Secured Remote Configuration Approach for Industrial Cyber-Physical Systems

Thomas Ulz, Thomas Pieber, Christian Steger
Institute for Technical Informatics
Graz University of Technology
Graz, Austria
{thomas.ulz, thomas.pieber, steger}@tugraz.at

Sarah Haas, Rainer Matischek
Design Center Graz
Infineon Technologies Austria AG
Graz, Austria
{sarah.haas, rainer.matischek}@infineon.com

***Abstract*—Facilitating remote updates of configuration parameters for industrial cyber-physical systems (ICPSs) is an emerging requirement due to interconnected production facilities. However, allowing remote configuration changes entail the following security issues. Malicious configuration updates through unprotected configuration interfaces can physically harm the ICPS or the respective process, and even threaten human lives. Also, for configuration interfaces to be remotely accessible, corporate networks need to be configured accordingly to provide access possibilities. Such additional access possibilities might then be used by adversaries when attacking corporate networks and thus, are often seen as a security weakness. If ICPS are not updated, outdated configurations also lead to security weaknesses. To mitigate these issues, we present a secured remote configuration approach for ICPS that protects the configuration interface as well as configuration data. The approach utilizes appropriate security measures and is realized as external configuration update module to allow easy verification of ongoing update processes.**

***Index Terms*—Industrial Cyber-Physical System; Remote Configuration; Industry 4.0; Security; Hardware Security.**

I. Introduction

Industrial Cyber-Physical Systems (ICPSs) represent various challenging security aspects compared to traditional Information and Communication Technology (ICT) systems and Internet of Things (IoT) devices. Since ICPSs are used in industrial processes, the availability of these systems is of utmost importance, and thus, ICPSs need to be operated continuously [1]. In addition, ICPSs interact with the physical world; therefore, a malfunctioning ICPS might cause physical damage to the device itself, other devices, or even to human lives [2]. Various attacks that targeted ICPS [3] and caused serious incidents have been documented. Probably the most well-known of these incidents, Stuxnet [4], has raised awareness regarding the danger that is posted by ICPSs that are not properly secured. To mitigate security issues, various countermeasures have been proposed. One of the more popular countermeasures being the isolation of ICPSs by restricting network access [5].

In contrast to that measure, recent strategies such as Industry 4.0 or the Industrial Internet of Things (IIoT) aim at integrating any device that is involved in an industrial process into the Internet [6]–[8]. Cardenas et al. [9] analyze potential attacking points for such interconnected Cyber-Physical Systems (CPS) and highlight types of attacks such as deception attacks [10] that are unique to CPS. However, also problems known from the IoT such as using default configurations, or username and password combinations are a major threat for ICPSs [11], [12]. To mitigate configuration-related issues, the configuration and reconfiguration capabilities of ICPSs need to be improved. Especially with the increase in enterprise network value due to interconnected devices, configuration management for these devices becomes an important issue [13].

Configurations of ICPSs that are connected to the network or even to the Internet can be done remotely and administrated by a cloud-based configuration management system [14]. However, such remote configuration approaches entail the following two security related drawbacks that must not be neglected: (i) Remote access to any ICPS that should be enabled for remote configuration updates needs to be granted. If access is granted on demand, a lot of administrative overhead is caused. To reduce overhead, devices could automatically check for configuration update. However, for this approach any device must be granted access to an external entity. In both scenarios, monitoring configuration updates is nearly impossible. (ii) Accidental or deliberate misuse of configuration interfaces might be used to perform attacks that could influence the correct functionality of the respective ICPS by applying malicious configurations [15], [16]. Also, malicious configuration parameters such as cryptographic keys might also lead to security breaches such as revealing confidential information or industrial espionage.

Contributions. To mitigate the previously mentioned security issues, we present an approach for ICPS remote configuration. Our approach proposes the use of *dedicated update hardware* that is *temporarily* attached to devices whenever configuration updates should be performed. This hardware allows easy monitoring of ongoing configuration updates while providing data confidentiality, integrity, and authenticity by applying adequate security measures. To the best knowledge of the authors, no such solution has been proposed previously.

