Understanding SIL

Prepared on behalf of the IRSE International Technical Committee
by Rod Muttram and Clive Kessell

INTRODUCTION / BACKGROUND

The term 'SIL' or 'Safety Integrity Level' (originally Software Integrity Level) is one of the most misunderstood and misused terms in the Railway industry.

SILs relate to specific safety functions can only be allocated to a function. The safety integrity of a system or piece of equipment is then normally listed as being the highest SIL of the functions executed by it. However, very rarely do all functions within a particular system or piece of equipment have to meet the highest SIL involved. Recently some customers have shown a tendency to request that a system or piece of equipment meets a particular SIL, without appreciating that if this is needed at all, maybe only one or two functions within that system actually need a SIL. This is particularly true for CTC (Centralised Train Control) or ATO (Automatic Train Operation) systems.

In some cases Safety Integrity Levels for equipment and subsystems are specified without any knowledge or linkage to real safety requirements, functions or system architecture simply because of a misguided belief that a high SIL must be a 'good thing' and is somehow 'state of the art'. Unfortunately, certain suppliers encourage this SIL escalation, promoting their particular products as 'better' because they have been assessed to a particular SIL in certain markets and configurations. Such suppliers choose to ignore any deficiencies in their architecture or subsystems that drive the need for any of their particular subsystems to carry a specific SIL, or differences in the application and/or the fact that other supplier's architectures may be different but equally satisfactory.

Clients sometimes state that SIL2 is required for a complete ATO or CTC (for instance) for qualitative or reliability rather than safety reasons. That is misguided and also fails to recognise that SIL relates only to safety functions. Just because SILs are defined in terms of reliability does not mean the converse, whereby reliabilities can be defined as SILs, is also true. Indeed applying a SIL to something with no safety function is logically and semantically flawed.

WHAT THE STANDARDS SAY

The term SIL derives from a number of standards on safety engineering in use in the railway industry, principally IEC61508 and is used in the derivative CENELEC EN50128 and EN 50129.

Part4 of IEC 61508 defines safety integrity as …*'the likelihood of a safety-related system satisfactorily performing the required safety functions under all the stated conditions, within a stated period of time'.*

...and a safety integrity level (SIL) as… *'a discrete level (one of four) for specifying the safety integrity requirements of safety functions'.*

Whilst a SIL is derived from an assessment of risk, it is not a measure of risk; it is a measure of the intended reliability of a system or function. Four safety integrity levels are defined. The target probabilities of dangerous failures to which they relate are based on whether the system in question is operating 'on demand' (e.g. a shut-down system) or continuously. In general, the argument in deducing a SIL goes like this: the greater the required risk reduction, the more reliable the safety-related system which is providing it needs to be, so the higher its SIL.

Note two key points:

- SIL relates only to safety-related systems and their safety functions;
- Safety Integrity Levels are defined in terms of the reliability of the system in executing its safety or safety-related functions.

It is unfortunate that SILs are defined in reliability terms, as this leads to the constant confusion between SIL and the system reliability required for other reasons.

This confusion is dangerous and will inevitably lead to systems being delivered that do not meet the customer's true performance aspirations and have higher than expected whole life costs.

THE EFFECTS OF MIS-SPECIFYING SIL

When the SIL is increased, a reduced tolerable hazard rate is required; thus the risk of a shutdown will also increase as any defect (either transitory or systematic), detected by the system will normally result in a move to a safe state (usually a shut-down) as that is likely to be the only safe and practical response. The additional software or circuitry to do the monitoring has its own inherent reliability and may shut the system down when the primary system is actually functioning correctly. Thus by imposing a SIL on functions that have no safety content, reliability can be decreased without any benefit, just the opposite of what was intended.

Further, when any modifications are made or nonconformities corrected in a system of defined SIL, the necessary assurance activities of that SIL must be repeated. This adds cost and also delays system improvements to reliability or system level performance derived from functions with no safety content. The authors have witnessed client/operator organisations arguing against, or actually reducing, the level of rigour applied to later modifications, usually because they do not want the cost or time delay associated with involving the original contractor/design team in the change. If a SIL is not to be maintained, then why ask for it in the first place?

For software, EN50128 describes a series of techniques that can be used to give a particular **level of confidence** in the integrity of that software. However, it is not possible to accurately predict software failure rates and the belief that the application of the measures recommended for a particular SIL will result in zero software failures for the tested software is misguided and wrong. Thus applying the designated SIL measures for software is necessary **but not sufficient** to declare that a system containing software is 'safe' for a particular application.

Unfortunately, as already mentioned, SIL has become used by ill-informed people as shorthand for a quality or reliability requirement and the highest level (SIL 4) as shorthand for *"we want it as safe as possible".*

Note again that SIL relates to **safety** functions and their **safety** integrity requirements. Just because SIL is expressed as a reliability figure, this does not mean that the converse is also true; reliability should **not** be expressed as a SIL where safety functions are not involved.

