IEC 61508 Weaknesses and Anomalies

Peter Bernard Ladkin
RVS Bielefeld White Paper 2
12 February 2013, minor modification 20 February 2013

Background: System safety consists of a set of best-practice principles for attempting to assure adequate safety of engineered systems which may engage in dangerous behavior. Systems are collections of objects (subsystems) with behavior (changes of state, which may cause changes of state of the system environment). There are some well-understood principles of system safety (relative freedom from the most damaging consequences of dangerous behavior) which apply no matter the type (design, operational mode) of system in question. Many engineered systems at time of writing are controlled or partially controlled by digital electronics. Functional safety of such systems is regulated, as far as this goes, by the standard IEC 61508 for functional safety of systems involving electrical, electronic and programmable-electronic (E/E/PE) systems. In the future, engineering systems may well be controlled by nanotechnogical or biological/biochemical behavior, which is not governed by IEC 61508. Nevertheless, for the foreseeable future (say, 20 years or more), E/E/PE systems will lie at the heart of most engineered complex systems. System safety standards for E/E/PE systems willl remain for this period of time the most important and applicable standards for system safety. What IEC 61508 requires from system developers and assessors remains for this period of time prominent amongst system safety standards.

IEC 61508 is developed and maintained by IEC TC 65, specifically subcommittee SC 65A. The IEC says "All IEC International Standards in the IEC 61508 series were developed by IEC SC (Subcommittee) 65 A: Industrial-process measurement, control and automation - Systems aspects". The derivation from industrial-process automation is apparent in the standard itself. However, IEC 61508 is **the** international standard for assessing safety of all safety-relevant systems based on digital-electronic subsystems, and not all of those are industrial-process systems. Transportation systems, including not only public-transport but also road-traffic systems, are not industrial-process systems and largely do not share their characteristics. However, IEC 61508 claims to be the standard for functional safety of all safety-critical systems based on E/E/PE technology, and standards for, say, system safety in railways are understood to be "derivative" from IEC 61508. This administrative subordination leads to anomalies, in that it is not based on engineering science in any way; appropriate safety measures for industrial-process systems, even "derivative" measures, are not necessarily appropriate for all E/E/PE-based systems.

There are specific technical problems with IEC 61508 that are not adequately addressed in current IEC standardisation proceedings. These are:

1. That the conception of safety and safety assurance in IEC 61508 stems largely from the common situation in the process industries. An acceptable numerical level, expressed in terms of per-operational-hour and called "probability", of dangerous failure of a system or component is set somehow "externally" (by "society"). The system design is assessed for its accordance with that set level. If the set level is not reached, then supplementary system functions, called "safety functions", must be designed, whose purpose is to reduce the dangerous failure level to the acceptable level. Such a conception is appropriate for industrial processes, say for pipes carrying corrosive or hot fluids or gases, which may burst; one clads the pipes to contain the effluence of a burst, or one builds-in pressure sensors connected to valves which stop or redirect a flow at set parameter values. These are "safety functions". It is inappropriate for, say, vehicle control systems which may experience dangerous oscillatory system-operator coupling (SOC; in aviation, called aircraft-pilot coupling or APC, and sometimes but misleadingly pilot-induced oscillation, PIO). One can only reasonably address this situation if one knows where the SOC lies in the control domain, and one knows how often the system and operator enter that domain. Neither sort of knowledge is usually present at system-design time. This entails that the IEC 61508 standard has nothing to say about how one goes about identifying and avoiding such behavior.

Yet such systems form a significant proportion of safety-related digitally-based systems. Their characteristics and analysis need to be addressed in a suitable E/E/PE safety standard, and are not.

2. That denoting all dangerous conditions or behavior of a system as "dangerous failures", as IEC 61508 does, is misleading. Given an aircraft in close proximity to the ground on landing, a command to pitch down could well result in an accident. However, historically, for good reason, allowing an operator (pilot) the authority to pitch down sharply even on final approach in close proximity to the ground is acceptable. For example, to avoid an aerial conflict. This ability, and its realisation, is not a "failure" as the term is understood in engineering, although the behavior might well be dangerous and result in an incident or accident.