Outline. The remainder of this paper is structured as follows. Section II defines a system model and the respective assumptions. We give background information on involved technologies as well as discuss related work in Section III. Our secured remote configuration approach is then presented in

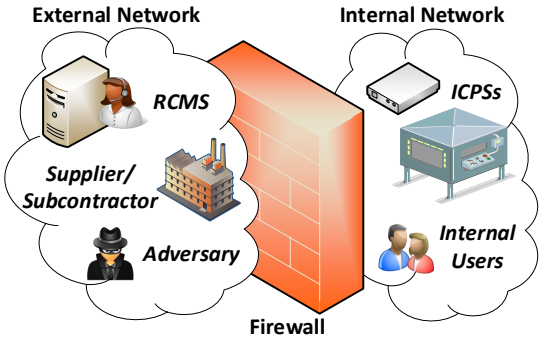

Fig. 1: System model: The internal network's entities are separated from the external network's entities by a firewall.

Section IV and evaluated using a threat analysis in Section V. This paper is then concluded with Section VI where we also discuss future work.

II. System Model and Assumptions

An overview of the system model that we consider for our presented approach is shown in Fig. 1. In this model, a *firewall* separates the *internal network* and its entities from the so-called *external network* and its entities. The internal network contains the following entities:

1) *ICPSs:* The ICPSs that are used in various industrial processes. Since the devices are located within the same network, they can communicate with each other.
2) *Internal Users:* Users that have access to the internal network and its ICPSs. These users might monitor or control the respective ICPSs.

The following entities are contained in the external network:

1) *Remote configuration management system (RCMS):* Any RCMS with its respective configuration database and users that perform remote configuration updates. Secured access to perform remote configurations must be granted for the RCMS.
2) *Suppliers/Subcontractors:* Other manufacturers that need access to certain information produced by the ICPSs contained in the internal network. For example, a just-in-time manufacturing process would require data to be sent to suppliers or subcontractors.
3) *Adversaries:* Adversaries that are trying to perform attacks targeting the ICPSs contained in the internal network. Attacks might target confidential data or the functionality of ICPSs which as a consequence would impact the manufacturing process. Access by adversaries must be prohibited by the firewall.

Assumptions. For our system model, we assume that the firewall is configured in a way, such that no entity from the external network is capable of accessing any entity in the internal network. That means any data or information required by an external entity must actively be delivered by the respective internal entity. As a consequence, this also means remote configuration updates initiated by an external entity are prohibited in this system model.

III. Background and Related Work

A. Wireless Technologies

The most widely used technologies for wireless Internet access nowadays are WiFi and cellular (3G/4G) [17]. Both technologies are also emerging as a choice for connecting CPSs to the Internet [18]. Although both technologies are very popular for wireless Internet access, they differ in areas such as protocol or required infrastructure. WiFi is designed to provide high bandwidths for access to local area networks (LANs) that are then connected to the Internet. Contrary, Internet access over cellular network technologies such as 3G or 4G is designed to cover larger areas while in general providing less bandwidth than WiFi. An emerging new standard, 5G, aims at providing reliable, high bandwidth connections over cellular networks [19].

B. Mutual Authentication

If one entity proves its identity to another entity when communicating with each other, a so-called authentication process is performed. For example, in the standard configuration of the Transport Layer Security (TLS) protocol, the client authenticates the server's identity [20]. If both entities authenticate each other, so-called mutual authentication is performed. This mode of operation is optional in TLS, but it is the default mode of operation in other protocols such as the Secure Shell (SSH) protocol [21].

C. Transport Layer Security (TLS)

TLS [20] provides a secured communication channel over an unsecured network. It is based on the Transmission Control Protocol (TCP) and thus applies to any network that uses TCP (e.g., Ethernet, WiFi, 4G/5G). TLS mainly aims at providing data confidentiality and integrity by using symmetric cryptography. Also, authenticity can be provided by authenticating a communication partner using public-key cryptography.

D. Authenticated Encryption (AE)

To provide data confidentiality, integrity, and authenticity, private key cryptography is combined with message authentication codes in a secured way, resulting in so-called AE [22]. AE is used in several well-known protocols and standards, such as IPSec or SSH.

