IRSE SWISS SECTION

# Where are the CENELEC standards going?

Report by George Raymond

Austrian experts helped review CENELEC at a Swiss Section conference on 23 May 2014. ÖBB Railjet in Zurich; photo Hans and Jeanny De Rond, 2009.

A 23 May IRSE Swiss Section conference in Bern addressed the CENELEC standards for signalling – including weaknesses, strengths, past and future improvements and the roles of personal responsibility and common sense in interpreting and using the standards as the basis for affordable, simple and safe systems.

Markus Schneider of Siemens Switzerland's signalling development department described the long effort to combine the largely national standards before 2000 into the European CENELEC standards (see box).

### Main European railway standards for signalling

| | |
|---|---|
| **EN 50126-1:1999:** | **The specification and demonstration of reliability, availability, maintainability and safety (RAMS).** |
| **EN 50128:2011:** | **Software for railway control and protection systems. Replaced 2001 version.** |
| **EN 50129:2003:** | **Safety-related electronic systems for signalling. Replaced 1998 version.** |
| **EN 50159:2010:** | **Safety-related communication in transmission systems. Replaced 2001 version.** |

## ONLY THE BIBLE IS THE BIBLE

IRSE Swiss Section president Markus Montigel pointed out that the CENELEC standards should not be seen as a Bible. "Only the Bible is the Bible", he said. EN 50126 leaves room for interpretation by warning that its application should be flexible and effective in terms of size, complexity and cost. The standards are also inconsistent: checking fulfilment of "specified requirements" is the job of verification in EN 50126 and of validation in EN 50128.

Mr Montigel called CENELEC a helpful resource to be used reasonably and sensibly. Designers should assume personal responsibility, apply common sense and seek to implement a cheaper or simpler – and perhaps safer – system than CENELEC seems to specify.

# WEAKNESSES AND STRENGTHS

Kurt Preisinger of notified body Arsenal Race in Vienna described his experience with systems in the whole range of CENELEC safety integrity levels (SILs). Dangerous situations can arise once every 1000 hours in SIL 0 and once every 10 thousand million (1010) hours in SIL 4. Risk analysis yields the appropriate "tolerable hazard rate" and SIL for each application based on factors such as stopping distances for main lines, shunting and tramways. CENELEC's RAMS standards recognise that unreliability leads to dangerous manual fall-back methods. The focus of the standards is traceability, and on how instead of what.

Like the Bible, Mr Preisinger said, the CENELEC standards have internal contradictions. These are unavoidable when many interests are involved. The standards define process roles clearly, but people's corresponding qualifications only vaguely. The standards' level of detail and strictness is inconsistent. The texts contain many "softeners" and use examples that seem to be the rules themselves but require interpretation. He expected future versions of the standards to be more strict and detailed.

In order to draw practical support from CENELEC, Mr Preisinger said, you must adapt the standard to your process and not vice versa. You need to understand the purpose of the standard and be able to interpret it sensibly.

Mr Preisinger also described the standards' strengths. They place safety before cost and time pressures. Their four-eye principle blocks a reasoning error by just one person. The phase model with intermediate checks prevents chaos. Documentation ensures that the product and processes are reproducible.

The standards also offer other benefits: transferability and reusability of processes and project structures; extension of the standards' coverage to new systems on the basis of experience; cross-acceptance between countries; and comparability of solutions of equal and neighbouring SILs and with other standards for complex systems. The standards support project, safety and certification management. Although they seem to generate more work, complexity and functionality, this often reflects the greater complexity of today's systems. The standards may ultimately save time and money by revealing problems early in the life cycle. Workload can be reduced by using hierarchical document structures, cross-references and IT tools that may ultimately eliminate huge paper printouts.

### EN 50126: RAMS

Mr Schneider of Siemens said that the first version of EN 50126 from 1999 explained key terms, defined RAMS management and its life cycle, and addressed risk acceptance criteria, which triggered discussion. But its very general handling of risk and safety integrity needed much interpretation. For Mr Schneider, the next version of EN 50126 needs to cover risk management analogously to the European Common Safety Method and make RAMS subordinate to the central notion of risk, as is usual for example in the machine-making industry and medical technology.

Markus Hirt of Thales Switzerland described using EN 50126-1 for RAMS management in a non-homogeneous railway project: the Gotthard base tunnel. The project has linked EN 50126-1's RAMS phases to milestones and payments for subcontractors. The 1999 version of EN 50126-1 had no rules for the structure of a safety case, so they used EN 50129's structure. The preliminary 2012 version of EN 50126-1 now specifies such a structure. Whereas the phase model of the 1999 version foresaw no corrections until installations had entered service, the draft 2012 version has many more feedback loops into risk analysis and previous phases and even back to the basic concept.

For Mr Hirt, the astronomical safety goals of EN 50126-1, which prescribe no dangerous situations "until the sun stops shining", say nothing more than "perfectly safe". How can you judge a component's failure rate without statistical experience? EN 50126-1 forces you to assume a risk reduction that is hard to justify or to demonstrate in operations. Following EN 50126-1 to the letter doesn't necessarily make an implementation safe. The standard provides only weak support for safety management, and its application is neither self-explanatory nor can it be taught. Only competent employees can master it.

