travelex-hackers-shut-down-German-car-parts-company-Gedia-in-massive-cyber-attack.

[10] Kerr, P.K., Rollins, J., Theohary, C.A., 2010. The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability. Congressional Research Service URL: https://fas.org/sgp/crs/natsec/R41524.pdf.

[11] Lasi, H., Fettke, P., Kemper, H.G., Feld, T., Hoffmann, M., 2014. Industry 4.0. Business & Information Systems Engineering 6, 239–242. doi:10.1007/s12599-014-0334-4.

[12] Lu, S., Lysecky, R., 2019. Data-driven Anomaly Detection with Timing Features for Embedded Systems. ACM Transactions on Design Automation of Electronic Systems 24, 1–27. doi:10.1145/3279949.

[13] Mitre, 2020. CVE - Common Vulnerabilities and Exposures. URL: https://cve.mitre.org/.

[14] National Institute of Standards and Technology (NIST), 2020. Smart Manufacturing Operations Planning and Control Program. URL: https://www.nist.gov/programs-projects/smart-manufacturing-operations-planning-and-control-program.

[15] Phan, L.T., Lee, I., 2011. Towards a Compositional Multi-modal Framework for Adaptive Cyber-physical Systems, in: Proceedings of the 2011 IEEE 17th International Conference on Embedded and Real-Time Computing Systems and Applications - Volume 02, IEEE. pp. 67–73. doi:10.1109/RTCSA.2011.82.

[16] Rao, A., Carreón, N., Lysecky, R., Rozenblit, J., 2018. Probabilistic Threat Detection for Risk Management in Cyber-physical Medical Systems. IEEE Software 35, 38–43. doi:10.1109/MS.2017.4541031.

[17] Rao, A., Carreón, N., Lysecky, R., Rozenblit, J., Sametinger, J., 2019. Resilient Security of Medical Cyber-Physical Systems, in: Database and Expert Systems Applications, Springer International Publishing. pp. 95–100. doi:10.1007/978-3-030-27684-3_13.

[18] Rao, A., Rozenblit, J., Lysecky, R., Sametinger, J., 2017. Composite Risk Modeling for Automated Threat Mitigation in Medical Devices, in: Proceedings of the Modeling and Simulation in Medicine Symposium, 2017 Society for Modeling & Simulation International (SCS). pp. 899–908. doi:10.22360/SpringSim.2017.MSM.013.

[19] Real, J., Crespo, A., 2004. Mode Change Protocols for Real-Time Systems: A Survey and a New Proposal. Real-Time Systems 26, 161–197. doi:10.1023/B:TIME.0000016129.97430.c6.

[20] Riegler, M., Sametinger, J., 2020. Mode Switching from a Security Perspective: First Findings of a Systematic Literature Review, in: Kotsis, G., Tjoa, A.M., Khalil, I., Fischer, L., Moser, B., Mashkoor, A., Sametinger, J., Fensel, A., Martinez-Gil, J. (Eds.), Database and Expert Systems Applications, Springer International Publishing, Cham. pp. 63–73. doi:10.1007/978-3-030-59028-4_6.

[21] Sametinger, J., Steinwender, C., 2017. Resilient Context-Aware Medical Device Security, in: International Conference on Computational Science and Computational Intelligence, Symposium on Health Informatics and Medical Systems (CSCI-ISHI), pp. 1775–1778. doi:10.1109/CSCI.2017.310.

[22] Shultis, J.K., Faw, R.E., McGregor, D.S., 2016. Fundamentals of Nuclear Science and Engineering; 3rd Edition. CRC Press. URL: https://cds.cern.ch/record/2245430.

[23] Strasser, T.I., Andrén, F.P., Vrba, P., Šuhada, R., Moulis, V., Farid, A.M., Rohjans, S., 2018. An Overview of Trends and Developments of Internet of Things Applied to Industrial Systems, in: IECON 2018 - 44th Annual Conference of the IEEE Industrial Electronics Society, p. 2853–2860. doi:10.1109/IECON.2018.8591431.

[24] The Brussels Times, 2020. Cyber attack sees Picanol shares suspended. URL: https://www.brusselstimes.com/news-contents/economic/89253/cyber-attack-sees-picanol-shares-suspended/.

[25] United States Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA), 2020. Alert (AA20-099A) - COVID-19 Exploited by Malicious Cyber Actors. URL: https://us-cert.cisa.gov/ncas/alerts/aa20-099a.

[26] United States Nuclear Regulatory Commission (NRC), 2019. Standard Technical Specifications – Operating and New Reactors – Current Versions. URL: https://www.nrc.gov/reactors/operating/licensing/techspecs/current-approved-sts.html.