E. Secure Element (SE)

SEs are capable of providing a protected execution environment as well as protected storage. Compared to traditional processing units, fault attacks such as exploiting buffer overflows are mitigated by an SE. If the SE is capable of providing tamper resistance [23], it is even protected against invasive attacks usually require physical access to the hardware. The security level provided by an SE is assessed by the common criteria (CC) information technology security evaluation [24]. SEs that are CC certified and suitable for industrial use are provided, for example, by Infineon [25].

TABLE I: Comparison with related work. We analyze remote configuration capability, sufficient security mechanisms, update process monitoring, and suitability for industrial scenarios (compatible with firewall restrictions, scale to many devices).

	Remote	Secured	Monitoring	Industrial
Smart home / IoT [26], [27]	✓	✗/✓	✗	✗
Automotive updates [28], [29]	✗/✓	✓	✗/✓	✗/✓
CPS mesh networks [30]	✓	✗/✓	✗	✗/✓
NFC-based [31], [32]	✗	✗/✓	✓	✗/✓
This work	✓	✓	✓	✓

F. ICPS Configuration

Although an important topic, remote configuration management for CPS and ICPS is often neglected due to its complexity [33]. Instead of granting the required remote access to configuration management solutions, self-configuration of devices is often promoted as a viable alternative [34], [35]. However, although such a principle applies to many configuration parameters, it cannot be applied in scenarios such as key management [15].

Web-based remote configuration for devices such as WiFi routers is a widely used feature, although infeasible for industrial scenarios. In terms of manual configuration management solutions, various approaches have been proposed for different domains. In the smart home and IoT domain, remote update mechanisms that rely on secured protocols such as the TLS protocol are proposed [26], [27]. However, these approaches do not provide tamper resistant mechanisms. Also, ongoing update processes cannot be monitored by the user. In the automotive domain, secured firmware and configuration updates are often performed using local network infrastructure only [28], [29]. These solutions however, often provide sufficient security measures due to the safety regulations that apply in the automotive domain. Staub et al. [30] present an approach for secured remote updates over a mesh network. Since every device is connected at any time, monitoring of ongoing configuration update processes is impossible using this approach. An approach that provides a hardware and software secured configuration interface in NFC [31], [32] would be suitable for ICPS. However, using this approach no remote connections to the configuration interface can be made. A summarized comparison of our proposed secured remote configuration approach with related work is shown in Table I.

IV. Secured Remote Configuration for ICPS

A. Connection Concept

To facilitate secured remote configuration of ICPSs, we propose a concept that excludes the configuration interface from the ICPS itself. Instead, we suggest using a dedicated, so-called *config stick (CS)*. Such a CS temporarily needs to be attached to any ICPS that requires a remote configuration update, for instance via a Universal Serial Bus (USB) interface. A similar principle of decoupling network hardware was suggested by Radulescu et al. [36]. Our basic concept is illustrated in Fig. 2. As can be seen there, the CS contains two essential components, an SE and a wireless communication (WC) module. The SE handles all cryptographic operations that are going to be discussed in detail in Section IV-B. The WC module is responsible for equipping the CS with wireless networking capabilities. In our approach, we suggest supporting two different wireless technologies to connect the CS to a network and consequently to the Internet. Depending on the scenario and customers' requirements, either one of these two technologies can be used.

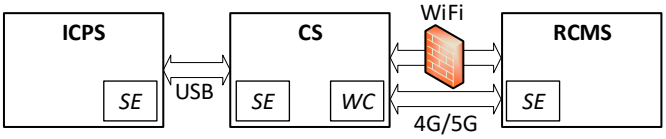

Fig. 2: Concept for configuration updates using the proposed CS. The CS is temporarily attached to the ICPS via USB. Remote connections are enabled via the WC module. The SE is used to perform security critical operations.

- *4G/5G.* If a 4G/5G module is included in the CS, directly accessing the Internet using such a module is possible. Thus, no additional access privileges need to be configured at a firewall. The drawbacks of such an approach are additional running costs that are entailed by requiring a 4G/5G data plan.
- *WiFi.* If a WiFi connection is used, the CS needs to access any remote configuration instance via the corporates firewall. That is, the firewall needs to be configured accordingly to grant Internet access to the respective CS. However, besides the configuration overhead, no additional costs are caused by this approach.

