

Title	A methodology for the assignment of safety integrity levels (SILs) to safety-related control functions implemented by safety-related electrical, electronic and programmable electronic control systems of machines
Publisher/Author	HSE
Publication Date	2004
Executive Summary	<p data-bbox="432 383 560 412">Objectives</p> <p data-bbox="432 441 1431 602">This contract research report describes the development by the authors, with funding from HSE, of a methodology for the assignment of required Safety Integrity Levels (SILs) of safety related electrical control systems of machinery. The rationale behind the methodology and how to use it in practice are also explained in some detail.</p> <p data-bbox="432 631 1431 761">The methodology has been developed and accepted for inclusion in an informative annex of the International Electrotechnical Committee standard IEC 62061: “Safety of machinery Functional safety of electrical, electronic and programmable control systems for machinery” currently being drafted.</p> <p data-bbox="432 790 608 819">Main Findings</p> <p data-bbox="432 848 1431 1010">A quantified, structured and systematic methodology has been developed for assigning SILs to SRECS safety functions in machinery. This has been developed and accepted for inclusion in IEC 62061 as an informative annex. Appendices in this report provide draft copies of the instructions for use for this methodology and the associated forms that are intended for inclusion in the informative annex.</p> <p data-bbox="432 1039 1431 1200">The methodology encourages the documentation of assumptions and takes into account the risk reduction measures provided by other technologies. This methodology is only one route to the decision as to the most appropriate SIL and is available for use when there are no machinery specific standards or codes of practice upon which to base this decision.</p> <p data-bbox="432 1229 1431 1328">From the validation carried out and the workshop held for members of Technical Working Group IEC/TC44/WG7 the following conclusions could be drawn about use of the methodology:</p> <ul data-bbox="432 1357 1431 1977" style="list-style-type: none"> <li data-bbox="432 1357 1431 1518">• it is difficult to use to assign SILs to functions related to emergency stops. An addendum to the methodology is required to explain both types of use of emergency stop equipment (in an emergency and as a high integrity manual stop) and to provide additional guidance in assigning SIL to the related functions. <li data-bbox="432 1541 1431 1671">• the paper format, in the use of forms, can appear unwieldy and inefficient. This is also out-of-date in modern CAD based design offices, which may make put off commercial users. The methodology needs to be developed into a self-documenting software based system to overcome these issues. <li data-bbox="432 1693 1431 1854">• the methodology appears complex which may also put users off. However, the complexity is necessary in ensuring that people think properly about the way an accident develops. Additionally, the methodology captures the full range of harm outcomes without being overly pessimistic. This adds some complexity, but avoids over-estimation of the risk and an onerous SIL being assigned. <li data-bbox="432 1877 1431 1906">• the guidance on the datum event for NFS type accidents is insufficiently clear. <li data-bbox="432 1928 1431 1977">• overall, the methodology was found to be fit-for-purpose and usable, and generated SILs that appeared sensible. <p data-bbox="432 2000 1431 2047">The complexity of the methodology is offset by clear step-by-step instructions that lead the user through the completion of the forms. If followed carefully whilst</p>

completing the forms the task is not too onerous. But if the user attempts to fill in the forms without proper reference to the instructions mistakes can easily be made. A number of minor changes to the instructions and from box descriptors have, however, been identified in the process of writing this report that would improve their clarity.

This SIL allocation methodology assists the machinery sector to assign SILs using a rigorous, structured and transparent risk based approach. The forms also provide a detailed audit trail. The benefits of the technique outweigh the disadvantages, namely its apparent complexity.

Although the methodology has been developed for SIL assignment in the machinery sector, there is no reason why this cannot be expanded to cover SIL assignment in other sectors. The basic approach should be generic across all industries, although some limited development would be required. Certain concepts developed in this work would also be very useful in other areas. For example, the concept of involvement time has application in other sectors, and the combination of person type and involvement time has value for both overall installation risk assessment and deriving individual risk.

Recommendations

1. Further validation of the methodology is required as this has been very limited to date. Validation needs to look at its usability and also the output from the methodology. The SILs derived need to be checked for consistency, sense and accuracy. Having regard to the general lack of structured, documented risk assessment in the sector, it is recommended that the usability of the methodology by target groups be validated.
2. The forms should be updated to include boxes for dates, persons responsible, list reference documents and to improve management of change control.
3. Minor changes to the instructions and form box descriptors should be made to improve their clarity before the standard is published for next committee or public comment.
4. The flow diagrams presented in this report may usefully be added to annex A of the standard.
5. The methodology should be expanded to cover the emergency stop function, and associated guidance produced.
6. The scope of the methodology should be extended to include damage to health, especially from cumulative effects, and to include hygiene to satisfy an Essential Health and Safety Requirement of the Machinery Directive for food processing machines (this would also require expanded scope for IEC 62061 as this is not a risk arising directly at the machine)
7. The concepts of involvement time and Person Type Use Type combinations should be extended and applied more widely in the field of machinery risk assessment, for example in the revision to ISO 14121 (formally EN 1050), or outside the machinery sector, in risk assessment more generally.
8. The methodology should be developed further and applied to other sectors.

Table of Contents	1	Introduction	1
	2	Background	2
	2.1	IEC 62061 and its relationship with IEC 61508	2
	2.2	Functional safety and safety integrity levels	3
	2.3	Risk assessment and risk reduction in the machinery sector standards	5
	2.4	Emerging risk assessment methodologies for machinery	6
	2.5	SIL assignment methodologies in other sectors	8
	2.6	Recognised deficiencies in machine risk assessment practice	10
	3	Objectives	12
	4	SIL assignment assign	14

	4.1 Introduction.....	14
	4.2 Overview of the methodology	16
	4.3 Preparation – Step 1	16
	4.4 Safety function analysis and mapping – Step 2	18
	4.5 Identification of potential accidents – Step 3	19
	4.6 Accident scenario frequency estimation for NFS accidents – Step 4	20
	4.7 Accident scenario frequency estimation for FT accidents – Step 5	24
	4.8 Harm frequency estimation – Step 6	25
	4.9 Harm frequency summation – Step 7.....	27
	4.10 SIL assignment – Step 8	31
	4.11 Plausibility check and sensitivity	32
	4.12 Forms	33
5	Assumptions implicit in the SIL assignment methodology.....	35
6	Validation.....	36
	6.1 Comparison with other methods	36
	6.2 User tests	36
	6.3 Summary of validation.....	37
7	Conclusions	38
8	Recommendations	40
9	Appendices	41
	9.1 Appendix A: Instructions for use	41
	9.2 Appendix B: Copy of forms included in Annex A of IEC 62061..	57
	9.3 Appendix C: Relating risk to persons	67