Available online at www.sciencedirect.com

ScienceDirect

Procedia CIRP 52 (2016) 84 – 89

www.elsevier.com/locate/procedia

Changeable, Agile, Reconfigurable & Virtual Production

Efficiency and security of process transparency in production networks—a view of expectations, obstacles and potentials

Elisabeth Ilie-Zudor[a], Zsolt Kemény[a,*], Davy Preuveneers[b]

[a]Fraunhofer Project Center PMI, Institute for Computer Science and Control, Hungarian Academy of Sciences, Kende u. 13–17, H-1111 Budapest, Hungary
[b]iMinds–DistriNet–KU Leuven, Celestijnenlaan 200A, B-3001 Heverlee, Belgium

[*] Corresponding author. Tel.: +36-1-279-6180; fax: +36-1-466-7503. *E-mail address:* zsolt.kemeny@sztaki.mta.hu

Abstract

Much of the resilience and flexibility of production networks lies in the transparency of processes that allows timely perception of actual process states and adequate decisions or intervention at the proper point of the production system. Such degree of observability and permeability do, however, bear risks of malevolent tapping or interference with the information stream which, in the case of production systems, can put both business and physical processes at risk, requiring careful exploration of security threats in horizontal and vertical integration, and individual end-to-end connections likewise. Also, different levels of networked production present specific needs—high throughput and low time lag on the shop-floor level, or tolerances for confidence, gambling and bounded-rational views in cross-company relations—that may conflict with security policies. The paper presents a systematic summary of such apparently contradicting preferences, and possible approaches of reconciliation currently perceived to be relevant on various abstraction levels of production networks.

Peer-review under responsibility of the scientific committee of the Changeable, Agile, Reconfigurable & Virtual Production Conference 2016
Keywords: Production networks; process transparency; security; performance

1. Introduction

The past 1–2 decades have been marked by changes in industrial production that can be attributed to the mutually amplified tendencies of (1) changing consumer demands and environmental impact regulations requiring more effort and faster adaptation, and (2) the ability of the industry—at least, in a technical perspective—to address these evolving challenges. On one hand, industrial production is, nowadays, required to be more responsive to the diversity of demands (i. e., various degrees of customization and additional services tailored to the individual customer) and their quick changes (requiring tighter development and lead times and more adaptivity). On the other hand, efficient use of resources is gaining importance in view of competitive pressure and more stringent environmental regulations.

Dynamically changing production networks—as opposed to fixed supply chains, often centered around a single "major player" determining long-term roles—proved to be a feasible way of tackling the aforementioned challenges. Here, participants of varying size, expertise and production capacities engage in collaboration, often on a project-by-project basis, to meet the perceived demands—not excluding the possibility of simultaneously acting as competitors in connection with another production order. The emergence of such product development and production structures is, to a decisive degree, owing to greatly improved process transparency in design, production and logistics, with observations or sharing transactions often crossing both corporate and technological borders. This trend is individible from the development of theoretical foundations and applicable technologies putting the observability to use, often mentioned among characteristics of a "fourth industrial revolution" [1–4]. The most significant of these are advances in handling "big data" and extracting useful high-level information from large amounts of low-level and unstructured data, modeling of processes and corresponding measures of prediction and control, planning of mostly discrete and structured aspects of production (e. g., scheduling and assignment problems), negotiation and contract mechanisms with formal guarantees, and support for various forms of human involvement (most significantly, decision support and human-comprehensible (re)presentation of underlying knowledge).

Such degree of process transparency and precise intervention requires much more data to be collected, communicated and stored than it was typical in earlier industrial practice, and both the amount and the potential propagation of production-related information present new challenges. Aside from inter-

Peer-review under responsibility of the scientific committee of the Changeable, Agile, Reconfigurable & Virtual Production Conference 2016
doi:10.1016/j.procir.2016.07.018

operability problems arising from the heterogeneous nature of production networks, security and performance limits are the two focal areas of concern. The paper gives a state-of-practice review on problems and solutions applicable to production networks. The remainder of this paper is structured as follows. In section 2, we discuss common threats, countermeasures, and limitations of state-of-practice security solutions. Section 3 reviews contemporary solutions and trade-offs. We conclude in section 4 summarizing our main insights and identifying interesting topics for further research. The areas of problems, limitations and solutions reviewed in the paper are also summarized in Figure 1.