Independent of the wireless technology that is chosen to be included in the CS, configuration updates are always initiated by connecting the CS to the respective ICPS. Thus, the CS actively polls the RCMS for configuration updates. The CS only allows outgoing connections; incoming network traffic is automatically rejected. A sequence diagram showing a high-level abstraction of the configuration update process is shown in Fig. 3. As shown there, the CS is powered by the respective ICPS and initiates the configuration update process. After successfully applying a configuration update, the RCMS's database is updated to indicate the successful application of new configuration data for the respective ICPS.

Advantages/Disadvantages. If the presented CS concept is used for performing configuration updates, the following advantages and disadvantages result.

+ During normal operation of the ICPS, the configuration interface is not attached to the device itself. Thus, malicious configurations cannot be applied, and attacks that target the ICPS' configuration interface are not possible.
+ It is straightforward to monitor and control ongoing configuration update processes for any service technician. ICPSs that do not have a CS attached are currently not

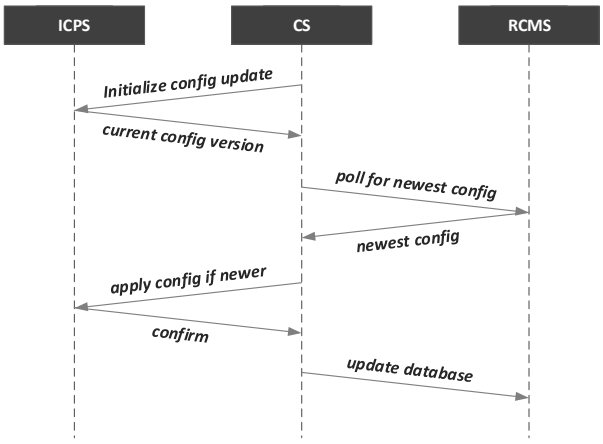

Fig. 3: Configuration update process. The CS is powered by the ICPS and initiates the remote configuration update process.

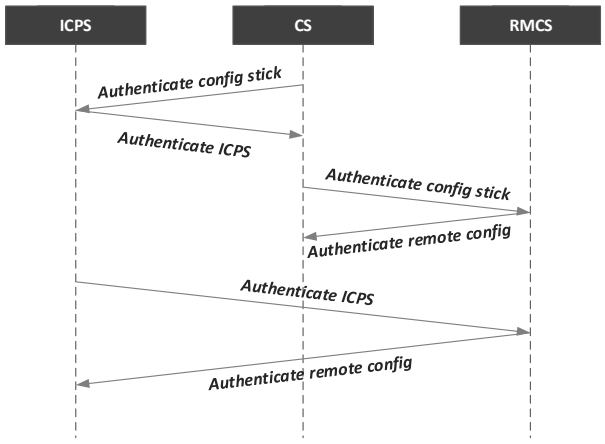

Fig. 4: 3-Way mutual authentication process that involves three separate mutual authentication steps between entities.

being updated. Thus, making it convenient to control which ICPSs are updated at any given time.

+ Using CSs, no or only minimal overhead is required to allow remote configuration updates. If the 4G/5G variant is used, no access rights need to be granted. If the WiFi variant is used, only a small number of CSs need to be granted Internet access, instead of any ICPS that needs to be remotely configured.
– Due to the fact that the CS needs to be attached to the ICPS that requires a configuration update, manual overhead is imposed compared to automated updates. However, this overhead mostly results from the advantageous feature that configuration interfaces are not attached to ICPSs during normal operation.

B. Security Concept

The security concept for our proposed secured remote configuration approach consists of two critical steps: (i) mutual authentication of all three involved entities, and (ii) establishing a secured data transfer channel to transmit configuration data. Both of these steps make use of functionality provided by an SE that is included in the all three entities (ICPS, the CS, and the remote config management system, see Fig. 2).