### EN 50128: Software for railway control and protection systems

Mr Schneider of Siemens said that the original 2001 version of EN 50128 focused on avoiding or reducing systematic mistakes in software development; i.e. on software quality assurance. It introduced specific rules, roles and responsibilities. But it had no error model for software writing. Implicitly based on the waterfall model, EN 50128 didn't mention newer development and testing methods already known at the time. It created a need to explain the conformity of new methods for software development and quality assurance, which in turn requires finding people familiar with the state of technology in 2001. The standard also placed too little emphasis on the personal responsibility of the person in each role.

Mr Schneider said that the 2011 version of EN 20128 is more detailed and strict than the 2001 version. But the 2011 version does not make clear which faults in current practice it seeks to correct. The 2011 version has rules for each phase, including an explicit link to verification; extension to more roles; explicit process descriptions; additional phases and new topics such as tooling; and last but not least a better chapter structure. But verification duties have become much more extensive in the 2011 version and additional roles blur responsibilities and hamper an overall view. The new versions of EN 50126 and 50129 should leave more room for interpretation and avoid the new perfectionism in EN 50128.

Nowadays, Mr Schneider said, people are ever more averse to risk and try to mitigate it with more rigid rules. But projects require not just perfect rules and formalism but also individual responsibility, trust and room in which to find solutions that are both innovative and free of errors.

Werner Schütz of Thales Austria said that the 2011 version of EN 50128 better distinguishes two key concepts, roughly summarised as follows:

- Verification checks that the results (process, documentation, software or application) of a phase fulfil requirements in terms of completeness, correctness and consistency;

- Validation checks that an object (process, documentation, software or application) fulfils user needs, particularly for safety and quality.

The 2011 version defines a new quality management process at a higher level. Verification and validation are now based on a number of interrelated roles, including developer, tester, integrator, verifier, validator, project manager, safety manager and configuration manager. In smaller projects, one person able to simultaneously fulfil several of these roles may be hard to find. One danger is limiting verification to documents while neglecting project results. EN 50128 now explicitly refers to testing, which is the most important verification method. Mr Schütz recommended performing validation throughout the project and not just at the end.

**EN 50128 now also prescribes classifying an organisation's tools into three categories:**

- T1 tools that don't affect the code or data, even indirectly;
- T2 tools that help test or verify a product's safety, and could fail to detect errors, but can't introduce them and;
- T3 tools that contribute to the code or data, even indirectly.

In order to meet EN 50128's tooling requirements, Thales Austria has created an overview that shows the selection arguments and justification for each tool and conditions for its use. To use the tool, each project must then prove these conditions are fulfilled. For issues such as tool qualification, coordination would be possible with other standards, but this could lead to the "consulting industry" that has arisen in automobile manufacturing.

Mr Schütz said the new version of EN 50128 brings additional work due to the new level of verification and more documentation of checks. But test organisation remains the same. He said the standard needs to be made clear for people who are not standards specialists.

### EN 50129: Safety-related electronic systems for signalling

Mr Schneider of Siemens said that EN 50129, whose latest version dates from 2003, addresses electronic (not relay) railway signalling systems and functional safety and is applicable from SIL 1 to 4. It defines main concepts such as the safety case. A weakness is that EN 50129 copied the role model from 50128, but without stating tasks and responsibilities. The next version of EN 50129 should additionally address IT security; procedural safety; COTS cross-acceptance for SIL levels (in relation to EN 61508 for example); different SIL levels on the same computer; large systems versus small components; and field-programmable gate arrays (FPGAs).

## DISCUSSION

Discussion with the audience yielded these comments:

- Specific rules are required for the more complex responsibilities in bigger projects. More people mean many more interfaces;
- Some people just try to follow the standards and "turn off their brains";
- You always must leave people some freedom of movement;
- Complete compliance with CENELEC is economically impossible;
- All project participants must apply the CENELEC standards from the start. You mustn't wait until the Swiss Federal Office of Transport (FOT) tells you the project has to conform to CENELEC. But the FOT has helped projects find practical solutions for the standards' implementation.

## PRESIDENT'S CLOSING COMMENTS

Markus Montigel said that since its May 2011 founding, the IRSE Swiss Section has acquired eight corporate members and grown individual membership from 33 to 57. Upcoming Swiss Section events include the Gotthard Base Tunnel in September 2014, Schweizer Electronic in November 2014 and the 2018 Convention.

The author thanks the conference speakers for reviewing this article.

## ON THE MOVE

### Russell Gell appointed as Engineering Director

Following the organisational changes made towards the end of last year, DEG Signal has appointed Russell Gell as its new Engineering Director.

Russell joins us from a leading role at London Underground, with a long and rich background of more than 25 years of experience of railway signalling, with 15 of those years spent in the metro environment.

The position is part of the new structure of the company and will lead improvements in quality, processes and assurance and it expands our consultancy capability. Russell's detailed knowledge of the metro market will help us to understand and better support the astonishing growth in capacity and level of service that LU has been implementing year on year.