Re-Envisioning Industrial Control Systems Security by Considering Human Factors as a Core Element of Defense-in-Depth

Jens Pottebaum*,†
Product Creation
jens.pottebaum@hni.upb.de

Jost Rossel*
System Security
jost.rossel@upb.de

Juraj Somorovsky*
System Security
juraj.somorovsky@upb.de

Yasemin Acar*,§
Empirical Software Engineering
yasemin.acar@upb.de

René Fahr*,†
Behavioral Economic Engineering
and Responsible Management
rene.fahr@upb.de

Patricia Arias Cabarcos*
Human-Centered
IT Security
pac@mail.upb.de

Eric Bodden*,†,‡
Secure Software
Engineering
eric.bodden@upb.de

Iris Gräßler*,†
Product Creation
iris.graessler@hni.upb.de

**Paderborn University, Paderborn, Germany*
†Heinz Nixdorf Institute, Paderborn, Germany
‡Fraunhofer IEM, Paderborn, Germany
§The George Washington University, Washington, USA

***Abstract*—The security of Industrial Control Systems is relevant both for reliable production system operations and for high-quality throughput in terms of manufactured products. Security measures are designed, operated and maintained by different roles along product and production system lifecycles. Defense-in-Depth as a paradigm builds upon the assumption that breaches are unavoidable. The paper at hand provides an analysis of roles, corresponding Human Factors and their relevance for data theft and sabotage attacks. The resulting taxonomy is reflected by an example related to Additive Manufacturing. The results assist in both designing and redesigning Industrial Control System as part of an entire production system so that Defense-in-Depth with regard to Human Factors is built in by design.**

***Index Terms*—Defense-in-Depth, Human Factors, Production Engineering, Product Design, Systems Engineering**

1. Introduction

Industrial control architectures—including various types of Industrial Control Systems (ICSs)—form the backbone of any Cyber-Physical Production System (CPPS). These ICSs, like Process Control Systems and Programmable Logic Controllers, can be realized, for instance, by multi-agent systems [10], [23]. They ensure both communication within the production systems and factory settings, as well connection with cloud services like scheduling systems. Durability is a key requirement of established systems, often running for long periods of time in manufacturing companies. Upgrading to cyber-physical capabilities means either replacing existing ICS or retrofit solutions [29]. As a system element of an integrated production system, ICSs can be both an attack target and a mitigation element for the entire system.

The Defense-in-Depth paradigm emphasizes sophisticated security solutions to be implemented in CPPSs through integrated ICSs [9]. Nonetheless, it always assumes missed attacks and, thus, security breaches that are unavoidable [42]. This is in line with three of the top four security related business concerns [34]. In CPPS design, all types of threats need to be considered interdependently. IT attacks might affect the operation of physical assets. While Defense-in-Depth of ICS has been established already, existing approaches narrow down threat analysis to very ICS specific events, vectors, and detection measures [30]. They slice a system into layers instead of modeling and analyzing threat chains from Human Factors in business layers down to control layers.

For instance, Additive Manufacturing (AM) is considered as an example of highly digitized production, controlled and monitored through ICS [19] (see Figure 1). Product geometries and process specifications, including pre- and post-processing, are provided by engineers. They design, implement and verify specifications. Machine parameters, programs and scheduling of specific machines are managed by production managers. Their tasks highly depend on settings from series production to individual orders. Workers run the actual process and handle input material and manufactured parts. They operate with parameter settings as well as physical materials and parts. Considering an exemplary attack, the laser of an AM machine might operate out of qualified boundaries, leading to defects in manufactured parts. Security zones can be introduced as countermeasures, but these could be breached as well. Thus, malicious laser control data might be injected by all mentioned roles.

Knowing that attackers always try to find new attack routes, Defense-in-Depth requires anticipation of future threat scenarios, including those that at the time still seem to be unrealizable [21]. Recognizing the interaction of humans in designing, planning and operating ICSs, we adopt fundamentals from human-centered design. With the aim to make systems usable and useful, we adopt Human Factors and principles of ergonomics. While this approach intends to enhance effectiveness and efficiency as well as improves, for instance, accessibility [44], we consider Human Factors also as a dimension to be included in our assessment of threats, a connection commonly made in security research [18]. We strongly emphasize

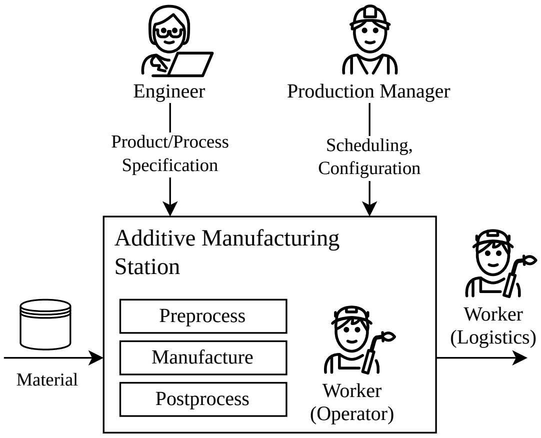

Figure 1. Overview of a production process in the exemplary field of Additive Manufacturing.