3. That SW inherits quantified reliability requirements from the quantified HW SILs. There seems to be a culture of denial around this, but there is a clear and correct argument that it must be so in general (although there are exceptions). See [Ladkin 2009,2013].

4. That SW development is adequately regulated through SW SILs. Suppose a system is driven by SW, for example the fly-by-wire control system of a computer-controlled aircraft. There are certain "dangerous states" of the system, for example those in which SOC is possible. IEC 61508 sets numerical conditions upon the frequency (or "probability") with which such states are encountered in system operation, and requires that it is ruled out by system design that those states are encountered more frequently. However, only the first condition (equivalent to SIL 1) and not the other three (equivalent to SILs 2-4) may be shown by the best possible current methods and their thorough application to have been attained. The only means of showing that the other three (equivalent to SILs 2-4) are attained is through demonstrating that the SW is perfect, which is currently infeasible for any other than simple SW. But most SW falling IEC 61508 is more complex than this. It is inappropriate for a standard routinely to require measures which are infeasible.

5. That there is no required tracing (traceability, derivation) of SW safety requirements from the higher level system or component safety requirements. This is how the phenomenon in item 3 manages to happen.

Note: The German national committee is concerned about traceability, but has not yet grasped the nettle on Item 3.

6. That the methods demonstrated to produce quality SW are applicable and constitute best practice at any place in the no–SIL, SIL1…SIL4 chain - there is no reasonable distinction between SILs that affects best-practice SW development. It follows that the tables in [....] showing how rigorous one needs to be per SIL are misleading and inappropriate.

Note: One of us (Ladkin) is in the last stages of negotiating a project supported by the German Federal Ministry of Economics and Technology in the "Innovation in Standards" program, which runs through the electrotechnology standards agency DKE, for determining which rigorous mathematical and other formal methods in industrial use are mature and therefore ripe for inclusion in standards, particularly IEC 61508. The project work will generally be based on the white paper / keynote conference paper (Ada Connection 2011, Edinburgh) entitled Functional Safety of Software-Based Critical Systems (Ladkin, also describing work of Littlewood). This white paper was also presented as a keynote talk at IET System Safety Conference 2012 (also in Edinburgh).

There are two issues here
* The inappropriateness of the SIL regime to guide the methods used in SW development. Establishing the criticality of the SW is essential for other reasons, and SILs may well be one way to do that;
* Provision of up-to-date guidance on practical formal methods and rigor. The German project addresses this.

7. That provisions for relatively-safe SW re–use are inadequate. That is, to use IEC 61508 terms, methods for qualifying preexisting SW as "proven in use" are inadequate.

Note: The German committee has a concrete proposal on the table, and the IEC Maintenance Team is convening to discuss it, in advance of the formal "maintenance", planned to start in 2014. The MT Convenor is Audrey Canning, Secretary Ron Peirce, both GB. A meeting will take place in Frankfurt shortly.

The elephant in the room is that no one knows how to adhere to the raw statistical requirements and at the same time come to reasonable practical judgement about the suitability of existing SW.

8. That the role of SILs is far broader than appropriate. It could be argued SILs are now so entrenched, and used for so many different purposes other than those foreseen by the IEC 61508 standard, that arguing to take them out will likely be fruitless. And it could even be counterproductive, given that some idea of the criticality and required quality of components is needed, and SILs do that, even if not perfectly. The European railway Common Risk Management scheme has taken them over for its risk matrices, but with different boundaries to those in IEC 61508. However, the use of SILs for regulating the methods to be used for developing SW for safety-relevant systems is inappropriate.

References

[Ladkin 2009] Peter Bernard Ladkin, Two notes to York Safety-Critical Systems Mailing List, 21 and 22 May 2009. Available at http://www.cs.york.ac.uk/hise/safety-critical-archive/2009/0160.html and http://www.cs.york.ac.uk/hise/safety-critical-archive/2009/0163.html . Rewritten as working paper for German standardisation group DKE GK 914, October 2009.

[Ladkin 2013] Peter Bernard Ladkin IEC 61508 Case Study, RVS White Paper 3, 20 February 2013. A rewritten version of [Ladkin 2009]. Available at http://www.rvs.uni-bielefeld.de/publications .