2. Focal problems in production networks

As recent attacks on SCADA systems by dangerous malware like Stuxnet, Duqu, Flame, and Gauss [5,6] have shown, cybersecurity is a growing concern for production networks, as many of the manufacturing systems in operation today were never designed with networked production and large-scale machine-to-machine connectivity in mind. This section reviews common threats, countermeasures, and limitations of state-of-practice solutions to secure production networks.

2.1. Common threats in networked production systems

Security threats and countermeasures in networked production systems cover two areas of concern [7], i. e., (1) *system security* to protect the organization's networks, software systems and physical production facilities from disruption and denial-of-service attacks, and (2) *information security* which deals with defending information from unauthorized access, use, disclosure, tampering or destruction. With process transparency in networked production as an emerging trend, the latter becomes far more important and challenging.

Intercepting and injecting of information. An important security threat deals with unauthorized access to information, either through (1) circumventing authentication by spoofing one's identity using a legitimate user's authentication credentials, or (2) sidestepping access control with an *elevation of privilege* attack where an unauthorized user (legitimate employee or attacker) penetrates all system defenses to gain access to or alter confidential information. Such attacks can take place on data *at rest* in a database (e. g., with an SQL injection attack [8]) or on data *in transit* between two network production facilities with an adversary executing a Man-In-The-Middle (MITM) attack (e. g., an SSL strip attack [9]).

With Cyber-Physical Systems gaining importance in networked production, the attack surface grows with ample opportunities for an intruder not only to collect information from a particular device or sensor, but also as a way to break into a single node and move laterally across the trusted production network [10] in order to tap into even more sensitive information on customers, suppliers and commercial strategies [11]. Disruption of physical processes by taking control of actuators or manipulating sensor data is also becoming an area of concern in CPS [12–14].

Aggregation and inference attacks. Production transparency is a key feature of Industry 4.0 [15]. Production assets will create data that can be tracked, collected, and analyzed in real-time across the organizational boundaries of the company. Hence, there is the inherent risk of losing control over information shared with partners in the value chain, and how they might use and share that data [7] with competitors.

Beyond information security threats in such business-to-business scenarios, there are also privacy concerns for the customer. With just-in-time individualized production and manufacturing, it is likely that the undesirable information disclosure threats due to inference attacks in social networks [16] will emerge in production networks as well. We expect that key obligations of the upcoming EU General Data Protection Regulation (GDPR) and technical compliance with such regulatory frameworks [17] will have a significant impact on networked production.

Human decisions and social engineering. User behavior has often been identified as playing a major role in security failures, and that is why humans are usually considered the weakest link in the security chain [18]. According to research from security software firm Trend Micro [19], more than 90% of cyberattacks begin with a *spear phishing* email, a form of phishing that uses information about the target to make the attack more specific and personal. Recent work by Krombholz [20] provides a taxonomy of well-known social engineering attacks.

While human behavior is often the weakest point in withholding confidential information, it can also become a barrier to disclosing information that is beneficial to be shared—both on the level of individual sharing decisions, and in setting up sharing policies. This can be the result of a limited horizon of knowledge regarding information handling processes in the production network [21], effecting that transparency is maintained in a limited range of participants only [22], or gambling behavior is practised that deteriorates the overall efficiency of cooperation [23,24].

2.2. Limits of countermeasures

Network intrusion detection systems and firewalls are frequently used to detect a variety of malicious access patterns and threats. Such countermeasures usually operate at the edge of the organization's network, and are sufficient to mitigate simple security attacks. With networked production, the trust boundaries of the organization's network continuously change, demanding for more dynamic solutions where access control is pushed towards all elements in the production network. Nayak *et al.* [25] proposed Reasonance, a system for securing enterprise networks where the elements in the network enforce dynamic access control policies based on both flow-level information and real-time alerts managed by OpenFlow [26] enabled switches. Much more challenging are *advanced persistent threats* (APT) [27] where the objective of the intruder is to achieve ongoing access without being detected. Such attacks make use of sophisticated evasion techniques, malware and other backdoors. They are usually not conducted to disrupt the service and therefore more difficult to detect. Mitigating such threats require sophisticated anomaly detection algorithms to identify unexpected information flows.

Application-level weaknesses have been the cause of many data breaches. For data *at rest*, encrypted databases [28] have been proposed to handle SQL queries over encrypted data.