that Defense-in-Depth threat analysis (which is the focus of this paper) and countermeasures need to be traceable and adaptable with regard to the dynamics of possible attacks. Thus, this systemic Defense-in-Depth approach to be applied in the product and production engineering phase means an extension of known approaches of Design-for-X [46]. The paper at hand specifically focuses on Human Factors behind “human errors and sabotage”, which are ranked among the top ten threats in 2022 [16]. Examples of relevant real-world attacks in this area include the Ukraine power grid shutdown in 2015 [27] and the hijacking of a US water management plant in 2021 [11]. In both cases, the attacker’s success relied on human factors, such as exploiting configuration errors introduced by administrators, and leveraging employees poor password practices or security unawareness. We use exercises on threat modeling in a specific use case to merge different disciplinary research perspectives into a joint ICS threat analysis approach as a foundation for Defense-in-Depth.

Initially, the paper provides fundamental categories of security breaches, background from the field of Cyber-Physical Systems (CPSs) and CPPSs, as well as relevant aspects of Human Factors research (Section 2). Related work is presented in Section 3 and used to derive a taxonomy of attack routes through roles in CPS/CPPS design and realization (Section 4). Its application is used for preliminary conclusions in Section 5, contributing insights and an outlook from ongoing research.

2. Background

Security breaches related to Human Factors can be distinguished by two main categories: data theft and sabotage [49]. While the intention of data theft is to steal intellectual property or sensitive data (product piracy, phishing, . . .), sabotage affects operation of a product, or a whole production system, either by manipulating the product’s model or the specific instance itself. The intention is to either attack the company (e.g., by production shutdown) or users. Even in the latter case, indirectly the company is impacted (product breaks causing injuries/casualties).

According to the SANS report on the “State of ICS/OT Cybersecurity in 2022 and Beyond” [34], the human-machine interface or operator workstation is the second system component at greatest risk for compromise, right after engineering workstations. This means, besides technical routes, such breaches can be realized by attacking humans in design and operation of ICS in CPPS [20]. The distinction between primary and secondary attacks (cf. [16]) is essential in the field of Human Factors. Primary attacks are initiated from outside a company. A focus can be derived on how employees can be enforced to perform malicious actions, which is out of the scope of the paper at hand. Instead, we focus on secondary attacks assuming that actors in specific roles act maliciously, either as outsiders with access into the company, or insiders.

When considering ICSs, we can distinguish three types of roles in terms of work environment, responsibilities, and corresponding permissions (cf. Figure 1):

- Engineers design and plan CPPS down to ICS programs. They act as requirements engineers, system architects, software engineers or process engineers [22]. They work in office environments using engineering tools like Computer Aided Design (CAD), Model-Based Systems Engineering (MBSE) and Integrated Development Environment (IDE).
- Production managers schedule specific machines, handle orders and care for Maintenance, Repair, and Overhaul (MRO). They access tools like Enterprise Resource Planning (ERP), Manufacturing Execution System (MES) and Production Control System (PCS) from the office, but from within the technical environment of the factory.
- Workers perform tasks close to machines, robots etc. and, for example, check quality of parts in assembly.

With regard to these categories of roles, Human Factors need to be considered when anticipating security breaches.

3. Related Work

In our work, we investigate four major pillars to consolidate related work regarding the analysis of and adoption to Human Factors to strengthen ICS security. Research on *Counterproductive Workplace Behavior (CWB)* provides fundamentals on potential personality profiles of malicious actors. Background can be brought in from the field of *IT security* in software development. Turning into the specific domain of production, we use AM as a reference example of technologies. AM is often referred to as a completely digitized process, potentially affecting complex ICS architectures. *Authentication* measures are based on knowledge about human machine interaction, covering both empirical backgrounds and countermeasures. The field of empirical research on *Human Factors in engineering* acting as attackers is hardly tackled on overarching system level and, for instance, mechanical engineering.

Attacker profiles and personalities. In the management and organizational behavior literature, attacks in an ICS performed by employees of the company are classified as one dimension of Counterproductive Workplace Behavior (CWB). Robinson and Bennett [39] came up with four dimensions of deviant workplace behavior, where property deviance including sabotaging equipment and stealing from the company is one of them. A key question when anticipating the threat scenarios is the motivation of the malicious employee. The motivation of the employee for deviant behavior is typically linked to the employees' personality trait. In a meta-analysis [33] the personality traits associated with the Dark Triad, Narcissism, Machiavellianism, and psychopathy [35] are typically linked to CWB. In addition, the Honesty-Humility trait of the HEXACO personality domains [5] is associated with CWB according to a meta-analysis by Pletzer et al. [36].