3-Way Mutual Authentication. To ensure the authenticity of each entity involved in a remote configuration update, the process shown in Fig. 4 is applied. Since the update process involves three entities (ICPS, CS, RCMS), a simple mutual authentication process cannot be applied. Therefore, we propose performing the following three mutual authentication steps:

1) ICPS and CS perform mutual authentication. After the process is successfully performed, the ICPS is ensured that a trusted CS is used, while the CS has verified that a configuration update will be performed for a trusted ICPS. Since the CS is powered by inserting it into the ICPS, the mutual authentication step between these two entities is always performed first.
2) After a trust relationship between ICPS and CS is established successfully, the CS and the RCMS perform a mutual authentication process. This checks the CS that it is connected to a trusted RCMS, while the RCMS is assured to transfer data to a trusted CS.
3) After both ICPS and RCMS have established a trust relationship with the CS, it can act as a gateway to enable a trusted connection between ICPS and RCMS. Thus, as the last step a mutual authentication between ICPS and RCMS is performed.

After all three mutual authentication steps have been performed successfully, a trust relationship between all three entities involved in the configuration update process is established. Since no such mutual authentication process was yet proposed in a secured device configuration scenario, we denote this process as *3-Way Mutual Authentication*.

Secured Data Transfer Channel. After a trust relationship between all three entities is established via our proposed 3-way mutual authentication process, a secured data transfer channel can be established. Since the CS is trusted by the ICPS and the RCMS, it can act as a gateway when establishing the secured data channel. Therefore, two encrypted connections (from ICPS to CS and from CS to RCMS) are used. The secured data channel between CS and RCMS either uses WiFi or 4G/5G, and thus, the TLS protocol can be used. Data that is transferred over between ICPS and the CS is protected by AE. Since the CS must not be able to read the actual configuration data (just a version indicator is required), the configuration data can be transmitted end-to-end encrypted from the RCMS to the ICPS. The ICPS then verifies the data package and decides if the configuration should be applied. A successful configuration update is then reported to the RCMS via the CS (see Fig. 3).

Use of SE. We assume that an SE is included in the ICPS, the CS, and the RCMS to perform the following three tasks:

1) Certificates and private keys used for mutual authentication are stored in the secured memory of the SE. Thus, an attacker with physical access to any device is not able to gain access to any of this confidential information.
2) The authentication of other entities in the mutual authentication process is performed in the secured execution environment of the SE so that attacks that try to tamper with the authentication process are mitigated.
3) Private keys are generated by the SE and stored in its secured storage, such that these keys cannot be easily extracted by an attacker. If the keys are used to perform encryption and decryption operations, these operations are also performed in the secured execution environment of the SE, such that side-channel attacks that try to reveal these keys are mitigated.

V. Threat Analysis

To evaluate the level of security provided by our proposed remote configuration update approach, we perform a formal threat analysis. The list of threats is by no means exhaustive; it rather highlights the (from our point of view) most important issues. The threat analysis is going to highlight all *entities (E)* capable of influencing the system's security, the *assets (A)* that need to be protected, *assumptions (As)* that are made regarding entities and assets, the actual *threats (T)*, applied *countermeasures (C)* to mitigate the threats, and *residual risks (R)* that cannot be mitigated by our approach.

Entities: The entities that are capable of influencing the security of our approach are identified first.

- **(E1):** ICPS that needs to be updated.
- **(E2):** CS that is used to perform configuration updates.
- **(E3):** RCMS that handles managed device configurations.
- **(E4):** ICPS manufacturer.
- **(E5):** CS manufacturer.
- **(E6):** Adversary.

Assets: The assets that need to be protected by our approach to be considered sufficiently secured are then identified.

- **(A1):** The ICPS's *configuration interface* must be protected against any type of attack.
- **(A2):** The ICPS's *functionality* must not be compromised by any type of malicious action.
- **(A3):** Transferred *configuration data* may contain confidential information and thus, needs to be protected.

Assumptions: After entities and assets are identified, we identify the respective assumptions that are made.

