Original article
Dependability, vol. 18 no.1, 2018 DOI: 10.21683/1729-2646-2018-18-1-46-52

Design of a system with a higher safety integrity level out of components with an insufficient safety integrity level

Schäbe Hendrik, *T V Rheinland InterTraffic, Cologne, Germany*

Schäbe Hendrik

Abstract. Aim. *Technical systems are becoming more and more complex. An increasing number of technical systems contains electronic equipment and software, thus their functional safety is of utmost importance. The safety integrity level is defined by a discrete number that characterizes the set of measures against random and systematic failures depending on the specified risk reduction requirements. The concept of safety integrity levels (SIL) was developed as part of various systems of standards. While the safety architecture of a system is considered, the main question arises: how systems with higher SIL are made out of components and subsystems with low SIL. The answer to that question will allow using existing and certified components in the development of systems with specified safety integrity levels, probably with higher SIL than the SIL of the components.* **Methods.** *The paper analyzes and compares the existing rules of system combination with safety integrity levels set forth in various functional safety standards, e.g. EN 50126/8/9, ISO 26262, IEC 61508, DEF-STAN-00-56, SIRF and the Yellow Book. Beside the tolerable failure rates, the system design requirements must make provisions for combining low SIL subsystems to make higher SIL systems. The widest set of methods is defined for SIL 4 compliance. However, this set of methods cannot be reworked for all possible systems into a simple rule for the combination of systems with lower SIL into systems with higher SIL. In general, the combination of systems into a serial structure will make a system with the safety integrity level equivalent to the lowest subsystem safety integrity level. Tentatively, we can assume that by combining two subsystems with the same safety integrity level we can create a system with a safety integrity level one step higher.* **Results.** *It is shown that the general SIL allocation rule established in the DEF-STAN-00-56, the Yellow Book or the SIRF standards cannot be recommended for all countries and any situations. Failure rate and/or observation intervals must be taken into consideration. Its is proven that general rules can only be given for subsystems connected in parallel and some SIL combinations (see e.g. the Yellow Book, SIRF). In each case common failures must be taken into consideration. The general rule may be as follows: in order to achieve system SIL one level higher than the initial level, two component subsystems with the SIL one level lower must be connected in parallel. Other system architectures must be thoroughly studied.*

Keywords: *safety integrity level, combination of subsystems, allowable failure rate.*

For citation: *Sch be H. Design of a system with a higher safety integrity level out of components with an insufficient safety integrity level. Dependability 2018; 18(1): 46-52. DOI: 10.21683/1729-2646-2018-18-1-46-52*

1. Introduction

Technical systems are becoming more and more complex. An increasing number of technical systems contains electronic equipment and software, thus their functional safety is of utmost importance. The safety integrity level is defined by a discrete number that characterizes the set of measures against random and systematic failures depending on the specified risk reduction requirements. The concept of safety integrity levels (SIL) was developed as part of various systems of standards. While the safety architecture of a system is considered, the main question arises: how systems with higher SIL are made out of components and subsystems with low SIL. The answer to that question will allow using existing and certified components in the development of systems with specified safety integrity levels, probably with higher SIL than the SIL of components.

The concept of safety integrity levels is defined and used in a number of standards, such as IEC 61508 [6], DEF-STAN 0056 [1], EN 50126 [2], EN 50128 [3], EN 50129 [4] and many others (see, for example, [5, 7, 8]). In those standards are commonly defined four different safety integrity levels.

A safety integrity level is defined by the following two primary aspects:

a) Successfully managing random failures requires that the maximum tolerable hazardous failure rate of all the systems' safety functions must not be exceeded.

b) A set of measures must be in place to protect the system against systematic failures.

It should be noted that for software only systematic failures are of relevance and the identification of failure rate values is not foreseen. That is due to the fact that normal software is not supposed to have random failures.

2. Safety integrity levels

Table 1 shows four safety integrity levels and tolerable hazard rate (THR) levels as per standards [1], [4] and [6].