So far, the profiling of attackers is based mostly on assuming personas based on publicly available sources of data with information about the characteristics and motives of people who have been known to attack systems (cf. Atzeni et al. [6]). With administering personality questionnaires to participants in incentivized lab experiments, it is possible to relate personality traits directly to unethical decision-making, as demonstrated by Heck et al. [26] for the relation of the Honesty-Humility personality trait with cheating behavior. According to the economic approach to crime [7] the supposed offender is doing a cost-benefit analysis. An attacker with criminal motives will accordingly attack only if the probability of success and the gain is higher than the probability to be detected and the expected fine. In Abbink and Sadrieh (2009) an incentivized pen-and-paper classroom experiment proved itself as a useful research method to establish a trait called the "joy of nastiness" by the authors [2]. People might have a pleasure of harming others without having a personal advantage of other people's damage.

IT security in Cyber-Physical Systems. There are several works considering the security of Cyber-Physical Systems [14], [24], [37]. A good overview of potential threats provide Ratasich et al. [37]. They categorized the threats according to different layers (physical, network, control, and information layer) and provided mitigation strategies for the presented attacks.

Security research in Cyber-Physical Systems is especially active in the field of AM [14], [24]. Gupta et al. presented AM as one of the central parts of a typical Cyber-Physical System. They gave an overview of attacks and categorized them according to attacks on printer hardware, raw materials, and design files. The research on AM is not only limited to industrial applications but also to consumer devices and software since many users now possess 3D printers. This can be observed in the overview of the field by Yampolskiy et al. [49] who highlighted two main attack types: data theft and model sabotage [49]. In the following, we show how such attacks affect 3D printers and thus can have potential impact on CPSs.

To steal data, attackers can target 3D printers directly or perform specific side-channel attacks. A 2016 study by Do et al. [13] revealed that MakerBot 3D printers could be controlled by attackers through their WiFi connection, enabling data extraction and print manipulation. McCormack et al. built on this research and identified vulnerabilities in various networked 3D printers [31]. Side-channel attacks targeting 3D model data have been extensively studied due to concerns of industrial espionage. Al Faruque et al. demonstrated the use of audio recordings of the printing process as an acoustic side channel to reconstruct the model accurately [3]. Similarly, Song et al. and Hojjati et al. found that modern smartphone sensors, such as microphones and magnetic sensors, could also be used to exfiltrate 3D model data with high precision [41], [28].

Sabotage attacks concentrated around manipulations of printed models. In 2017, Belikovetsky et al. introduced attacks on desktop 3D printers [8]. The attacks require malware installed on the user's personal computer. In one attack, the malware manipulates the low-level instructions sent to the printer to weaken the model structurally.[1] Sturm et al. achieved a similar effect, attacking the model files directly [43]. During a user study, they further evaluated whether their malicious modifications would be detected by the person creating and producing the file. None of the participants noticed the changes in software, some noticed them during production but attributed them to a machine fault [43]. Zeltmann et al., on the other hand, bypassed industrial testing facilities and proved that it is possible to manipulate G-code instructions without the difference being detected in the manufactured parts [50].

Security issues in authentication mechanisms. An important security issue in ICSs are attacks that leverage flaws in the implementation and usage of user authentication mechanisms. Default or even hard-coded passwords are a widespread problem and an easy attack vector that was exploited in high-profile incidents, such as the shutdown of a top U.S. oil pipeline [15]. Once this first protection barrier is surpassed, subsequent attacks can be executed, for example, to exfiltrate knowledge or damage the integrity of the ICS using the privileges and resources of the stolen account.

Given the massive amount of critical data and software used in CPPS, recent research is looking at how to introduce strong authentication protections that are suitable for these specific scenarios [1]. Security best practices recommend the use of multifactor authentication, for which current mechanisms lack usability [38]. Besides, the richness of sensors in CPPSs allows for the implementation of seamless and continuous multi-biometrics [17]. In this space, however, there is little research on providing context-based authentication [4]. This type of solution would adapt the required authentication level depending on the current risk and user environment, for example: activating a hands-free mechanism if the user is working, or triggering a multifactor request only if the data accessed is highly sensitive. In this paper, we give an important first step into understanding the types of attacks that humans in an CPPS can perform determining this part of the risk surface will help in designing context-aware authentication mechanisms, as well as other protections that can be layered in a Defense-in-Depth fashion.

