CHAPTER 13

Cybersecurity in IEC 61508:2010 and IEC 61511:2016

The general standard for functional safety of systems involving E/E/PE systems is IEC 61508:2010 [1]. A so-called sector-specific "derived" standard for process plants, which involve E/E/PE-based industrial automation and control systems (IACS) is IEC 61511:2016 [2]. Recently, the cybersecurity properties and possible vulnerabilities of such safety-related systems have come into question, as some have been cyberattacked and organisations and governments attempt to secure important infrastructure against such cyberattack. I lay out here explicitly the clauses in these two widely-applicable international industrial standards. I suggest they do not suffice to protect against cybersecurity vulnerabilities that have been exhibited "in the wild" in nuclear power plants, as reported by Chatham House [1]. I conclude there is an urgent need for supplementary measures to eliminate the most common cybersecurity vulnerabilities in critical-infrastructure systems. Such need has been addressed by recent UK HSE guidance [1].

13.1 The Need

IEC 61508:2010 is a general standard for functional safety of systems with electrical/electronic/programmable electronic (E/E/PE) components [1]. It consists of seven parts, of which the first three are normative. The first part is general, the second concerns electronic/programmable electronic hardware and systems, and the third part concerns itself with software and its development. IEC 61508 does not cover commercial aviation or medical systems. De facto, it does not cover railways, which

have their own set of functional safety standards developed through the European Union standardisation organisation CEN and its electrotechnical part CENELEC; nor does it cover road-automotive applications, which are currently developed through ISO, However, both the rail E/E/PE functional-safety standards and those for automotive applications are notionally written as an adaptation of the processes enunciated in IEC 61508 to their specific sectors.

IEC 61511:2016 is a functional safety standard for E/E/PE-based industrial automation and control systems (IACS) in process plant which is explicitly derived from IEC 61508 [2]. Many of the developers of IEC 61511 on the IEC committee are also developers of IEC 61508. IEC 61511 includes specific measures to be applied to basic process control systems (BPCS) and also safety-instrumented systems (SIS), which are subsystems specifically intended to assure the appropriate level of safety during plant operations. Software involved in BPCS and SIS is explicitly governed by IEC 61508-3 (the third part of IEC 61508) according to IEC 61511.

13.2 The Approach to Safety

These two IEC standards approach system safety in a similar way. They are guided by ISO/IEC Guide 51, which provides general guidance as to how system safety issues are to be addressed in international standards in which they are relevant [3]. Hazard identification, a risk analysis and then a risk assessment is to be performed, and risk reduction must be undertaken if the actual risk is unacceptable. The steps in Guide 51 are:

Hazard Identification: A hazard is a "potential source of harm" (IEC 61508-4:2010), where harm is "physical injury or damage to the health of people or damage to property or the environment" (ibid.) Hazards are normally thought of as situations which are precursors to harm. Situations are often states, but can also be events.

Risk Analysis: The severity of a hazard is assessed, that is, the worst case of harm which can arise through a hazard. Then the likelihood of the hazard occurring, along with the the likelihood that the severity will actually result from the occurrence of the hazard, is estimated. (What is actually wanted is the expectation of loss, as it is known in statistics. It is often hard or impossible to

distribute the loss across the range of possible outcomes, and so the worst case is taken in engineering as a conservative estimate of outcome.)

Risk Assessment: The calculated risk is evaluated against the acceptable risk, and if it is higher, then.....

Risk Reduction: Measures must be introduced into the system to reduce the risk to an acceptable level. Risk reduction measures in IEC 61508 and related standards involve

Redesign: to avoid as much of the risk as possible. The introduction of so-called safety functions, functions introduced explicitly to mitigate the hazard and/or its effects.

It is not my purpose here to discuss this way of categorising risk and risk reduction measures. It is what is currently required in all ISO or IEC international standards related to safety, as per Guide 51.

Malicious intrusion into an IACS, either human or malware (malicious software), can

induce hazards For example, by inducing or allowing more reactants into a reactor whose reaction is chemically exothermic, the temperature of the reactor could be raised to a hazardous level.

elevate the frequency of hazards The acceptability of the risk of a specific hazard is based on an estimate of how frequently it occurs. Such estimates are often based on experience. For example, let us say it is expected on the basis of experience that the temperature in the above reactor will not be elevated more than once a year. If it is elevated daily by malicious interference, then the functional life of the reactor and its materials may well be shortened in such a way as to invalidate the existing safety analysis.

inhibit the proper operation of safety functions Say that a safety function has been built into the system which reacts to an elevated temperature by shutting off reactant ingress into the reactor, and opening reactor vents to allow the reaction product to expand into a larger space, thereby reducing pressure in the reactor. The safety function has been implemented by an E/E/PE system whose

inputs are temperature sensors and outputs are actuation command to shut off inflow and open the overflow vent. A malicious actor (a person or malware) could intervene by inhibiting the sensor inputs, or by changing the execution of the safety function so that not all necessary actions are taken.