The tolerable hazard rate of a system is the maximum tolerable level of hazardous failures of component equipment that is defined by the safety integrity level specified for such equipment. Here we note that SIL values are identical for [4] and [6] and different for [1]. Thus, their SILs are not comparable. Even despite the fact that the THR values for [4] and [6] are identical, the provided measures of systematic failure protection are different, their SILs are not identical.

Standards [2] and [3] do not set forth any target values of hazardous failure rate. Standard [2] only requires the presence of safety integrity levels, while standard [3] is dedicated to software and describes SIL without numerical THR values. Standard [1] specifies target values of hazardous failures implicitly in the form of verbal equivalents only.

3. Combination of safety integrity levels

In this section we will describe the rules of combination of safety integrity levels (SIL) as they are used in various standards.

3.1. DEF-STAN-00-56 standard

In standard [1], the rules are given in item 7.4.4, table 8. The reader should not confuse these rules of SIL combination ([1]) with the SIL of [4], as they are different characteristics.

These rules come down to the following:

The combination of two SIL 3 devices connected in parallel results in a SIL 4 system;

The combination of two SIL 2 devices connected in parallel results in a SIL 3 system;

The combination of two SIL 1 devices connected in parallel results in a SIL 2 system;

The combination of two SIL x and SIL y devices connected in parallel results in a SIL $\max(x; y)$ system;

Note that "combination of devices connected in parallel" means that two devices or functions are combined in such a ways as only the hazardous failure of both components (or their functions) can cause a hazardous failure of the system. Out of these rules we see that the combination of two devices will at best lead to a SIL that is only one level higher than the component SILs. Additionally, a system with a certain SIL cannot be built by combining devices or functions without a SIL, at least with no application of these general SIL combination rules.

3.2. The Yellow Book

Another interesting source is the Yellow Book [10]. The Yellow Book is a British national regulation that became obsolete when common safety methods appeared. Nevertheless, it contains interesting information. In [10] SIL is defined the same way as in [4], yet the rules are quite different from those set forth in standard [1].

Table 1. Four values for different SILs and standards

SIL	IEC 61508 / EN 50129	DEF-STAN-00-56
1	10^{-6} 1/h ≤ THR < 10^{-5} 1/h	Frequent ≈ 10^{-2} 1/h
2	10^{-7} 1/h ≤ THR < 10^{-6} 1/h	Probable ≈ 10^{-4} 1/h
3	10^{-8} 1/h ≤ THR < 10^{-7} 1/h	Occasional ≈ 10^{-6} 1/h
4	10^{-9} 1/h ≤ THR < 10^{-8} 1/h	Remote ≈ 10^{-8} 1/h

Table 2. Combination of SIL rules in the Yellow Book (Table 17-2)

Upper SIL level	Lower level function SIL		Combinator (if required)
	Main	Other	
SIL 4	SIL 4 SIL 4 SIL 3	no SIL 2 SIL 3	no SIL 4 SIL 4
SIL 3	SIL 3 SIL 3 SIL 2	no SIL 1 SIL 2	no SIL 3 SIL 3
SIL 2	SIL 2 SIL 1	no SIL 1	no SIL 2
SIL 1	SIL 1	no	no

3.3. GOST R IEC 61508

Standard [6] does not have a good rule of SIL combination as in the previously mentioned ones. Nevertheless, this standard enables the improvement of the safety integrity level through the combination of lower SILs of subsystems. The general rule is as follows (see IEC 61508-2, item 7.4.4.2.4): "Selecting the channel with the highest safety integrity level that has been achieved and then adding N safety integrity levels to determine the maximum safety integrity level for the overall combination of elements". Here *N* is the number of allowable hazardous faults for the system of elements combined in parallel, i.e. the number of hazardous faults that allowed for the system. It should be noted that in order to achieve a certain system safety integrity level by means of component combination, the requirements for the number of allowed hazardous faults and proportion of right-side failures of elements must be met in accordance with the table of IEC 61508-2. Type A/B elements/systems should be distinguished (IEC 61508-2, item, 7.4.4.1.2).