Empirical research on Human Factors in software development. Empirical research methods that involve professionals involved in production helps better understand security issues in software development processes [47], [48], [25], [40], [32] which can be opportunities for attack. Interviews [48], [25], ethnographies, and surveys [47] with those involved in the engineering process, as well as large-scale measurements on software products are used

[1] The attacked instructions are G-Codes [12], [45]. These are used for Computer Numerical Control (CNC) machines, like mills and 3D printers. G-codes generally instruct the machine's movement.

to identify how human factors can attack and be attacked, as well as how human factors can be root causes for widespread security problems. We follow the example of systematically assessing actors, their access capabilities, and their potential goals to contribute our taxonomy of attacks on Cyber-Physical Systems.

4. Towards Categorization of Attacks to be anticipated for Defense-in-Depth

To understand Human Factors and their impact on possible breaches, different types of attacks need to be considered. Drawing initial conclusions from, both, Section 2 and the related work, we argue that attacks on Cyber-Physical Production System (CPPS) and their Industrial Control System (ICS) elements differ based on their *goal*, *scope*, and *stealth factor*.

Goal The attack's goal describes what an attacker tries to achieve. Based on the related work, we distinguish between *Sabotage* and *Theft*.

Scope The scope of the attack is defined by the permissions the attacker can use. The roles *Engineer*, *Production Manager*, and *Worker* capture these permissions.

Stealth An attacker might either act covertly, as not to be discovered, or they might intend to be discovered. We label these types as *high stealth* and *low stealth*, respectively. We do not consider this factor to be binary (see Section 4.3).

In this section, we will show how these notions can be understood when combined and how attacks can be categorized using them.

4.1. Achievable Impact

Engineers, product managers, or workers can turn malicious, intrinsically or extrinsically manipulated by outsiders, and may attempt to sabotage the process or steal Intellectual Property (IP). The achievable impact of an attack is the combination of its goal and scope (see Table 1).

The impact on the company regarding sabotage and theft can vary widely depending on the company's sector. Sabotaging the product can range from dissatisfied customers to people dying as a result, if the product is safety-critical. IP theft mainly leads to loss of Unique Selling Points (USPs) for the company, as product information is leaked to the competition before an official announcement, they can start early with plans for marketing campaigns and competing products. Again, in safety-critical products, the theft of product information might lead to severe repercussions.

As an engineer has full access over the product specification, they can manipulate them to sabotage the whole production of a given product. A sabotaged product could be detected in production, but—depending on the quality controls in place—might reach the end-user. A production manager, on the other hand, can only sabotage parts of the production and might be limited by time and location. They, additionally, have the capabilities to affect the production assets (i.e., machines and materials) and workers negatively. Sabotages by a worker are limited by their direct access to the produced parts, both in time and location. A worker is the most limited when trying to sabotage a production, but also has fewer processes checking for potential problems, so the sabotage might be easier to accomplish.

Table 1. THE SCOPE AND THE GOAL OF AN ATTACK DEPEND ON A USER ROLE THE ATTACKER CAN EXPLOIT.

	Goal	
Scope	**Sabotage**	**Theft**
Engineer	whole product class	full product information
Production Manager	series of product instances, affecting assets and workers	full production information
Worker	product instances, affecting assets	partial production information

All the information an engineer, a production manager, or a worker can steal, and provide to a competing company, results in a loss of USPs. In the case of an engineer stealing, this provides the competitors the full information about a product. The production manager can provide all the information about the production, and a worker can steal individual products, which can be reverse-engineered, and parts of the production information.

4.2. Possible Attack Instantiations

Figure 2 provides a high-level overview of attacks on CPPS including integrated ICS. Attackers might target different parts of the system. They might contaminate product elements like raw materials, supplied parts, software libraries, or integrated web services. They might manipulate product and/or process specifications, production schedules, and machine controls. As discussed in the previous section, the attacks strongly depend on the role the attackers can influence. In the following, we discuss several instantiations of attacks exploiting different permissions.

Engineer. As discussed in Section 2, an engineer has a core role in the engineering process. They are responsible for developing and processing the product specification, and can gain access to all simulation data. An attacker exploiting this role might perform different sabotage attacks. They might insert any problem into the design (e.g., select "weak" materials), set up downstream roles to be vulnerable, extend control parameter intervals beyond what mechanical properties can sustain, or implement backdoors. They might manipulate customer orders (cancel/delay delivery of product parts) and influence safety systems. They might also perform different forms of theft attacks. For example, they can steal their own designs or customers personal information (contact data, payment information, product orders).