- **(As1):** Potential adversaries might have remote access or physical access to the ICPS.
- **(As2):** The updates provided by the RCMS are assumed to be trustworthy and not malicious.
- **(As3):** Applied protocols for the secured data channel (TLS, AE) are assumed to sufficiently protect data confidentiality, integrity, and authenticity.
- **(As4):** The used SEs provide sufficient protection against physical attacks and are certified by a trusted third party (e.g., CC certification process [24]).
- **(As5):** The RCMS is assumed to be sufficiently secured against cyber-attacks that directly target the configuration database or any other stored information.

Threats: Finally, threats and respective countermeasures or residual risks are identified.

- **(T1):** Attacks targeting the ICPS configuration interface.
  Entities/Assets: (E1), (E6); (A1), (A2)
  (C1a): Configuration interface is detached from ICPS and realized as dedicated CS.
  (C1b): Interface to CS and to RMCS is protected by 3-way mutual authentication process.
- **(T2):** Application of malicious configuration data.
  Entities/Assets: (E1), (E3), (E6); (A1), (A2), (A3)
  (C2a): 3-way mutual authentication prevents malicious entities from applying configuration updates.
  (C2b): The subsequent secured data channel is used to protect transferred configuration data.
- **(T3):** Impersonation attack as either CS or RCMS.
  Entities/Assets: (E1), (E2), (E3), (E6); (A1), (A2), (A3)
  (C3): 3-way mutual authentication is performed. The relevant certificates and key material are stored in the secured and tamper resistant SE's memory.
- **(T4):** Security issues in either the CS or ICPS interface.
  Entities/Assets: (E1), (E2), (E4), (E5); (A1), (A2), (A3)
  (C4): When using a CC certified SE, this threat is also mitigated by the CC certification process.
- **(T5):** Side-channel attack revealing secrets.
  Entities/Assets: (E1), (E2), (E6); (A1), (A2), (A3)
  (C5): Due to requiring tamper resistant SEs in our proposed architecture, side-channel attacks are considered infeasible for adversaries.
- **(T6):** Denial-of-Service attack on active CS or RCMS.
  Entities/Assets: (E2); (A1)
  (C6): Since the system architecture is designed such that only outgoing connections are required, incoming connections are rejected by firewalls in case of using the CS's WiFi variant.
  (R6): Denial-of-Service attacks targeting the CS's 4G/5G interface or the RCMS cannot be mitigated by our presented approach.

VI. Conclusion and Future Work

In this paper, we present an approach for secured remote configuration of ICPS. In our approach, we suggest detaching the configuration interface from ICPSs for two reasons. First, if no configuration interface is attached, it is not practical to attack the interface during normal operation of the ICPS. Second, a detached configuration interface introduces less overhead in terms of required network configuration compared to allowing network access for each ICPS that should be capable of remote configuration updates. By introducing our so-called 3-way mutual authentication process and by applying standard protocols to establish a secured data channel, our approach provides confidentiality, integrity, and authenticity of configuration data. The threat analysis demonstrates that we

are capable of completely mitigating five out of the six most harmful threats that we identified. The final threat, denial-of-service attacks, are usually hard to mitigate but sill partially mitigated by our proposed approach. As future work, we plan to investigate the possibility to deploy local gateways for CS. This would allow connecting the CSs using technologies such as Bluetooth to connect to the gateway that is then connected to the Internet.

ACKNOWLEDGMENT

This work has been performed within the IoSense (http://iosense.eu) project. This project has received funding from the Electronic Component Systems for European Leadership Joint Undertaking under grant agreement No 692480. This Joint Undertaking receives support from the European Union's Horizon 2020 research and innovation programme and Germany, Netherlands, Spain, Austria, Belgium, Slovakia. IoSense is funded by the Austrian Federal Ministry of Transport, Innovation and Technology (BMVIT) under the program "ICT of the Future" between May 2016 and April 2019. More information: https://iktderzukunft.at/en/.

REFERENCES

[1] R. R. Rajkumar, I. Lee, L. Sha, and J. Stankovic, "Cyber-Physical Systems: The Next Computing Revolution," in *Proceedings of the 47th Design Automation Conference*. ACM, 2010, pp. 731–736.

[2] P. Derler, E. A. Lee, and A. S. Vincentelli, "Modeling CyberPhysical Systems," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 13–28, 2012.