An element can be regarded as type A if for the components required to achieve the safety function the following conditions are fulfilled:

a) the failure modes of all constituent components are well defined;

b) the behaviour of the element under fault conditions can be completely determined;

c) there is sufficient dependable failure data to show that the claimed rates of failure for detected and undetected dangerous failures are met.

Other elements/systems are type B. The rules for achieving required SILs for systems of type A and type B per IEC 615008-2-2 are given in Tables 3 and 4 respectively.

Tables 3 and 4 clearly show that standard [6] does not provide a simple rule for SIL combination. Not only the subsystem combination solutions and the number of allowed hazardous faults define a system's safety integrity level, but the proportion of right-side failures as well. However it can be observed that as the number of allowable hazardous faults and the proportion of right-side failures of an element is maintained in cases when same type (A

Table 3. Rules for achieving required SIL in type A systems

Percentage of an element's right-side failures	Number of hazardous faults allowed for a system		
	0	1	2
< 60%	SIL 1	SIL 2	SIL 3
60% -< 90%	SIL 2	SIL 3	SIL 4
90% -< 99%	SIL 3	SIL 4	SIL 4
> 99%	SIL 3	SIL 4	SIL 4

Table 4. Rules for achieving required SIL in type B systems

Percentage of an element's right-side failures	Number of hazardous faults allowed for a system		
	0	1	2
< 60%	Not allowed	SIL 1	SIL 2
60% -< 90%	SIL 1	SIL 2	SIL 3
90% -< 99%	SIL 2	SIL 3	SIL 4
> 99%	SIL 3	SIL 4	SIL 4

or B) subsystems are used, the SIL increases by one. That means that if there are two same-SIL subsystems with the same proportion of right-side failures of an element, their combination will increase the SIL by one level. A combination of subsystems with different types and/or different proportions of right-side failures of an element may yield different results and in such cases additional analysis may be required.

3.4. SIRF 400

The SIRF standard [9] is the German standard of the methods of railway rolling stock safety jointly developed by the German railway industry, Deutsche Bahn, German railway operators society and German federal railway administration. This document can be referenced in Germany, while outside of Germany this standard my not be recognized.

The document describes the following principles. If two subsystems are connected in series (e.g. with an IF gate in the fault tree) the lowest SIL will also be the resultant SIL of such system.

00	01
10	11

Figure 1. Allowable combinations for SIL 1 (per standard [9])

00	01	02
10	11	12
20	21	22

Figure 2. Allowable combinations for SIL 2 (per standard [9])

00	01	02	03
10	11	12	13
20	21	22	23
30	31	32	33

Figure 3. Allowable combinations for SIL 3 (per standard [9])

00	01	02	03	04
10	11	12	13	14
20	21	22	23	24
30	31	32	33	34
40	41	42	43	44

Figure 4. Allowable combinations for SIL 4 (per standard [9])

For combinations of parallel systems the following rules are set forth:

a) systems with SIL > 0 must not be made out of elements with SIL 0;

b) SIL can be decreased only by one level for the AND gate in the fault tree;

c) exception out of (b): one branch assumes all the safety functions;

d) exception out of (b): common failure analysis is performed;

e) in case of (d) the appropriate method (FMEA, HAZOP, etc.) must be used down to the lowest level of the fault tree in order to show that common failures are impossible.

Note that the SIRF standard uses the term "SAS" that is generally equivalent to SIL, but is not completely identical. Figures 1 to 4 show the allowed and forbidden combinations. The green color shows allowed combinations, the red shows the forbidden combinations, while the yellow means that subsystem independence is to be established only based on deep analysis. Figures 1 to 4 show the SIL combinations allowed per [9].

While neglecting the combination of two independent SIL 2 subsystems for achieving a SIL 4 system, we can see that primarily the combination of two same-SIL subsystems will result in a system with the SIL one level higher.