Production Manager. A production manager is responsible for production planing and control. They might perform many forms of sabotage attacks. They might let machines run out of their operational conditions by influencing their temperature. They might introduce problems into the process with corresponding quality gates (e.g., manipulate

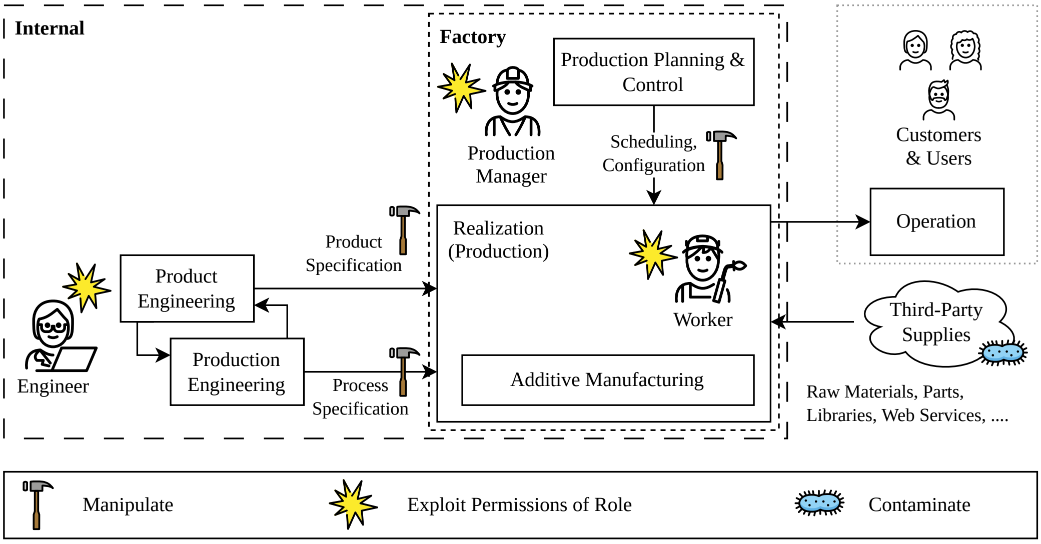

Figure 2. Perspective of the attacker on different roles/parts of the ICS.

quality gates, change machine parameters so that properties like material density are not in spec), change material composition (e.g., use too much of recycled instead of new material), or turn off security measures like multifactor authentication. They might also steal process specifications or machine configurations.

Worker. A worker is responsible for the realization of the additive manufacturing process. An attacker gaining this role might shut down their own machines or products. They might manipulate parameters of their own machines so that produced parts are out of specification. They might perform these manipulations in a stealthy way and hide quality issues in human controlled quality gates. They might also ignore mistakes in the designs, leading to product problems. When exploiting theft attacks, workers might, for example, steal the part of the design or production process that they got access to.

4.3. Attack Motivation

The related work indicates that personality types have to be considered when categorizing attacks and, specifically, anticipating the impact of attacks (cf. Section 3). Without going into the complexity of the personality profiles of the attackers, the following distinction of two fundamental attack motives seems to be useful for a further taxonomy of attack routes:

- criminal/economic (trying to make profit), and
- nasty/terroristic (intentionally destroying).

We argue that these fundamental motives can be correlated to the notions of attack goal and stealth; Table 2 shows these correlations.

Table 2. ASSUMPTIONS REGARDING THE CORRELATION OF PERSONALITY TYPES AND ATTACK GOALS/STEALTH.

	Goal	
Stealth	**Sabotage**	**Theft**
high	economic/criminal (affect rival)	economic/criminal (acquire knowledge)
low	terroristic/nasty	terroristic/nasty (extortion)

4.4. Human Factors as a Core Element of Defense-in-Depth

Defense-in-Depth requires anticipation of threats, even assuming that some attacks are missed. Focusing on secondary attacks, assuming that people act maliciously with the permissions of an internal role, Defense-in-Depth for ICS needs to consider Human Factors. The core conclusion is that "depth" in Defense-in-Depth requires a view not only on elements of the system under development, but also on humans in roles along the development path.

Generic categories of roles are introduced to determine the scope of attacks. Engineers, production managers and workers need to be granted dedicated but often high levels of access to specifications, application software, communication systems, manufacturing assets and materials. Encrypted data might be accessible on that path. Defense-in-Depth needs to consider this *scope* when analyzing potential threat scenarios and testing ICS on Defense-in-Depth compliance. The *goal* of an attack can be categorized as sabotage or theft. Combining scope and goal, the achievable impact differs significantly. While engineers cannot directly impact production, they can inject malicious content in specifications and setups. As described in Section 3, such attacks can get undetected [8], [43].

The *stealth* level highly influences the severity of attacks. For instance, while economically motivated theft attacks shall remain covert as long as possible, or until a date determined by the attacker, a terroristic attack might be conducted just to be as visible as possible. A covert attack always requires measures to hide detectable effects. Manipulating, for instance, an Additive Manufacturing (AM) machine (like presented in Figure 1) might require manipulation of quality control. Consequently, the likelihood of attacks on system elements like ICSs significantly depends, besides capabilities, on the motivation of attackers. They can be modeled as attacker profiles on the personal and organization levels, or even on specific personality types. In generic terms, a distinction can be made to economic and terroristic attacks.