Ascribing a SIL to non safety-related functions is meaningless. Unfortunately, since EN50128 describes techniques to be applied to software 'as a whole', it tends to reinforce these misconceptions. Of course it is not unreasonable for a client to ask for certain assurance practices to be applied when software is being prepared so as to secure a low defect rate. However, this should not be called SIL where no safety is involved, as to deliver SIL requires more than just 'one-time software assurance' as outlined above.

Where software is assured using SIL2 methods, that does not make the whole system on which it runs a SIL2 system and it should not be described as such. Many other things may be needed to deliver true SIL2 for any safety functions. Where a few particular functions of a system such as a CTC do have safety integrity requirements, these are best segregated or delivered using such techniques as 'click and confirm', which use operator actions and feedback from the SIL 4 interlocking to confirm correct operation. It is worth remembering that humans are prone to error and cannot be relied upon to perform at an equivalent level to any SIL. Thus to require a SIL for anything that simply passes on a human command is usually pointless. Techniques like 'click and confirm' are good in that they potentially reduce human error rates by forcing confirmation (within a limited time frame) of a required action, giving a chance to correct any error.

Similarly careful thought is needed for any system that has ATO but also needs to provide for human drivers. Drivers have no SIL and the ATP must cope with this, so it is highly questionable to then ascribe a SIL to the ATO. Some suppliers put features such as roll-forward protection in their ATO, meaning that it must have a 'real' SIL. This must be considered less than optimal system design for a system which will be driven manually for a percentage of the time. Most train operators will specify a percentage of manual driving for ATO systems so that drivers maintain competence. The Victoria Line of London Underground (the most recent upgrade has ATO at SIL2) was originally to be operated in ATO for 75% of the time and trains were to be driven in manual mode (with ATP protection) for the remainder of the time. This would keep the drivers familiar with the train and the routes involved. In reality it was found that the drivers were unable to keep to the timetable in manual mode (with ATP protection) and the percentage was reduced to 10%. This means that for 10% of the time the train is controlled by a non-SIL driver and safety depends wholly on the ATP. The authors have also seen it argued that a SIL2 ATO is needed to meet an overall safety target to avoid 'provoking the ATP too much'. This is 'playing with the numbers' and mixing 'continuous' and 'on-demand' safety in a way that the authors consider undesirable. What matters is that the ATP responds to the demand when an unsafe condition occurs with the required integrity.

A 'one for luck' or 'just provide it' mentality has developed on SIL – it is always hard to argue against better safety, but ascribing a SIL or too high a SIL to something that does not need it is a waste of money and will not make the system safer. One low-integrity component in a safety function can render that whole function low integrity and having higher integrity components within the same safety 'chain' will not help, it just wastes money and scarce skill resources.

For a SIL to be ascribed to a whole system requires all the elements of all of the safety-related functions of that system to be assessed. If any element involved in delivering the safety-related functions has an unknown status then no SIL can be allocated to the functions concerned. People often talk about components or minor subsystems as being 'SIL4'. Again this is a misuse of the term; they should be described as 'having a failure rate suitable for inclusion in SIL4 functions or a SIL4 system if they cannot be used as a safety system in their own right. That is not to say that some functions within one subsystem or component will not have specific SIL4 design requirements to support that, e.g. the requirement for a signal "not to display an aspect more permissive than the circumstances allow".

Note that it also matters whether a safety function is continuous or on-demand, and if 'on-demand' the conditions of use and the required period of time for the function to occur should be stated. A SIL requirement or offer without these qualifiers is meaningless or dangerous or both. The SIL targets are different for continuous and on-demand safety functions.

In addition, to guarantee an overall system SIL will usually require proper maintenance of the system. Things such as point machines can rapidly lose their integrity if not properly maintained; equally a SIL that can only be achieved via excessive maintenance is not cost-effective and brings risks if a maintenance cycle is missed.

Remember also that if safety at a subsystem level is achieved in a way that destroys system level reliability; it may necessitate the use of operational control measures that are much less safe than the non-failsafe alternatives. Beware therefore of safety achieved by 'failsafe' techniques at the expense of reliability. Look out for prescriptive safety requirements that are in conflict with reliability or availability requirements. Safety without availability is pointless. A railway where all the trains are stopped is very safe (at least for a while) but also completely useless.

This does not mean that well-proven design techniques that use failsafe principles are a bad thing. Indeed the use of some of these well-proven building blocks can save a lot of analysis and can support a high level of system safety provided they are used within a suitable overall architecture that meets the required availability.

In general, safety and availability must be specified in a compatible way to produce a meaningful set of requirements and where that is not the case, the requirements should be challenged.

COMMON PITFALLS

As stated above, SIL has unfortunately become a term that is now often used (and mis-used) without any great thought or understanding.