3.5. Numerical approach

In this section we will perform calculations using only hazard rates, i.e. tolerable hazard rates that are to be ensured by means of combination of homogeneous subsystems. Possible measures of prevention of systematic failures are not taken into consideration.

The analysis is based on the following assumptions:

1) a comparator is not required;

2) T is the test interval. During the inspection all failures and defects are identified and eliminated that will make a subsystem as good as new;

3) the system consists of two subsystems that are connected in parallel and have identical SILs;

4) it is required to create a subsystem with a SIL one level higher than that of the component subsystems.

The hazard rate of the combined system is roughly identified as follows

$$\lambda=\lambda_1\cdot\lambda_2\cdot T,$$

where λ_1 is failure rate of the first system, 1/h;

$\lambda_2$is failure rate of the second system, 1/h;

T is the observation period, h.

Table 5. SIL and tolerable hazard rates of subsystems and whole system for the observation period of 10000 hours

System		Subsystems		
SIL	**Rate value**	**Required rate value**	**SIL**	**Rate value**
4	10^{-8} 1/h	10^{-10} 1/h	3	10^{-7} 1/h
3	10^{-7} 1/h	10^{-8} 1/h	2	10^{-6} 1/h
2	10^{-6} 1/h	10^{-6} 1/h	1	10^{-5} 1/h

Table 5 below contains the results for the time period T = 10000 h, i.e. about a year.

We can see that for all three cases (SIL 2...4 for systems) the subsystems will comply with the requirements (target level) if the subsystems have the SIL one step lower that the target SIL of the system. However, this calculation must be complimented with the common failure analysis. To that effect, we will use [6]. Despite the fact that [4] shows another approach in 3.2, we will use [6] due to the simple fact that it provides numerical values. In the worst case, beta, i.e. common failure ratio, will be 10%. That is the part of the failure rate that is to be used for describing common failures. Later, in the process of identification of hazardous failure rate of the combined system, common failures will dominate. If now each subsystem has the SIL n, the hazardous fault rate of the combined system will be 10% of $10^{-(n+4)}$1/h, i.e. will be equal to $10^{-(n+5)}$1/h.

Thus, the combined system can have the SIL of (n+1) at best. It should be concluded that without special assumptions on common failures the system's safety can be increased by one level by combining two subsystems with the same SIL.

3.6. Brief summary of SIL combination methods

Beside the tolerable failure rates, the system design requirements must make provisions for combining low SIL subsystems to make higher SIL systems. Standard [1], in its item 7.3.3 states: "Design rules and techniques appropriate to each Safety Integrity Level... shall be determined prior to implementation...". There are no specific rules.

Standards [6] (part 2, annex A3, annex B) and [4] (annex E) set forth different methods for different SILs. The widest set of methods is defined for SIL 4 compliance. However, this set of methods cannot be reworked for all possible systems into a simple rule for combining systems with lower SIL into systems with higher SIL. However, the general rule seems to be that a system's SIL can be improved one level by combining two subsystems with a lower SIL.

4. Examples

Example 1

The system consists of two subsystems and does not contain software. A comparator is not required. Each subsystem verifies the differences between itself and the other subsystem and disables the other subsystem in case of discrepancies. That means that a shutdown of the whole system is a safe situation. Figure 5 shows the block diagram of the system of example 1.

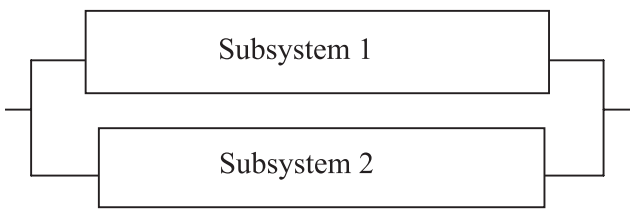

Figure 5. Block diagram of the system of example 1

If the safety integrity level of both subsystems is SIL 3 and they are independent, they can be combined into a SIL 4 system. The design rules for SIL 3 and SIL 4 systems differ insignificantly. If a system is to be SIL 2, it suffices to combine two SIL 1 subsystems. If both subsystems are SIL 2 and the system is to be SIL 3, the system is to be studied more thoroughly. The design rules for a SIL 3 system differ from those used for SIL 2 systems.