To be able to holistically assess threats and defenses in the concept of Defense-in-Depth, we need to meaningfully include Human Factors in all security (safety, resilience) considerations, drawing on established Human Factors research and development practices.

5. Conclusion

Defense-in-Depth of ICSs needs to be specified in engineering, configured in production management and maintained on shop floor level. Corresponding measures need to be treated as a critical element in CPPS ensuring communication. "Depth" in the Defense-in-Depth of ICSs needs to be re-envisioned in terms of consideration of Human Factors. Threat scenarios need to incorporate goals, scope and stealth levels of attacks through or by humans. Requirements of defense measures need to cover all of these threat scenarios. That means access restrictions and authentication measures, but especially a deep analysis of interdependencies within CPPSs starting from product specifications downstream towards asset administration.

Further research needs to focus on Defense-in-Depth in design and testing of Cyber-Physical Systems and CPPS. This requires, at the same time, empirical research understanding both attack routes starting with attacker motivations and goals combined with roles in scope. Meaningful next steps are to empirically assess actors' awareness, considerations, and mitigations of the attack classes we discuss. We plan to assess past successful attacks and establish how Human Factors contributed to or enabled attacks. Together with stakeholders, we will co-develop sustainable security processes, practices, and education to better address the role of Human Factors in the Defense-in-Depth in CPPS, and empirically evaluate progress.

Acknowledgements

All emojis designed by OpenMoji – the open-source emoji and icon project. License: CC BY-SA 4.0

References

[1] Andrea F. Abate, Lucia Cimmino, Immacolata Cuomo, Mario Di Nardo, and Teresa Murino. On the Impact of Multimodal and Multisensor Biometrics in Smart Factories. *IEEE Transactions on Industrial Informatics*, 18(12):9092–9100, 2022.

[2] Klaus Abbink and Abdolkarim Sadrieh. The pleasure of being nasty. *Economics Letters*, 105(3):306–308, 2009.

[3] Mohammad Abdullah Al Faruque, Sujit Rokka Chhetri, Arquimedes Canedo, and Jiang Wan. Acoustic Side-Channel Attacks on Additive Manufacturing Systems. In *2016 ACM/IEEE 7th International Conference on Cyber-Physical Systems (ICCPS)*, pages 1–10, April 2016.

[4] Patricia Arias-Cabarcos, Christian Krupitzer, and Christian Becker. A survey on adaptive authentication. *ACM Computing Surveys (CSUR)*, 52(4):1–30, 2019.

[5] Michael C. Ashton and Kibeom Lee. Honesty-humility, the big five, and the five-factor model. *Journal of Personality*, 73:1321–1354, 2995.

[6] Andrea Atzeni, Cesare Cameroni, Shamal Faily, John Lyle, and Ivan Flechais. Here's Johnny: A Methodology for Developing Attacker Personas. In *2011 Sixth International Conference on Availability, Reliability and Security*, pages 722–727, 2011.

[7] Gary S. Becker. Crime and Punishment: An Economic Approach. *Journal of Political Economy*, 76(2):169–217, 1968.

[8] Sofia Belikovetsky, Mark Yampolskiy, Jinghui Toh, Jacob Gatlin, and Yuval Elovici. Dr0wned – Cyber-Physical Attack with Additive Manufacturing. In *11th USENIX Workshop on Offensive Technologies (WOOT 17)*, Vancouver, BC, August 2017. USENIX Association.

[9] Eric Cosman, Jim Gilsinn, Frederick Hirsch, Pierre Kobes, Ekaterina Rudina, and Ron Zahavi. IoT Security Maturity Model: 62443 Mappings for Asset Owners and Product Suppliers: An Industry IoT Consortium and ISA Whitepaper.

[10] Luis Alberto Cruz Salazar, Daria Ryashentseva, Arndt Lüder, and Birgit Vogel-Heuser. Cyber-physical production systems architecture based on multi-agent's design pattern—comparison of selected approaches mapping four agent patterns. *The International Journal of Advanced Manufacturing Technology*, 105(9):4005–4034, 2019.

[11] Cybersecurity and Infrastructure Security Agency. Alert (aa21-042a), compromise of u.s. water treatment facility, 2021.

[12] DIN Standards Committee Machine Tools. DIN 66025-1—Numerical Control of Machines, Format; General Requirements, January 1983.

[13] Quang Do, Ben Martini, and Kim-Kwang Raymond Choo. A Data Exfiltration and Remote Exploitation Attack on Consumer 3D Printers. *IEEE Transactions on Information Forensics and Security*, 11(10):2174–2186, October 2016.

[14] Ahmad E. Elhabashy, Lee J. Wells, and Jaime A. Camelio. Cyber-physical security research efforts in manufacturing – a literature review. *Procedia Manufacturing*, 34:921–931, 2019. 47th SME North American Manufacturing Research Conference, NAMRC 47, Pennsylvania, USA.

