Available online at www.sciencedirect.com

ScienceDirect

IFAC Papers Online
CONFERENCE PAPER ARCHIVE

IFAC-PapersOnLine 49-29 (2016) 133–137

Developing and Operating Industrial Security Services to Mitigate Risks of Digitalization

Dr.-Ing. Dipl.-Phys. Christoph Jansen *

**Siemens AG, Digital Factory Division, Erlangen, Germany*
(Tel: +49/9131/7-33919; e-mail: christoph.jansen@siemens.com).

Abstract: Managers of industrial facilities have to handle the transition to digitalization of their sites: They have to leverage the potentials of digitalization to ensure their competitiveness, but at the same time they have to handle the complexity that comes along with Industry 4.0 in diverse dimensions. This article describes major drivers of this complexity to outline the environment of today's challenges for managers of this technical transition – and shows how Industrial Security Services can contribute to stabilize the industrial system.

Keywords: Industrial Cyber Security, IT-Security, Digitalization, Industry, Managed Services, DevOps, Cyber-Security Operation Center, Resilience, MSSP.

1. INTRODUCTION

1.1 Digitalization in industrial environments

Advantages of digitalization have been widely discussed to improve productivity of industrial sites and hence competitiveness of the industrial player.

Huber (2013) describes that Industry 4.0 is addressing the merging of modern information and software technology on the one hand with classical industrial processes on the other hand, including the consequences of this change for industry to remain competitive. This merging has its conceptual roots in the Cyber-Physical Systems (CPS), consisting of two major components: a physical process and a cyber system. The aim of a CPS is to monitor the behaviour of physical processes, and actuating actions to change its behaviour in order to operate and improve the physical process as Wan et al. (2010) point out. The cyber system comprises of networked devices with sensing, computing, and communication capabilities.

In consequence, as the degree of connectivity increases exponentially, the physical systems become increasingly more susceptible to security vulnerabilities in the cyber system. Accordingly, a number of severe security incidents have become publicly known:

- a hack of an air traffic control mission support system that has been described by Mills (2009),
- a hack of medical devices implanted in human body that has been reported by Leavitt (2010),
- a penetration of power systems, resulting in power outages, as revealed by O'Connell (2008),
- a demonstration of a software tool that disables a car engine and breaking system remotely, described by Koscher et al. (2010), and
- a virus that infected the SCADA system of a nuclear production facility, as documented by Fuhrmans (2010) or Karnouskos (2011).

The latest societally relevant consequence is, that NATO has declared cyberspace as a genuine frontier for war.

1.2 Cyber threats and protection concepts for industrial environments

Operating industrial sites becomes more vulnerable if highly connected Cyber-Physical Systems are not applied properly to industrial facilities. Hence, manifold initiatives have been taken by national governments like the German "IT-Sicherheitsgesetz" to give guidance to operators of critical infrastructures (BSI 2014). Critical infrastructures contain industries such as: Food & Beverages or Water & Wastewater.

Table 1. Threat landscape for industry (not-complete).

Attack	Example
Targeted attack to automation system	Buffer overflow in file parsing function
	USB stick with malicious SW is (accidentally) used
Attack via internet on decentral control system	Wrong firewall configuration
	SQL injection
Unauthorized access from office to production network	No host-based access restrictions configured
	Wrong firewall configuration

2405-8963 © 2016, IFAC (International Federation of Automatic Control) Hosting by Elsevier Ltd. All rights reserved.
Peer review under responsibility of International Federation of Automatic Control.
10.1016/j.ifacol.2016.11.076

Malicious reconfiguration via remote access	Weak passwords
	Privilege escalation
	No detection mechanisms for manipulations
Disruption of machine to machine communication (PROFINET)	Malware infection
	Buffer overflow leads to crash of communication stack
	Hacker device is placed in network

Table 1 gives a non-complete overview of cyber threats for industrial facilities.