[3] T. Ulz, S. Haas, and C. Steger, "Cyber-Physical System and Internet of Things Security: An Overview," in *Solutions for Cyber-Physical Systems Ubiquity*. IGI Global, 2018, pp. 248–277.

[4] R. Langner, "Stuxnet: Dissecting a Cyberwarfare Weapon," *IEEE Security & Privacy*, vol. 9, no. 3, pp. 49–51, 2011.

[5] S. Karnouskos, "Stuxnet Worm Impact on Industrial Cyber-Physical System Security," in *IECON 2011-37th Annual Conference on IEEE Industrial Electronics Society*. IEEE, 2011, pp. 4490–4494.

[6] N. Jazdi, "Cyber Physical Systems in the Context of Industry 4.0 ," in *Automation, Quality and Testing, Robotics, 2014 IEEE International Conference on*. IEEE, 2014, pp. 1–4.

[7] J. Lee, B. Bagheri, and H.-A. Kao, "A Cyber-Physical Systems architecture for Industry 4.0-based manufacturing systems," *Manufacturing Letters*, vol. 3, pp. 18–23, 2015.

[8] A.-R. Sadeghi, C. Wachsmann, and M. Waidner, "Security and Privacy Challenges in Industrial Internet of Things," in *Design Automation Conference (DAC), 2015 52nd ACM/EDAC/IEEE*, 2015, pp. 1–6.

[9] A. Cardenas, S. Amin, B. Sinopoli, A. Giani, A. Perrig, and S. Sastry, "Challenges for Securing Cyber Physical Systems," in *Workshop on Future Directions in Cyber-Physical Systems Security*, vol. 5, 2009.

[10] C. Kwon, W. Liu, and I. Hwang, "Security Analysis for Cyber-Physical Systems against Stealthy Deception Attacks," in *American Control Conference (ACC), 2013*. IEEE, 2013, pp. 3344–3349.

[11] A. Cui and S. J. Stolfo, "A Quantitative Analysis of the Insecurity of Embedded Network Devices: Results of a Wide-Area Scan," in *Proceedings of the 26th Annual Computer Security Applications Conference*. ACM, 2010, pp. 97–106.

[12] E. Le Malécot and D. Inoue, "The Carna Botnet Through the Lens of a Network Telescope," in *Foundations and Practice of Security*. Springer, 2014, pp. 426–441.

[13] Z. Kerravala, "As the Value of Enterprise Networks Escalates, So Does the Need for Configuration Management," *The Yankee Group*, 2004.

[14] A. W. Colombo, T. Bangemann, S. Karnouskos, J. Delsing, P. Stluka, R. Harrison, F. Jammes, J. L. Lastra *et al.*, "Industrial Cloud-Based Cyber-Physical Systems," *The IMC-AESOP Approach*, 2014.

[15] Y. Mo, T. H.-J. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, and B. Sinopoli, "CyberPhysical Security of a Smart Grid Infrastructure," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 195–209, 2012.

[16] S. Sridhar, A. Hahn, and M. Govindarasu, "CyberPhysical System Security for the Electric Power Grid," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 210–224, 2012.

[17] W. Lehr and L. W. McKnight, "Wireless Internet access: 3G vs. WiFi?" *Telecommunications Policy*, vol. 27, no. 5, pp. 351–370, 2003.

[18] F.-J. Wu, Y.-F. Kao, and Y.-C. Tseng, "From wireless sensor networks towards cyber physical systems," *Pervasive and Mobile Computing*, vol. 7, no. 4, pp. 397–413, 2011.

[19] P. Popovski, "Ultra-Reliable Communication in 5G Wireless Systems," in *5G for Ubiquitous Connectivity (5GU), 2014 1st International Conference on*. IEEE, 2014, pp. 146–151.

[20] T. Dierks and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2," Internet Requests for Comments, RFC Editor, RFC 5246, August 2008. [Online]. Available: http://www.rfc-editor.org/rfc/rfc5246.txt

[21] T. Ylonen, "SSH - Secure Login Connections over the Internet," in *Proceedings of the 6th USENIX Security Symposium*, vol. 37, 1996.