[15] David Endler. One Stolen Password Took Down The Colonial Pipeline – Is Your Business Next? *Forbes*, September 2021.

[16] Federal Office for Information Security. Industrial Control System Security: Top 10 threats and countermeasures 2022. Technical Report 005, BSI Publications on Cyber-Security, 2022.

[17] Zhiwei Gao, Aniello Castiglione, and Michele Nappi. Guest Editorial: Biometrics in Industry 4.0: Open Challenges and Future Perspectives. *IEEE Transactions on Industrial Informatics*, 18(12):9068–9071, 2022.

[18] Simson Garfinkel and Heather Richter Lipford. Usable security: History, themes, and challenges. *Synthesis Lectures on Information Security, Privacy, and Trust*, 5(2):1–124, 2014.

[19] Ian Gibson, David Rosen, and Brent Stucker. *Additive manufacturing technologies: 3D printing, rapid prototyping and direct digital manufacturing*. Springer, New York and Heidelberg and Dodrecht and London, second edition edition, 2015.

[20] Iris Gräßler. Competitive engineering in the age of industry 4.0 and beyond. In Imre Horvath, Jose Pablo Suarez Rivero, and Pedro Manuel Hernandez Castellano, editors, *Proceedings of the 12th International Symposium on Tools and Methods of Competitive Engineering (TMCE)*, pages 213–232, 2018.

[21] Iris Gräßler, Eric Bodden, Jens Pottebaum, Johannes Geismann, and Daniel Roesmann. Security-oriented fault-tolerance in systems engineering: a conceptual threat modelling approach for cyber-physical production systems. In *Advanced, Contemporary Control: Proceedings of KKA 2020—The 20th Polish Control Conference, Łódź, Poland, 2020*, pages 1458–1469. Springer, 2020.

[22] Iris Gräßler, Dominik Wiechel, and Jens Pottebaum. Role model of model-based systems engineering application. In *IOP Conference Series: Materials Science and Engineering*, volume 1097, page 012003. IOP Publishing, 2021.

[23] Sten Gruner, Mario Hoernicke, Michael Thies, Gerrit Fachinger, Nicolas Camargo Torres, and Tobias Kleinert. A Reference Architecture for Modular Industrial Automation Systems. In *2021 26th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*, pages 1–8. IEEE, 2021.

[24] Nikhil Gupta, Akash Tiwari, Satish T. S. Bukkapatnam, and Ramesh Karri. Additive manufacturing cyber-physical system: Supply chain cybersecurity and risks. *IEEE Access*, 8:47322–47333, 2020.

[25] Julie M Haney, Mary Theofanos, Yasemin Acar, and Sandra Spickard Prettyman. “We make it a big deal in the company”: Security Mindsets in Organizations that Develop Cryptographic Products. In *SOUPS@ USENIX Security Symposium*, pages 357–373, 2018.

[26] Daniel W. Heck, Isabel Thielmann, Morten Moshagen, and Benjamin E. Hilbig. Who lies? a large-scale reanalysis linking basic personality traits to unethical decision making. *Judgment and Decision Making*, 13(4):356–371, 2018.

[27] Kevin E Hemsley, E Fisher, et al. History of industrial control system cyber incidents. Technical report, Idaho National Lab.(INL), Idaho Falls, ID (United States), 2018.

[28] Avesta Hojjati, Anku Adhikari, Katarina Struckmann, Edward Chou, Thi Ngoc Tho Nguyen, Kushagra Madan, Marianne S. Winslett, Carl A. Gunter, and William P. King. Leave Your Phone at the Door: Side Channels That Reveal Factory Floor Secrets. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, CCS ’16, pages 883–894, New York, NY, USA, 2016. Association for Computing Machinery.

[29] David Jaspert, Martin Ebel, Alexej Eckhardt, and Jens Poeppelbuss. Smart retrofitting in manufacturing: A systematic review. *Journal of Cleaner Production*, 312:127555, 2021.

[30] Eric D. Knapp and Joel Thomas Langill. Risk and vulnerability assessments. In *Industrial Network Security*, pages 209–260. Elsevier, 2015.

[31] Matthew McCormack, Sanjay Chandrasekaran, Guyue Liu, Tianlong Yu, Sandra DeVincent Wolf, and Vyas Sekar. Security Analysis of Networked 3D Printers. In *2020 IEEE Security and Privacy Workshops (SPW)*, pages 118–125, May 2020.

[32] Andrew Meneely and Laurie Williams. Strengthening the Empirical Analysis of the Relationship between Linus’ Law and Software Security. In *Proceedings of the 2010 ACM-IEEE International Symposium on Empirical Software Engineering and Measurement*, ESEM ’10, New York, NY, USA, 2010. Association for Computing Machinery.