Protection concepts for industrial sites have to take three dimensions into account: The technological measures, organizational measures and human-centred measure. The international standard IEC /ISA-62443 incorporates these measures as part of defence-in-depth (s. Fig. 1) as a multi-layer approach for securing industrial automation and control systems. This concept demands security controls at plant, network, and system level.

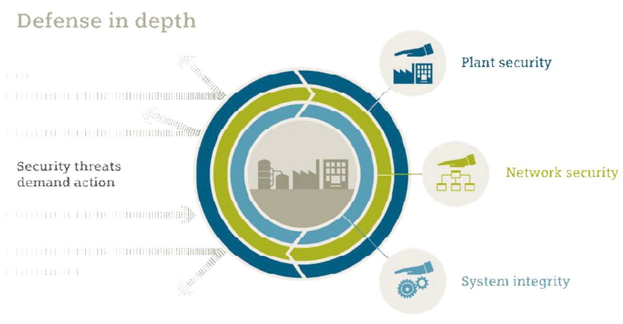

Fig. 1. Defence-in-depth.

Plant security uses various methods to secure physical access to critical components through doors, code cards etc.. This is typically subject to guidelines and processes, incl. cyclic risk assessments, implementation of appropriate security controls and continuous monitoring of the identified measures.

Network security has the aim to protect production networks from unauthorized access at the connections to other networks like the internet or the office environment of the plant. Segmentation of individual subnets in zones and conduits ("secure cells") provides additional security. Transfer of data between different subnets and secure cells has to be managed properly. Typical security controls are demilitarized zones, separating the plant IT through a perimeter firewall from the internet and managing the data traffic between DMZ and the automation network through an internal firewall.

System integrity includes the protection of automation systems and controls at device level against unauthorized access as well as the protection of the information they contain through hardening of the systems. It entails a user authentication and access management to automation and IT systems.

Technical concepts for securing industrial automation and control systems ICS are available to protect industrial sites with regard to availability of the production, integrity of data and the confidentiality of critical data on e.g. the product or customers. An example of good-practise covering state of the art security requirements is the security annex to the documentation of the process control system PCS7 and WinCC SCADA system (Siemens, 2008). This documentation is continuously updated by the current threat situation.

2. CHALLENGES OF NEW COMPLEXITY

However, these concepts are in practise quite often not properly applied. Especially the availability of connectivity features of Cyber-Physical Systems brings a broad variety of connectivity advantages (s. Colombo et al., 2014) – and risks (s. Geisberger and Broy, 2012) – with them. The security principle of need-to-connect between different secure cells or between components of the production network and outbound devices is quite often disregarded.

An important design principle related to protecting industrial plants is to segregate the underlying network into secure cells that contain assets of comparable criticality. These secure cells should only have interfaces to other logically separated secure cells following the need-to-connect principle. Secure cells of different protection levels should obviously never be connected.

One intention of a CPS is to achieve autonomous functionality. The interoperability of a CPS introduces new complexity in the security design of the system. A CPS, which normally operates autonomously in regular operating mode, may require interoperability with other CPSs or command and control centres when in emergency mode. Traditional secure communication solutions are not designed for inter-operation among heterogeneous applications. It is crucial for the design of CPS to ensure security while the cyber system is interacting with another one or while communication between the physical and the cyber system is taking place. Hu et al. (2016) distinguish *monitoring security* (from physical objects to cyber objects) and *control security* (from cyber objects to physical objects) as core activities of cyber-physical interaction security.

It is quite obvious that security becomes essential for the design of CPS in industrial environments. A CPS should be resilient to both natural faults and malicious attacks. The predominant protection targets for CPSs are availability, integrity, and confidentiality.

Availability refers to the ability of a system to be accessible and usable on demand. Lack of availability results in denial of service at the cyber system and might result in a lack of productivity at the physical system. The real-time constraints of CPSs introduce additional challenges. The goal of availability in CPSs is therefore to maintain the operational goals by preventing or surviving Denial-of-Service attacks to