Cybersecurity measures may be necessary to prevent any of the above phenomena occurring. Thus cybersecurity is an important component in assuring functional safety. Let us now see what cybersecurity measures are in fact required by current standards.

13.3 Cybersecurity in IEC 61508

The clauses in IEC 61508:2010 which mention cybersecurity are enumerated below

IEC 61508-1: 2010 Clause 1 Scope Subclause 1.2

In particular, this standard

.....

m) does not specify the requirements for the development, implementation, maintenance and/or operation of security policies or security services needed to meet a security policy that may be required by the E/E/PE safety-related system;

Subclause 7.4 Hazard and Risk Analysis Subclause 7.4.2.3

The hazards, hazardous events and hazardous situations of the EUC and the EUC control system shall be determined under all reasonably foreseeable circumstances (including fault conditions, reasonably foreseeable misuse and malevolent or unauthorised action). This shall include all relevant human factor issues, and shall give particular attention to abnormal or infrequent modes of operation of the EUC. If the hazard analysis identifies that malevolent or unauthorised action, constituting a security threat, as being reasonably foreseeable, then a security threats analysis should be carried out.

NOTE 1 For reasonably foreseeable misuse see 3.1.14 of IEC 61508-4.

NOTE 2 For guidance on hazard identification including guidance on representation and analysis of human factor issues, see reference [11] in the bibliography.
NOTE 3 For guidance on security risks analysis, see IEC 62443 series.
NOTE 4 Malevolent or unauthorised action covers security threats.
NOTE 5 The hazard and risk analysis should also consider whether the activation of a safety function due to a demand or spurious action will give rise to a new hazard. In such a situation it may be necessary to develop a new safety function in order to deal with this hazard.

Subclause 7.5 Overall safety requirements Subclause 7.5.2.2

If security threats have been identified, then a vulnerability analysis should be undertaken in order to specify security requirements.
NOTE Guidance is given in IEC 62443 series.

IEC 61508-2:2010 There are no clauses mentioning security.

IEC 61508-3:2010 In Annex D: Safety manual for compliant items – additional requirements for software elements

D.2.4 The following shall be included in the safety manual:
.....
m) Details of any security measures that may have been implemented against listed threats and vulnerabilities.
.....

In IEC 61508:2010 Parts 4-7 These parts of the standard are not relevant for our purposes because they are informative, not normative.

13.4 Cybersecurity in IEC 61511

In IEC 61511-1;2016 Subclause 8.2.4

A security risk assessment shall be carried out to identify the security vulnerabilities of the SIS. It shall result in:

- *a description of the devices covered by this risk assessment (e.g., SIS, BPCS or any other device connected to the SIS);*
- *a description of identified threats that could exploit vulnerabilities and result in security events (including intentional attacks on the hardware, application programs and related software, as well as unintended events resulting from human error);*
- *a description of the potential consequences resulting from the security events and the likelihood of these events occurring;*
- *consideration of various phases such as design, implementation, commissioning, operation, and maintenance; the determination of requirements for additional risk reduction;*
- *a description of, or references to information on, the measures taken to reduce or remove the threats.*

NOTE 1 Guidance related to SIS security is provided in ISA TR84.00.09, ISO/IEC 27001:2013, and IEC 62443-2-1:2010.
NOTE 2 The information and control of boundary conditions needed for the security risk assessment are typically with owner/operating company of a facility, not with the supplier. Where this is the case, the obligation to comply with 8.2.4 can be with the owner/operating company of the facility.
NOTE 3 The SIS security risk assessment can be included in an overall process automation security risk assessment.
NOTE 4 The SIS security risk assessment can range in focus from an individual SIF to all SISs within a company.

Subclause 11.2.12

The design of the SIS shall be such that it provides the necessary resilience against the identified security risks (see 8.2.4).
NOTE Guidance related to SIS security is provided in ISA TR84.00.09 and IEC 62443-2-1:2010.

Subclause 11.7.3.2

The maintenance/engineering interface shall provide the following functions with access security protection to each:

- *SIS mode of operation, program, data, means of disabling alarm communication, test, bypass, maintenance;*
- *SIS diagnostic, voting and fault handling services;*
- *add, delete, or modify application program;*
- *data necessary to troubleshoot the SIS;*
- *where bypasses are required they should be installed such that alarms and manual shutdown facilities are not disabled.*

Subclause 11.7.3.4

Enabling and disabling the read-write access shall be carried out only by a configuration management process using the maintenance/engineering interface with appropriate documentation and security measures such as authentication and user secure channels.

