Independent safety assessment – new standards, new challenges

Aryldo G Russo Jr

CENELEC is the European Committee for electrotechnical standardisation and responsible for standardisation in the electrotechnical engineering field. Standards 50126, 50128 and 50129 are generally accepted as the worldwide references for railway safety, and are the base reference for assessments performed by Independent Safety Assessment (ISA) bodies. Since the first publication the standards have focused on the pragmatic concept of safety, and all studies and analysis were done with the objective of demonstrating that all possible measures were taken in order to avoid hazards related to injuries or fatalities.

The analysed causes of hazards were generally self-contained in the system under assessment and did not take into account attacks that could come from external sources.

As the world evolves the standards have evolved, and as a result the new version of CENELEC EN50129:2018 includes, in a simple but effective way, a new chapter (6.4) that requires cybersecurity to be dealt with as part of the safety demonstration case and included in the safety case.

Cybersecurity is a vast area of discussion, and can be treated in different levels of depth and application, such as:

- Enterprise wide: where the attacks are company related and targeting company assets.
- Product/project wide: where the attacks intend to disturb the operation of some process.

At different levels different standards also exist, some of them more related to the company-specific issues, like the ISO 2700x series, others more related to the product/projects, like the IEC 62443 series. A study performed by one of the Shift2Rail initiatives concluded that the IEC 62443 series copes with almost all the railway domain requirements and should be the application choice for rail.

Figure 1 shows the different aspects that can be related to Cybersecurity aspects, and emphasises the relation between EN50129 and the aspects that should be evaluated in an ISA submission from now on.

EN 50129, now creates a new need, or a new task to be performed by ISA bodies. This is the

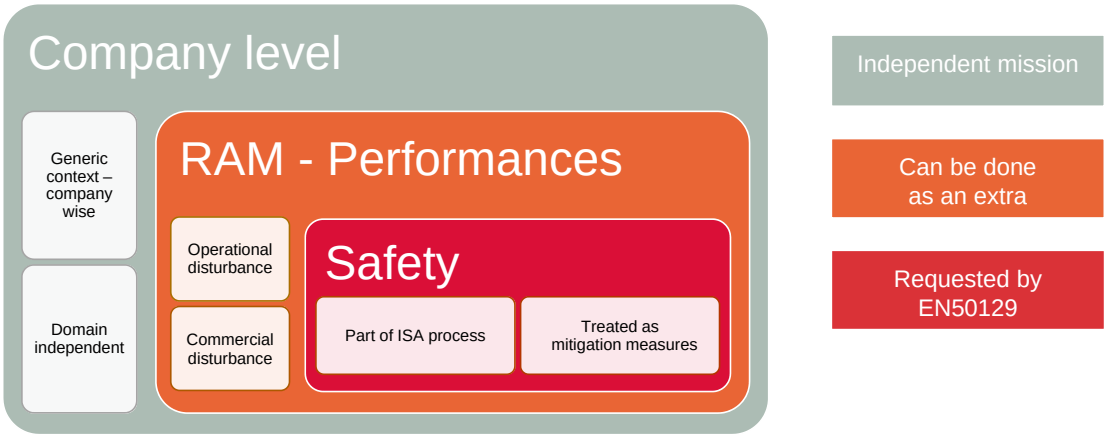

Figure 1 – The different aspects that can be related to cybersecurity.