Example 2

The system is largely identical to that of example 1, yet both subsystems are managed by common software (see figure 6).

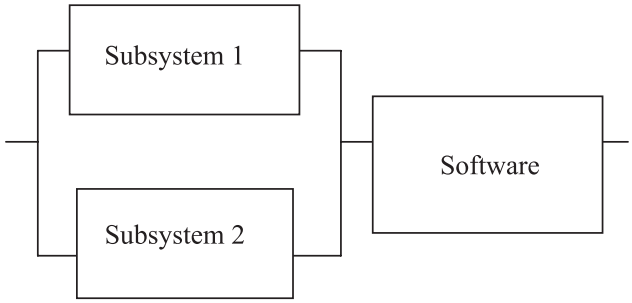

Figure 6. Block diagram of the system of example 2

If a system is to be SIL 4, the software is to be SIL 4 as well. (The SIL of the software must be at least as high as the system's). SIL 2 systems can be made of two parallel SIL 1 systems with SIL 2 software. If a system is to be SIL 3, the software is to be SIL 3 as well. If the hardware is SIL 2, in order to achieve the system's SIL 3 additional considerations must be given, as in example 1.

Example 3

This system is similar to the system of example 1, yet it contains diverse software. Figure 7 shows the block diagram of the system of example 3.

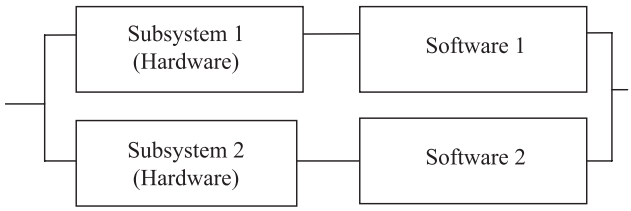

Figure 7. Block diagram of the system of example 3

Both subsystems use diverse software. SIL distribution follows the same considerations as in example 1. A system's SIL 4 can be ensured by two SIL 3 subsystems each with SIL 3 software. SIL 2 systems can be made of

two SIL 1 subsystems. In order to make a SIL 3 system out of two SIL 2 subsystems, additional considerations must be given.

Example 4

The system consists of one hardware channel, but the software is redundant (Figure 8). The software "redundancy" can be created using two different software packages or redundant programming methods (diverse software). In any case software diversity must be ensured.

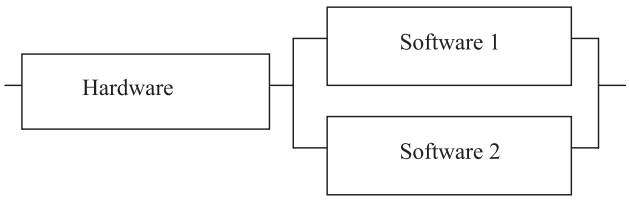

Figure 8. Block diagram of the system of example 4

Let us assume the system must be SIL 4. In this case, the hardware must also have SIL 4, while both versions of software must be designed at least per SIL 3. Additionally, it must be proven that each hardware failure is detected by software, i.e. at least two versions of software have been designed and that facilities are in place to initiate system safe state. If a system is to be SIL 2, the hardware must be SIL 2 and two versions of software each designed at least per SIL 1. A system's SIL 3 can be ensured if the hardware is SIL 3 and each version of the software is SIL 2. However, the feasibility must be thoroughly examined. The matter of independence of software versions operating within the same hardware is not trivial. In any case software must be diverse.

Example 5

In this example we are considering an electronic subsystem consisting of hardware, software and other system equipment operating in parallel (hardware bypass) (Figure 9).

