Proven knowledge in new industrial security specifications

Functional safety components protect workers against hazards to their life and health, for example by preventing access to hazardous parts of machinery and systems. Manipulation from outside that could adversely affect safety must also be prevented. This requires thorough observance of generally accepted good practice, and an appropriate response by manufacturers and operators in the event of security exploits.

In order for the safety functions of control systems to be reliably assured, the control system itself must also be both secure, i.e. protected against failure and manipulation. The increasing frequency with which industrial security disasters are now being reported is alarming. There are however grounds for optimism, because almost all security vulnerabilities can in fact be avoided very easily by observance of current good practice, as the following pertinent example shows.

As long ago as 1883, Auguste Kerckhoffs set out six basic requirements for secure, i.e. confidential communication. The second of these requirements was that the system should not require secrecy, and if it were to fall into enemy hands, no adverse consequences should arise. Guglielmo Marconi was evidently not aware of Kerckhoffs' document: secure (confidential) communication by means of his wireless telegraph system depended upon other parties not taking possession of one of the devices or replicating one of them and tuning it to the same frequency. Nevil Maskelyne drew attention to the problem in 1903 by transmitting obscene Morse code messages during Marconi's demonstration, thereby making him one of the first ever hackers. Although secure cryptographic methods are not new, design flaws similar to Marconi's can still be found today, for example in radio controls for traffic light systems[1] or industrial cranes[2].

Harmonized definitions of concepts are lacking

The University of Bremen's navigator for security-related standards[3] includes a database of currently around 800 standards and over 2,000 search hits for legislation. One problem is that the documents use different terms, and do not always define them clearly. While some documents deal comprehensively with security, and specifically with information security, others invent new portmanteau terms beginning with "cyber". These newly created terms must be defined precisely in the document, as they do not have a unique inherent meaning. "Cybersecurity" may refer to an activity, or to a measure taken to protect against attacks from the Internet; at other times it refers to a state in which a product is protected against radio-based attacks.

A better alternative to creating new terms is to work with the unambiguous terms "security" or "information security". Where the term's scope must be limited to radio-based attacks, for example, this restriction should be stated clearly. The EU Machinery Directive has chosen another, very elegant solution by requiring "protection against corruption"[6] in Annex III 1.1.9, and is also clearer on this point than the previous EU Machinery Directive. With this approach, it focuses on the objective of protection, for example that remote access must not lead to a hazardous situation. It does not address in detail how such corruption may be caused.

Fast communication is crucial

Fast and effective communication is a crucial part of an appropriate response to security vulnerabilities. However, the poor state of communication was demonstrated in December 2021, when a security vulnerability in the Log4J software library made headlines. This software library forms part of many industrial components, as well as many server services. Whilst some were blaming incorrect use of the library and arguing that the security issues could have been prevented had the documentation been read, many manufacturers were left wondering whether they were affected by security vulnerabilities. In some cases, they were not able to establish whether their products were affected until several months later.

In summary, the following were lacking:

- An emergency contact point for security within the company
- A standardized format for recommendations for action

Jonas Stein

Head of the DGUV's industrial security laboratory and Head of the DGUV security working group

Jonas.Stein@dguv.de

• In addition, a standard procedure for manufacturers to communicate that a particular product is not affected by a security vulnerability

The lack of harmonized information and interfaces is addressed by a catalogue of open specifications, developed by various consortia of companies, public bodies and organizations, that can be implemented immediately by any company (see table). An emergency contact point according to IETF specification RFC 9116 is stored on the website in a simple security.txt file[4]. A manufacturer can also refer in this file to his list of recommended actions (CSAF). A globally unique identifier (CPE, common platform enumeration) is assigned to each hardware and software product. This enables the international alerts (CVE, common vulnerabilities and exposures) to be referenced automatically to the precise product and version. The criticality of the security vulnerability is classified as closely as possible against a globally standardized index (CVSS, common vulnerability scoring system). The SPDX open specification[9] can be used to document, in machine-readable form, what libraries were used for each project. A program used by the operator can then regularly query for all products whether any security alerts have been issued, and display the recommended actions.

Some large companies are already employing these specifications. It is now crucial that all other companies swiftly follow suit, so that information on security problems is delivered quickly and at low cost.

As a first step, companies should at least ensure that they can be contacted in the event of a security incident, and make an emergency contact public. Instructions are provided at https://cert.dguv.de by which this can be implemented in a matter of minutes.

Open specifications on information security

Input information	Maintained by	Specification
Emergency contact point	Manufacturer, operator	"security.txt" RFC 9116
Product identifier/ID (manufacturer's name, product name, version, language version, etc.)	Manufacturer	CPE
Software bill of materials (SBOM)	Manufacturer	SPDX
Security vulnerability alert	CVE numbering authorities	CVE
Security advisory (recommended action for CVE)	Manufacturer	CSAF
Properties for criticality evaluation	Manufacturer	CVSS

Catalogue of open specifications; together, these will substantially enhance industrial security. In the years ahead, they will step up the urgently needed communication of security vulnerabilities.

1 ARD TV report on hackers switching traffic lights in Hannover to green (2021), https://ardmediathek.de Hacker Ampeln
2 Andersen et al, 2019, A Security Analysis of Radio Remote Controllers for Industrial Applications https://documents.trendmicro.com/assets/white_papers/wp-a-security-analysis-of-radio-remote-controllers.pdf
3 https://cybersecurity-navigator.de
4 Critical security vulnerabilities on machinery and installations, and the security.txt file: https://cert.dguv.de