Wilde

Safety Integrity Level Requirements of a Depot Protection System

Richard L Maguire
Wilde Analysis Ltd. Whitworth House, 28 Charles Street | Stockport, Cheshire, SK1 3JR

Executive Summary

Depot Protection Systems are installed in train maintenance facilities to control the safe movement of rail vehicles, protecting staff working in the vicinity. An analysis of the obligations of the safety functions performed by a Depot Protection System in a maintenance facility has concluded that a SIL 2 target level is required.

A system can only be deemed as SIL compliant system if assessed as a whole, rather than relying on compliant COTS (commercial off-the shelf) components in a system using software of unknown pedigree (SOUP). Zonegreen's DPPS^{TM} has been assessed to meet the hardware and software requirements of SIL 2. DPPS^{TM} uses standardised software and hardware across all installations, resulting in all DPPS^{TM} installations meeting SIL 2.

I. INTRODUCTION

A. Introduction to the Depot Personnel Protection System

Zonegreen Smart Depot Personnel Protection System (DPPS^{TM}) is installed in maintenance depots to protect personnel who are working in areas such as maintenance sheds or sidings roads, from unauthorised train movements. Each installation is based upon the same core software and hardware, with bespoke configurations that are developed for each customer's site requirements. The prohibition of train movement is primarily achieved through the deployment of derailers that are typically positioned outside each road at the entrance of a building. The derailers are linked to shunt signals that control trains movements to, from and within the road. They are also connected to audible and visual alarms that provide an alert to any train movements, authorised or not. Only personnel holding a higher authorisation RFID token (such as depot supervisor, team leader) are allowed to authorise a train movement through the DPPS^{TM} system. Movement of a controlled vehicle is achieved through a controlled logic sequence of procedures by the DPPS^{TM}: interlock checking, activating audio visual warning system, lowering derailer and setting inbound/outbound shunt signals [6].

In order to move a train in/out of the protected zone, a series of controlled movement procedures (known as inbound or outbound movement respectively) are executed by the DPPS^{TM}. When such movement operation is requested, the DPPS^{TM} will ensure that all users have logged-out of the road and that all the interlocks are in a safe condition (i.e. doors are opened, interlocking maintenance equipment, e.g. OLE, bogie drop, cranes etc are in the correct state) and secure before proceeding with the movement operation. The DPPS^{TM} system will then activate the audio-visual warning system to alert staff of movement operation, lower the derailer, and set the shunt signals to allow a vehicle to move in or out of the controlled zone. When the train has completed the movement, the derailer is then raised and warnings deactivated, thus protecting the road again and allowing users to logon to the system to work on the road safely [7].

B. Introduction to the IEC Standards

BS EN 50126 [1] is concerned with the general specification for the Reliability, Availability, Maintainability and Safety (RAMS) requirements of a total railway system and the necessary risk assessment, including development of SIL targets and their subsequent satisfaction demonstration, which covers the requirements for software for railway control and protection applications [4]. EN 50126 forms part of the railway sector specific application of IEC 61508 [2]. IEC 61508 is concerned with the functional safety of systems using complex electronics and programmable electronics whose failure could have an impact on the safety of persons and/or the environment. It describes methods to classify risk and specifies requirements on how to avoid, detect and control systematic design faults, particularly in software development, random hardware faults and common cause failures, and to a lesser extend operating and maintenance errors. IEC 61508 also stands out in its whole system approach to address the complete safety installation from sensor to actuator with its technical as well as management issues [5], rather than just an individual SIL rating on one particular element of the system or equipment under control.

II. SIL ALLOCATION

C. Introduction to Safety Integrity Levels

SILs are used to specify the safety integrity requirements for the safety functions performed by E/E/PE safety systems [2]. Using SILs allows the rare but possible safety system failures to be taken into consideration, in addition to those existing in the operational system. The most dangerous failures—those safety system failures that can provoke accidents—can be either systematic or random in nature [8].

Systematic failures are latent system failures that only become visible under certain operating conditions. Software flaws and design errors are included in this category, as are certain material failures caused by environmental perturbations (e.g., high temperature, electric or vibratory disturbances). Systematic failures can only be eliminated by modifying the system design or development & manufacturing processes, by applying operational procedures, or by providing additional documentation. Because they are deterministic in nature and are largely unpredictable, systematic failures cannot be quantified. Limiting or eliminating them requires making the quality assurance part of the risk management process a primary concern [8]. Though quality assurance is difficult, when the required SIL is higher, it is the rigour of the techniques and measures that are applied throughout the system that can prevent systematic failures from occurring.

Random failures always result from material component failures (i.e., they are hardware failures). Due to their probabilistic nature, these hardware failures can be quantified. The IEC 61508 standard [2] thus defines quantitative safety requirements for each SIL. The safety systems' operational demand modes are differentiated by using two different dependability parameters: PFDavg (average Probability of Failure on Demand) and PFH (Probability of dangerous Failure per Hour). Table 1 below, expresses quantitative SIL requirements with a minimal and maximal boundary for each parameter [8].