[33] Ernest H. O’Boyle Jr., Donelson R. Forsyth, George c. Banks, and Michael A. McDaniel. A Meta-Analysis of the Dark Triad and Work Behavior: A Social Exchange Perspective. *Journal of Applied Psychology*, 97(3):557–579, 2012.

[34] Dean Parsons. The State of ICS/OT Cybersecurity in 2022 and Beyond. Survey Report, October 2022.

[35] Delroy L. Paulhus and Kevin M. Williams. The Dark Triad of personality: Narcissism, Machiavellianism, and Psychopathy. *Journal of Research in Personality*, 36:556–563, 2002.

[36] Jan Luca Pletzer, Margriet Bentvelzen, Janneke K. Oostrom, and Reinout E. de Vries. A meta-analysis of the relations between personality and workplace deviance: Big Five versus HEXACO. *Journal of Vocational Behavior*, 112:369–383, 2019.

[37] Denise Ratasich, Faiq Khalid, Florian Geissler, Radu Grosu, Muhammad Shafique, and Ezio Bartocci. A roadmap toward the resilient internet of things for cyber-physical systems. *IEEE Access*, 7:13260–13283, 2019.

[38] Ken Reese, Trevor Smith, Jonathan Dutson, Jonathan Armknecht, Jacob Cameron, and Kent Seamons. A usability study of five two-factor authentication methods. In *Proceedings of the Fifteenth Symposium on Usable Privacy and Security*, 2019.

[39] Sandra L. Robinson and Rebecca J. Bennett. A Typology of Deviant Workplace Behaviors: A Multidimensional Study. *The Academy of Management Journal*, 38(2):555–572, 1995.

[40] Yonghee Shin, Andrew Meneely, Laurie Williams, and Jason A Osborne. Evaluating complexity, code churn, and developer activity metrics as indicators of software vulnerabilities. *IEEE transactions on software engineering*, 37(6):772–787, 2010.

[41] Chen Song, Feng Lin, Zhongjie Ba, Kui Ren, Chi Zhou, and Wenyao Xu. My Smartphone Knows What You Print: Exploring Smartphone-Based Side-Channel Attacks against 3D Printers. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, CCS ’16, pages 895–907, New York, NY, USA, 2016. Association for Computing Machinery.

[42] Keith Stouffer, Timothy Zimmerman, CheeYee Tang, Joshua Lubell, Jeffrey Cichonski, and John McCarthy. Cybersecurity framework manufacturing profile.

[43] Logan D. Sturm, Christopher B. Williams, Jamie A. Camelio, Jules White, and Robert Parker. Cyber-Physical Vulnerabilities in Additive Manufacturing Systems: A Case Study Attack on the .STL File with Human Subjects. *Journal of Manufacturing Systems*, 44:154–164, July 2017.

[44] Technical Committee: ISO/TC 159/SC 4 Ergonomics of human-system interaction. ISO 9241-210:2019 Ergonomics of human-system interaction — Part 210: Human-centred design for interactive systems, July 2019.

[45] Technical Committee: ISO/TC 184/SC 1 Physical device control. ISO 6983-1:2009—Automation Systems and Integration—Numerical Control of Machines—Program Format and Definitions of Address Words—Part 1: Data Format for Positioning, Line Motion and Contouring Control Systems, December 2009.

[46] Sandro Wartzack, Harald Meerkamm, Stefan Bauer, Hartmut Krehmer, Andreas Stockinger, Michael Walter, and Benjamin Schleich. Design for X (DFX). In Frank Rieg and Rolf Steinhilper, editors, *Handbuch Konstruktion*, pages 463–484. Carl Hanser Verlag GmbH & Co. KG, München, 2018.

[47] Charles Weir, Ben Hermann, and Sascha Fahl. From needs to actions to secure apps? the effect of requirements and developer practices on app security. In *29th USENIX Security Symposium*, pages 289–305, 2020.

[48] Dominik Wermke, Noah Wöhler, Jan H Klemmer, Marcel Fourné, Yasemin Acar, and Sascha Fahl. Committed to trust: A qualitative study on security & trust in open source software projects. In *2022 IEEE Symposium on Security and Privacy (SP)*, pages 1880–1896. IEEE, 2022.

[49] Mark Yampolskiy, Wayne E. King, Jacob Gatlin, Sofia Belikovetsky, Adam Brown, Anthony Skjellum, and Yuval Elovici. Security of Additive Manufacturing: Attack Taxonomy and Survey. *Additive Manufacturing*, 21:431–457, May 2018.

[50] Steven Eric Zeltmann, Nikhil Gupta, Nektarios Georgios Tsoutsos, Michail Maniatakos, Jeyavijayan Rajendran, and Ramesh Karri. Manufacturing and Security Challenges in 3D Printing. *JOM*, 68(7):1872–1881, July 2016.