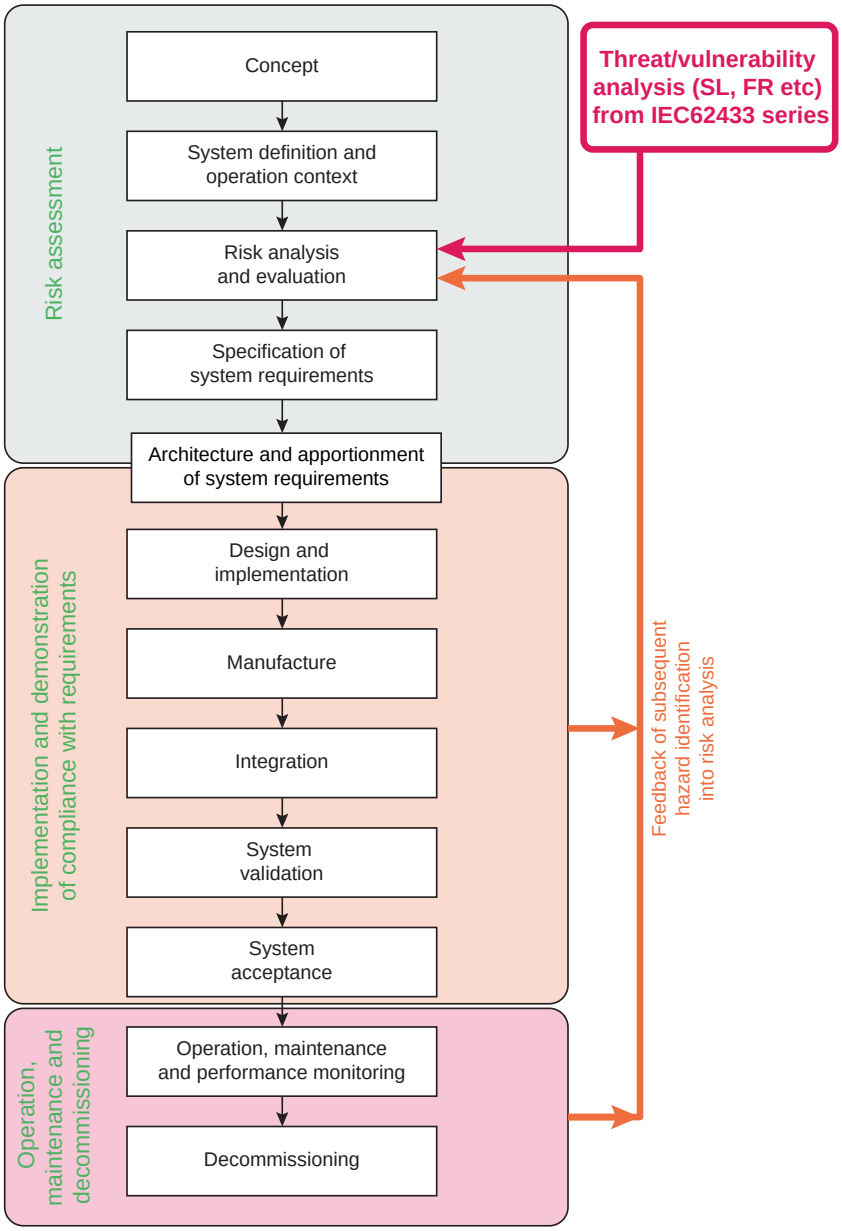

Figure 2 – A simplified view of the system lifecycle from EN50129, showing the point at which cyber security requirements should be included and the feedback loop from hazard identification to risk analysis/evaluation.

evaluation of cybersecurity (as causes) which needs to be taken into account during the safety demonstration process. One possible way to integrate the new requirements is into the system lifecycle, as demonstrated in Figure 2.

So, in an abstract way and as a minimum, the points below should be checked during the assessment to guarantee the consistency of the safety demonstration:

- Top level assessment
  - Was cybersecurity taken into account during the initial development phases (conception and risk analysis)?
  - Were top level cybersecurity plans prepared?
- Technical assessment (taking into consideration that the IEC 62443 series were defined as the reference)
  - For each sub-system, were the functional requirements (FR) evaluated and the security level (SL) allocated?
  - Each of the sub-tasks for FR coverage were correctly applied?
  - Is the evidence consistent?

As technology moves forward, new threats arise, or become more important, as is the case with cybersecurity. The standards bodies are aware of this, and the updates of the current standards take account of these new aspects.

It is important to be rigorous during the assessment stages of a safety submission to be sure that the new requirements are all well covered. A good assessment strategy should be in place, such as the one discussed in this article.

About the author ...

Aryldo G Russo Jr is director of innovation at CERTIFER, France, and a senior lead assessor. He has been working on safety related projects since 1999, and has accumulated relevant experience of both research and development, and validation of industrial safety-critical projects, particularly in the railway domain. He has been responsible for the complete RAMS activities of several SIL 2, 3 and 4 railway projects, and contributed to the remaining safety and validation activities. Aryldo is CEng and a Fellow of the IRSE and SaRS (Safety and Reliability Society).

What do you think?

Is cyber-security adequately addressed in every project? Do current standards make sense and are they fit for purpose? Have you successfully incorporated cyber securities into your system design? Let us, and other members, know of your experience and views, email us at **editor@irsenews.co.uk**.