Subclause 11.8.6

Forcing of inputs and outputs in PE SIS shall not be used as a part of application program(s), operating procedure(s) and maintenance (except as noted below).
Forcing of inputs and outputs without taking the SIS out of service shall not be allowed unless supplemented by procedures and access security. Any such forcing shall be announced or set off an alarm, as appropriate.

Subclause 12.4.2

The following information shall be contained in the application program or related documentation:
.....
k) If required by the SRS, the means by which:

- *the correctness of field data is ensured, (e.g., comparison between analog sensors to improve the diagnostic coverage);*
- *the correctness of data sent over a communication link is ensured*

(e.g., when communicating from an HMI, before implementation of a command an 'ack' or 'acknowledge' is transmitted);

- *communications are made secure (e.g., cyber security measures)*
- *.....*

13.5 Cybersecurity in IEC 61511-2, Guidelines for the application of IEC 61511-1

There is included a fair amount of material about access security for SIS access and BPCS access. Additionally, consideration is given to separation between the two types of system for security reasons. Annex F works through an example:

F.22 Security

The security measures taken with respect to the SIS design maintain safety integrity by preventing unauthorized or inadvertent modification of any of the SIS functions or devices including the logic solver, the application logic, the user interfaces, sensors and final elements. For those devices (e.g., interface devices) where it is more difficult to control physical access, the use of administrative procedures should be implemented. Some basic security approaches implemented were:

- *written approval with reasons for access;*
- *written approval with persons requiring access identified;*
- *definition of required training and/or familiarity with the system before access is permitted;*
- *definition of who is to have access to the system, under what circumstances, and to perform what work. This included the procedures needed to control the use of maintenance bypasses.*
- *SIS features that facilitate access control. Examples of such design features include:*
  - *clear identification of SIS devices via distinctively colored labels;*
  - *physical separation of SIS and BPCS equipment (making it easier to secure the associated enclosures with key-locks);*

  - *use of a diverse technology (which would typically require a different maintenance interface).*

The use of PES based SIS introduced additional security concerns because of the relative ease of making changes in the application logic. For these systems, additional features were implemented including:

- *restricting access to the maintenance/engineering interface;*
- *establishing administrative policies/procedures that define the conditions under which the maintenance interface may be connected to the system during normal operation;*
- *use of virus checking software and appropriate program and file handling procedures in the engineering console to help avoid corruption of the embedded and/or application logic;*
- *the use of SIS utility software that tracks revisions in the application logic and allows the determination (after the fact) of when a change was made, who made the change, and what the change consisted of;*
- *no external connections of the SIS or BPCS to the internet or phone lines.*

13.6 Cybersecurity-related Events Recorded by Chatham House

The UK Royal Institute for International Affairs, known as Chatham House from the London buidling in which it is housed, published a report in October 2015 on actual cybersecurity vulnerabilities in the operation of nuclear power plants [1]. The investigators recorded inter alia the following security vulnerabilities (elaborations are mine):

- NPP operators plugging their iPhones and tablet computers into USB ports in the control room to charge them. If such ports were connected to the ICAS, malware on such devices could thus enter the IACS.

- Remote maintenance activity loading malware through a virtual private network (VPN). This happened in 1992. A maintenance contractor working from a remote location had some malware on the computer he was using to perform

system software maintenance, and the malware was loaded into the IACS during his activity. The care with which the VPN was designed and constructed aided rather than hindered this intrusion.

- Insiders introducing malware (deliberately or inadvertently). The "insider" threat, nominally authorised employees of the operator deliberately attempting to cause harm, is considered by cybersecurity experts to be one of the greatest.

- Connectivity between business systems and control systems affecting control. It is generally regarded as good practice to separate control systems from the computer systems within which the everyday business of the operator is conducted – logging employees in and out, scheduling shifts and so on. However, it is also often regarded as convenient to establish electronic connections between databases containing business information, such as which employee is on which shift, and control systems, say to allow the employee to authenticate himherself to the control system only when heshe is scheduled for a shift. Establishing such connectivity, though, allows an intruder into the business system, typically less well protected, or even a business employee not authorised for control, electronic access to the IACS.

- SCADA. Supervisory control and data acquisition systems (SCADA) are pervasive in the process industries. Data on the actual operation of the system, say part of the electricity grid, are gathered automatically and sent remotely, say, to a general monitoring organisation which maintains a picture of the state of the grid generated from the various suppliers and users. Such SCADA systems are often built upon Internet protocols and use the Internet as a physical transfer network. Such protocols mostly allow two-way communication, and may well have known vulnerabilities. Such vulnerabilities may allow intruders to gain access to the network from outside, "reversing" the data path of usual operation, as it were. One way of protecting against this is to use "data diodes", typically glass-fiber systems with the data generated by lasers on one end and read at the other. It is physically impossible for any data to be transmitted in the reverse direction, hence the nickname "data diode".

