CHAPTER 12

A High-Level View of Safety and Cybersecurity

Summarising an endeavour in a few words has advantages and disadvantages. The disadvantages is that subtleties are elided. Amongst the advantages is that it indicates the key processes, their purposes and goals. This in turn allows details to be derived from these key processes by refinement in the context of use.

When viewed as high-level endeavours, engineering safety and security of control systems are quite similar. Both are concerned with attempted to prevent unwanted things happening, with assuring the absence of those events. As with many situations of trying to assure an absence, both lack immediate feedback of success. Just because unwanted events have not happened so far, one cannot infer ipso facto that they will not happen in future. Maybe circumstances resulting in an unwanted event have simply not yet occurred, through happenstance. In contrast, there is immediate feedback of failure when an unwanted event occurs.

A similar situation occurs with bugs, faults in software which result in functional failure of the running software. This is also a situation of trying to assure an absence. It has been a mantra for five decades that software testing, still the most common method of evaluating software, even critical software, can only show the presence of bugs, not their absence[1] [1]. Nevertheless, testing is still seen by critical-system software standards as a main validation method – see, for example IEC 61508-3:2010 Subclause 7.7.2.7: "*The validation of safety-related software aspects of system safety*

1 "*. . . program testing can be a very effective way to show the presence of bugs, but is hopelessly inadequate for showing their absence*" [1].

shall meet the following requirements:... testing shall be the main validation method for software; analysis, animation and modelling may be used to supplement the validation activities; ... " [4]. Indeed, recent work by my company Causalis (October 2017) has shown that about a third of the almost sixty documentation requirements for critical software in [4] concern testing.

Similarly, in safety and cybersecurity there is a strong temptation to infer that if you have "gone through the motions" of assurance, that you are relatively safe, respectively, cybersecure. Everyone laughs at the drunk looking for his keys under the streetlamp, not because that is where he lost them, but because it is easier to see. However, he does see at least that they are not there where he looked. Similar is true of bugs and testing, hazards and safety, vulnerabilities and cybersecurity. Some degree of assurance is obtained by following some processes, because at least you know that things are not bad where you looked, although this degree of assurance is often not as high as wished.

12.1 High-Level Processes

Processes in safety assessment can be summarised:

- Know what you have got
- Know where the weak points are and their extent
- Control the weak points
  - Strengthen the weak points where possible
  - Decrease the exposure of vulnerable assets to an event exploiting a weak point
  - Monitor the weak points to give early warning

12.2 Applying to Safety

In safety, the weak points are hazards – states or events through which harm and/or damage can ensue. Strengthening the weak points means reducing the likelihood that harm and damage can ensue. Decreasing the exposure of vulnerable assets means reducing the severity of consequences. Monitoring hazards gives the chance

to react to them actively, say removing vulnerable assets to reduce the severity of a consequence, even when it negatively affects the daily business function of the system. ISO/IEC Guide 51 details measures concerned with safety in standards concerning safety-related systems [6]. It requires

- Hazard identification (cf. knowing the weak points)
- Hazard analysis (estimating the extent/value of vulnerable assets and severity of an incident,
- c.f., knowing the extent of a weak point)
- Risk analysis (cf. estimating the likelihood of an adverse event, and combining this information with the potential severity)
- Risk mitigation (reducing likelihood of an adverse event and/or reducing its severity; c.f., strengthening the weak points and decreasing the exposure)

If follows that the Guide 51 activities roughly follow the scheme indicated above.

12.3 Applying to Security

Security follows a similar set of themes. Consider, for example, the security of your house.

- *Know what you have got*: list your valuable items, including the house itself
- *Know where the weak points are and their extent*
  - where: windows and their latches, doors and their latches, roof access. Thin walls that can be cut or bored through.
  - extent: thin window glass or resistant glass. Locks: no locks (handle inside), knob locks, dead bolts, euro profile cylinders.
- *Control the weak points*
  - *Strengthen the weak points*: greater barriers to unauthorised access. Install resistant glass on ground-floor windows and doors; install window opening-locks or opening- inhibiting mechanisms; install dead bolts instead of or as well as knob locks on outside doors.
  - *Decrease the exposure of valuable assets*: keep keys in a key cabinet; put your wallet or purse in a safe or locked drawer when in the building; use Kensington locks for computer equipment.

  - *Monitor the weak points*: know who is coming in and out, who has access; install a burglar alarm.

It is left as an exercise for the reader to apply this high-level model to the physical security of, say, process plant. A similar high-level view may be taken of the cybersecurity of such plant in particular.

12.4 Applying to Cybersecurity

Cybersecurity is combinatorially very much more complex than physical security.

- *Know what you have got*: an inventory of system components and their versions is required by most standards and guidance on plant cybersecurity, although to varying extent.
- *Know where your weak points are and their extent*: this is typically a hard task in cybersecurity. Many countries have governmental Computer Emergency Response Teams, CERTs, which amongst other things archive vulnerabilities in digital equipment and software. The US has a special CERT for IACS, ICS-CERT. A comprehensive database of Common Vulnerabilities and Exposures (the CVE database) is maintained by a US government contractor, Mitre. A 2016 EU Directive, EU 2016/1148 [2], requires member countries to set up CERT-like entities, CSIRTs and legal requirements for cybersecurity incident reporting to a central authority. Then there is the more subtle issue of vulnerabilities in COTS systems: government agencies may wish to keep some vulnerabilities secret, in order to exploit them against adversaries: unfriendly countries, guerrillas and terrorists, criminals. A balance must be found between these competing requirements.
- *Control the weak points*
  - *Strengthen where possible*. Install cybersecurity patches when available, on a feasible schedule. Implement effective access control to valuable assets. Establish effective vetting for personnel with access. All these are key points in most guidance and standards.
  - *Decrease the exposure of valuable assets*. This is a tricky one. It could suggest: don't computerise unless you need to. This is the position of many voting-system analysts, for example, on evidence such as the recent

Voting Hacking Village event at Def Con 2017 in Las Vegas, where expert vulnerability identifiers were invited to analyse a wide variety of digital voting technologies, and every single one was penetrated [8]. However, voting is an activity with a series of absolute requirements that are difficult or impossible to implement in current digital technology with the required guarantee. IACS are different: vulnerabilities introduced through the use of digital computation are often compensated, or thought to be compensated, by the increased business advantages of doing so: a cost-benefit calculation. Most guidance and standards do not offer any explicit advice on this issue.

– *Monitor the weak points*. There is a requirement for monitoring in most guidance and standards, for example, in the "Detect" element of the US NIST Cybersecurity Framework Core of *Identify, Protect, Detect, Respond, Recover* [7].

Summary

I have argued that both safety and cybersecurity assurance of IACS follow a similar high-level process, and I have indicated how that process is realised in IACS safety standards and guidance as well as IACS cybersecurity standards and guidance.

Bibliography

[1] Edsger W. Dijkstra, The Humble Programmer, ACM Turing Award lecture, 1972. Available at https://www.cs.utexas.edu/ EWD/transcriptions/EWD03xx/EWD340.html.

[2] European Union, *DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union*, Official Journal of the European Union, Available at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148, accessed 2017-11-18.

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

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

[5] International Electrotechnical Commission, *IEC 62443 Industrial communication networks - Network and system security*, many parts, various dates.

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

[7] National Institute of Standards and Technology, Cybersecurity Framework. Available through https://www.nist.gov/cyberframework, accessed 2017-11-18.

[8] Bruce Schneier, News section, Cryptogram, August 15, 2017. Available from https://www.schneier.com/crypto-gram/archives/2017/0815.html#2, accessed 2017-11-18.