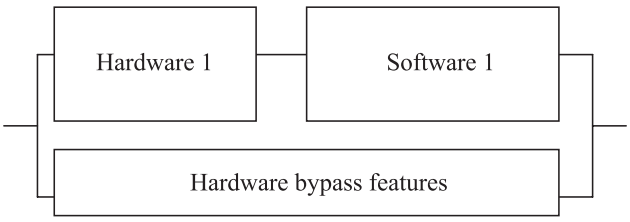

Figure 9. Block diagram of the system of example 5

If the hardware bypass facilities have the SIL required for the system, no SIL requirements should be imposed on hardware 1 and software 1. Additionally, the same logic as in example 1 can be used: SIL 4 of a system can be achieved through the SIL 3 of the subsystems (hardware 1 and software 1 on one side and SIL 3 of the hardware bypass features on the other side). Software 1 must have the SIL not lower that the SIL of hardware 1.

5. Conclusion

The general SIL allocation rule established in the DEF-STAN-00-56, the Yellow Book or the SIRF standards cannot be recommended for all countries and any situations. Failure rate and/or observation intervals must be taken into consideration. General rules can only be given for subsystems connected in parallel and some SIL combinations (see e.g. the Yellow Book, SIRF). In each case common failures must be taken into consideration. The general rule may be as follows: in order to achieve system SIL one level higher than the initial level, two component subsystems with the SIL one level lower must be connected in parallel. Other system architectures must be thoroughly studied. A good indicator of the compliance of the chosen system architecture with the target SIL is the fulfillment of the condition that the required system's failure rate per the SIL does not exceed the failure rate value calculated based on the failure rate of the component subsystems. Normally, combining subsystems into series a system is created that has the safety integrity level equivalent to the lowest SIL of the component subsystems.

6. References

1. DEF-STAN 0056 (1996) Safety management requirements for defence systems. Part 1: General requirements. Part 2: Guidelines. Issue 2, 13.2.1996.

2. EN 50126 – GOST R IEC 62278 Railway Applications. The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS); 2008.

3. EN 50128 – STB IEC 62279 Railway applications. Communication, signalling and processing systems. Software for railway control and protection systems; 2011.

4. EN 50129 – STB IEC 62425 Railway applications. Communication, signalling and processing systems. Safety related electronic systems for signalling; 2011.

5. Gräfling S, Schäbe H. The agri-motive safety performance integrity level – Or how do you call it? In: proceedings of the 11th International Probabilistic Safety Assessment and Management Conference and the Annual European Safety and Reliability Conference 2012. Helsinki (Finland): Curran Associates, Inc.; 2012. p. 6091-6100.

6. IEC 61508 (2010) Functional safety of electrical, electronic, programmable electronic safety-related systems. Parts 1-7; 2010.

7. Schäbe H. Definition of Safety Integrity Levels and the Influence Assumptions, Methods and Principles Used. In: Spitzer C, Schmocker U, Dang VN, editors. Proceedings of the International Conference on Probabilistic Safety Assessment and Management PSAM 7 / ESREL 2004. Berlin (Germany): Springer-Verlag London Ltd; 2004. p. 1020-1025.

8. Schäbe H, Jansen H. Computer architectures and safety integrity level apportionment. In: Sciutto G, editor. Safety and Security in Railway Engineering. WIT Press; 2010. p. 19-28.

9. SIRF (2011), Vehicle safety policy, version 1,1.6.2011.

10. Engineering Safety Management (The Yellow Book), Volumes 1 and 2. Fundamentals and Guidance, issue 4. 2007.

Note: the Yellow Book has been replaced with the CS-MREA application guide.

About the author:

Hendrik Schäbe, Dr. rer. nat. habil., Head of Risk and Hazard Analysis, TÜV Rheinland InterTraffic, Cologne, Germany**,** e-mail: schaebe@de.tuv.com

Received on 28.11.2017