[22] M. Bellare and C. Namprempre, "Authenticated Encryption: Relations among Notions and Analysis of the Generic Composition Paradigm," in *International Conference on the Theory and Application of Cryptology and Information Security*. Springer, 2000, pp. 531–545.

[23] S. Ravi, A. Raghunathan, and S. Chakradhar, "Tamper Resistance Mechanisms for Secure Embedded Systems," in *VLSI Design. Proceedings. 17th International Conference on*. IEEE, 2004, pp. 605–611.

[24] D. Mellado, E. Fernández-Medina, and M. Piattini, "A common criteria based security requirements engineering process for the development of secure information systems," *Computer standards & interfaces*, vol. 29, no. 2, pp. 244–253, 2007.

[25] J. Haid, "Hardware-based solutions secure machine identities in smart factories," *Boards & Solutions*, pp. 10–13, 2016.

[26] A. E. Nikolaidis, S. S. Papastefanos, G. I. Stassinopoulos, M.-P. Drakos, and G. A. Doumenis, "Automating Remote Configuration Mechanisms for Home Devices," *IEEE Transactions on Consumer Electronics*, vol. 52, no. 2, pp. 407–413, 2006.

[27] Q. Zhu, R. Wang, Q. Chen, Y. Liu, and W. Qin, "IOT Gateway: Bridging Wireless Sensor Networks into Internet of Things," in *Embedded and Ubiquitous Computing (EUC), 2010 IEEE/IFIP 8th International Conference on*. IEEE, 2010, pp. 347–352.

[28] G. de Boer, P. Engel, and W. Praefcke, "Generic Remote Software Update for Vehicle ECUs Using a Telematics Device as a Gateway," in *Advanced Microsystems for Automotive Applications 2005*. Springer, 2005, pp. 371–380.

[29] M. Steger, C. Boano, M. Karner, J. Hillebrand, W. Rom, and K. Römer, "SecUp: Secure and Efficient Wireless Software Updates for Vehicles," in *Digital System Design (DSD), 2016 Euromicro Conference on*. IEEE, 2016, pp. 628–636.

[30] T. Staub, D. Balsiger, M. Lustenberger, and T. Braun, "Secure Remote Management and Software Distribution for Wireless Mesh Networks," in *Proceedings of the 7th International Workshop on Applications and Services in Wireless Networks. ASWN 2007*, 2007.

[31] J. Haase, D. Meyer, M. Eckert, and B. Klauer, "Wireless sensor/actuator device configuration by NFC," in *2016 IEEE International Conference on Industrial Technology (ICIT)*. IEEE, 2016, pp. 1336–1340.

[32] T. Ulz, T. Pieber, A. Höller, S. Haas, and C. Steger, "Secured and Easy-to-Use NFC-Based Device Configuration for the Internet of Things," *IEEE Journal of Radio Frequency Identification*, vol. 1, no. 1, pp. 75–84, 2017.

[33] L. Gurgen, O. Gunalp, Y. Benazzouz, and M. Gallissot, "Self-aware cyber-physical systems and applications in smart buildings and cities," in *Proceedings of the Conference on Design, Automation and Test in Europe*. EDA Consortium, 2013, pp. 1149–1154.

[34] K. Nie, T. Yue, S. Ali, L. Zhang, and Z. Fan, "Constraints: The Core of Supporting Automated Product Configuration of Cyber-Physical Systems," in *International Conference on Model Driven Engineering Languages and Systems*. Springer, 2013, pp. 370–387.

[35] B. Bordel, R. Alcarria, D. Martín, T. Robles, and D. S. de Rivera, "Self-configuration in humanized Cyber-Physical Systems," *Journal of Ambient Intelligence and Humanized Computing*, vol. 8, no. 4, pp. 485–496, 2017.

[36] A. Radulescu, J. Dielissen, K. Goossens, E. Rijpkema, and P. Wielage, "An Efficient On-Chip Network Interface Offering Guaranteed Services, Shared-Memory Abstraction, and Flexible Network Configuration," in *Design, Automation and Test in Europe Conference and Exhibition, 2004. Proceedings*, vol. 2. IEEE, 2004, pp. 878–883.