- Off-the-shelf E/E/PE systems, known as COTS, often replace older mechanical/electrical systems which have exhausted their useful life. Such COTS

replacements are not necessarily completely secure, in particular if they were not originally specifically developed for critical operations, and may bring with them vulnerabilities which may be exploited by cyberattackers.

- "Air gaps" aren't. An "air-gapped" network is one which is physically not connected to any other digital computer network. It is popularly supposed that it is not vulnerable to intrusion from outside; that someone must physically break in in order to misuse the network. The weakness of such suppositions was shown clearly by the Stuxnet episode in 2010, whereby malware was introduced into a carefully-guarded nuclear-centrifuge facility in Iran, apparently without physical intrusion of personnel. It is supposed that the malware was loaded onto a USB stick that was left somewhere where authorised personnel might pick it up and plug it into a port to see what was on the stick (a so-called "trojan horse" attack). This is known as a "parking lot" attack, after an early incident where intruders distributed such trojan-horse USB sticks around the parking lot of the organisation whose network they wished to infiltrate.

- Undocumented Internet connections. There are, unfortunately, plenty of these in complex networks. They should not be there, but they are.

- Compromised SW updates. Software releases which "update" software on IACS are supposed to be thoroughly checked, authorised, signed and so on. However, occasionally they inadvertently contain malware.

- Default passwords left in place on COTS. One of the most common vulnerabilities is the use of common off-the-shelf devices, such as home Internet routers, without changing the default administrative passwords programmed on the devices at the factory. This also happens at critical facilities, and with devices that are attached to networks which have safety-critical functions. It should not, but it does.

13.7 Effectiveness of Cybersecurity Measures in IEC 61508 and IEC 61511

It is left to the reader as an exercise to determine in detail that the cybersecurity measures currently required in IEC 61508:2010 and IEC 61511:2016 do not suffice to eliminate any of the vulnerabilities mentioned above. I observe that IEC 61508 does not require any specific actions to enhance or ensure cybersecurity. It requires a "security threats analysis", respectively a "vulnerability analysis", respectively something to be written in the safety manual if something has been done. IEC 61511 requires access control to sensitive systems. However, there is no guidance as to who should be allowed access. The plant's private security service, for example? To some people, that might be reasonable – they are entrusted with physical security. To others, unreasonable. Security-employee physical behaviour can be controlled by patrolling in pairs. However, if one employee is typing at a keyboard, the other cannot necessarily see what heshe may be doing. The overt control through operating in pairs is not there in this case.

13.8 Guidance on Cybersecurity Measures in Safety-Related Systems

The UK Health and Safety Executive, the regulator of general safety in industrial plants, has recently published detailed guidance on cybersecurity measures in IACS [1]. This guidance is very specific, telling users how to deal with vulnerabilities associated with specific devices.

More general, abstract guidance is given by the German VDE in their "application rule", a category to be thought of as preceding a standard [7]. This guidance is enunciated in the form of principles and categories of protection, along with consideration of conflicts ("interference") between the goals of various categories.

Guidance on functional safety and cybersecurity was issued by the International Society for Automation, ISA, in 2013 and the second edition is now available [6].

Bibliography

[1] Caroline Baylon, Roger Brunt and David Livingstone, *Cyber Security at Civil Nuclear Facilities: Understanding the Risks*. The Royal Institute of International Affairs (Chatham House), October 2015. Available from https://www.chathamhouse.org/publication/cyber-security-civil-nuclear-facilities-understanding-risks , accessed 2015-05-23.

[2] UK Health and Safety Executive, *Cyber Security for Industrial Automation and Control Systems (IACS)*, March 2017. Available from http://www.hse.gov.uk/foi/internalops/og/og-0086.pdf , accessed 2017-05-23.

[3] International Electrotechnical Commission, *IEC 61508, Functional safety of electrical/electronic/programmable electronic safety-related systems*, 2nd Edition, 7 parts, 2010.

[4] International Standards Organisation/International Electrotechnical Commission, *ISO/IEC Guide 51 Edition 3, Safety aspects – Guidelines for their inclusion in standards*, 2014.

[5] International Electrotechnical Commission, *IEC 61511, Functional safety – Safety instrumented systems for the process industry sector*, 2nd Edition, 3 parts plus AMD1:2017, 2016/2017.

[6] The International Society of Automation, *ISA-TR84.00.09-2013 Cybersecurity Related to the Functional Safety Lifecycle*, 2nd Edition 2017.

[7] VDE Verband der Elektrotechnik Elektronik Informationstechnik e.V., *VDE-AR-E 2802-10-1, Zusammenhang zwischen funktionaler Sicherheit und Informationssicherheit am Beispiel der Industrieautomation – Teil 1: Grundlagen; Relation between functional safety and IT security on the example of industrial automation* (Part 1: Basic principles). Part 1 of 4 parts, April 2017.