Here are a few of the common problems:

- Conflicting requirements: a system or subsystem is required to have a certain SIL (usually 2 or 4) but certain components and architectures are also specified that conflict with delivering that requirement – e.g. the use of specified point machines, external locks, signal types, axle-counters, etc. that do not have the safety evidence to support an assessment (and maybe don't have the necessary performance). LED signals have been a common recent problem in this area;
- A requirement for one contractor to take 'total system safety responsibility' in a contract where they are not delivering the whole system and do not have the safety evidence for the parts supplied by others or already existing; or to state that the total system will be SIL 'x' when the supplier is only delivering part of the scope and the detailed safety performance of the rest is not specified, or worse, not known;

- ATO and CTC systems being specified as SIL2 in the absence of any knowledge of the system architecture and even when they may have no safety functions. Auto driving is not 'of itself' a safety function. If the system is designed to be periodically driven manually, then a human driver cannot be assured to meet any SIL. Human factor failure rates should then be used in risk assessments. If the ATO does contain safety functions such as door control or roll-forward protection then those functions can be allocated a SIL if necessary; the non-safety functions cannot be. Similarly most CTC functions have their safety assured by the interlocking that sits behind them. Anything associated with the execution of a manual command cannot have an overall integrity better than the manual input that initiates it. It is worthy of note that the Japanese railways with their long history of largely excellent safety performance and strong safety culture do not consider CTCs to be a safety system. That said, certain commands like 'emergency replacement' can have a safety function (normally some sort of combinational logic) and a SIL may appropriately be assigned to ensure that such a function is correctly executed to a defined level of certainty once a command is given. Wherever possible, these functions should be segregated in the overall architecture, thus minimising the impact that the subsystem will play in the overall safety assessment and ongoing safety management. Complex non-safety-related functions such as data analysis and decision support, often required as part of modern CTCs, need the functionality of High Level Operating Systems such as Windows or Linux and the imposition of unnecessary SILs in these areas will be in conflict with delivering such functionality cost-effectively;

- Specifying a SIL for subsystems without specifying the overall safety targets for the system of which they are part. For a meaningful safety assessment to take place an overall system safety target needs to be set and then tolerable hazard rates (THRs) derived for each of the subsystems contributing to it. A system of SIL4 subsystems is not necessarily a SIL4 system itself unless the assessment and the architecture and system design that underpins it are done correctly.

EXAMPLES

Taking the above issues into account, the following should be ensured:

- The scope of safety responsibility is aligned with the scope of delivery;

- Suppliers should generally seek only to take safety responsibility and responsibility for safety assurance for their own contractual delivery commitments in terms of hardware and software;

- Where a client wishes a contractor to take assurance responsibility for a larger scope, including scope delivered by the client itself or for other contractors the client has selected, then the terms of any offer must be carefully considered. In general, any such offer should include terms stating that failure by the client, or the third party contractor, to provide the necessary safety data or to meet their assigned THR's are considered to be 'force majeure' events;

- Where there are pre-decided elements that will limit the SIL of the overall system the contractors should ensure that they do not offer a higher SIL than is actually achievable but make clear exactly what the scope of the offer is, e.g. words such as "All new scope supplied will be designed to meet the requirements of EN50129 SIL4. Our current assessment is that the achievement of SIL4 at the system level will be limited by 'xxxxx'. We are happy to work with (the client) to confirm the system level assessment (using such techniques as hazard and fault tree analysis) and thus to determine such changes as will be required to raise the overall system to SIL4 integrity if required and practicable";

- Where the customer asks for a SIL2 CTC or ATO, the contractor should not reinforce the error by using similar wording in their offer but should use wording such as;

- Any identified safety functions within the CTC or ATO will be designed and assured to meet the requirements of EN50128 SIL2;

- If necessary (e.g. if the potential client reacts unfavourably to the above wording), it is acceptable to use terms such as "the balance of the software within the CTC (or ATO) will be written and assured using the same set of software assurance techniques as the safety-related functions". A contractor should **not** offer SIL2 on functions that are not safety-related. If a customer asks for that, get help to remove his confusion;

- Wherever possible, a contractor should attempt to offer a system architecture that segregates the safety-related functions from the non safety-related functions so that they do not have the constraints of re-test and re-validation applied to the non-safety functions as well. This can bring big benefits in whole life cost and NCR correction timescales;

- Ask the customer to specify what his safety target is, and what it relates to, in clear and preferably numerate terms. Remember that the conditions and time requirements (where relevant) must also be clear. If the client is not sophisticated enough to do that but is using 'SIL4' as a shorthand for 'we want it to be as safe as possible', then the contractor should specify within the offer what is meant by SIL4 (or SIL3, 2, 1, or 0) in the context of the response to the customer requirements and the overall system configuration. Creating mis-matched expectations only leads to problems later;

- Contractors should try not to use incorrect 'shorthand' when describing their own products. To do so can create unintended commitments that may be difficult or impossible to deliver. So, do not say things like 'Product X' 'is SIL4' but use wording such as: 'is designed to exceed the safety integrity requirements needed to meet EN50128/129 SIL4 when correctly installed, integrated and maintained'. Equally do not say 'the CTC will be SIL2', rather use wording such as 'the CTC software will be written and assured using appropriate techniques from EN50128 for functions requiring an assured safety integrity'. These are subtle but important differences.

CONCLUSION

SIL is one of the most misunderstood and thus misused terms in the railway industry. This commentary attempts to explain some of the common pitfalls and gives guidance on what should and should not be said or offered. More information can be found in the IRSE article 'The use and misuse of SIL'. Misuse of the term SIL by clients/customers should be challenged as any other wrongly specified requirement would be.