Safety Integrity Level	Low-demand mode of operation	High-demand mode of operation
	Average Probability of Failure on Demand (PFD_{avg})/activation	Probability of dangerous Failure per Hour (PFH)/h
SIL 4	$10^{-5} \leqslant PFD_{avg} < 10^{-4}$	$10^{-9} \leqslant PFH < 10^{-8}$
SIL 3	$10^{-4} \leqslant PFD_{avg} < 10^{-3}$	$10^{-8} \leqslant PFD < 10^{-7}$
SIL 2	$10^{-3} \leqslant PFD_{avg} < 10^{-2}$	$10^{-7} \leqslant PFD < 10^{-6}$
SIL 1	$10^{-2} \leqslant PFD_{avg} < 10^{-1}$	$10^{-6} \leqslant PFD < 10^{-5}$

TABLE I

Quantitative SIL Requirements [2]

D. SIL Allocation for a Depot Protection System

The top-level safety function of a Depot Protection System is to "Protect personnel from unauthorised train movement" [4]; the top level risk is "Train impacts with individual who is unaware of the train with the driver being unable to stop", this is presented through the independent Safety Integrity Assessment for DPPS Report [9]. The maximum tolerable event frequency is 3.3 x 10-5 (pa), based on the opinion that the risk constitutes a voluntary risk and has a severity of a 1-2 fatality scenario [9]. The contributory event of "Persons at risk (unaware of train)" has been quantified at 5 x 10-3 (pa); the contributory event "AVOID" has a probability of 0.5. Thus the residual PFD target becomes 5 10-3/0.5 = 10-2. Sharing this between the Beacon and Klaxon functions places a 10-1 PFD target on the beacons and klaxon instruments. However, these are voted 1oo3 (for hardware fault tolerance purposes) and thus a < SIL 1 target applies. However, the CPLD logic device is common to both beacon and klaxon functions, and thus attracts the full 10-2 PFD target which is at the boundary between SIL 1 and SIL 2. Hence a SIL 2 target is placed on the CPLD [9].

III. SIL SATISFACTION

E. Qualitative Process Assessment

Assessment of a full system design and implementation is required, rather than relying on compliant COTS (commercial off-the shelf) components in a system using software of unknown pedigree (SOUP). The following list of techniques and measures for a whole system development and analysis was generated from the tables presented in IEC61508 [2]. A compliant system should ideally be following all the Highly Recommended techniques and measures:

Zonegreen as a design authority have been externally reviewed and shown to explicitly evidence artefacts to demonstrate satisfaction of IEC 61508 to SIL 2. The following suite of documents demonstrates that Zonegreen's development regime is in compliance with SIL 2. Every Zonegreen DPPS™ product developed to this regime will inherit the functional safety qualities of SIL 2 :

- **Table A1 – Software Safety Requirements**
  - None are HR – but some safety requirement management is necessary
- **Table A2 – Software Architecture Design**
  - Modular Approach
  - Use of trusted/verified software elements
  - Structured Diagram Methods
  - Cyclic Behaviour
  - Time-triggered Architecture
  - Event-driven functionality (max responses)
- **Table A3 – Support Tools and Programming Language**
  - Suitable Programming Language
  - Strongly Typed Language
  - Certified Tools
  - Experience with Tools and Translators
- **Table A4 – Software Detailed Design**
  - Structured Methods
  - Semi-formal Methods
  - Modular Approach
  - Design and Coding Standards
  - Use of Trusted/verified software elements
- **Table A5 – Software Module Testing & Integration**
  - Dynamic Analysis Testing
  - Data Recording and Analysis
  - Functional – Black-box Testing
  - Test Management & Automated Test Tools
- **Table A6 – Programmable Electronics Integration**
  - Functional – Black-box Testing
- **Table A7 – System Safety Validation**
  - Functional – Black-box Testing
- **Table A8 – Modification**
  - Impact Analysis
  - Re-verification of changes
  - Regression Analysis
  - Configuration Management
  - Data Recording & Analysis
- **Table A9 – Software Verification**
  - Static Analysis
  - Dynamic Analysis
- **Table A10 – Functional Safety Assessment**
  - None are HR – but some functional safety assessment is necessary.

- Concept Description, System Description and System Requirement Specification
- System Functions, Safety Assessment and Safety Requirements
- System Architecture Design – Software & Hardware
- System Installation, Operation and Maintenance Manual
- System Safety Manual Information Suite
- Hardware Safety Requirements
- Hardware Module Design & Architecture
- Hardware Development Standard
- Hardware V&V Plan
- Hardware V&V Results
- Software Safety Requirements
- Software Module Design & Architecture
- Software Development Standard
- Software V&V Plan
- Software V&V Results

F. Conclusions

The range of techniques and measures that have been applied to the DPPS™ are shown to include all the Highly Recommended (HR) techniques for SIL 2 compliance. The verification and validation processes have been shown to be developed from tests, analyses and inspections of the hardware and software items of the whole DPPS™ system. Traceability has been shown between system requirements, software & hardware requirements and test specification. It has been independently judged that the entire DPPS™ system development process, testing and implementation has been demonstrated as satisfying the clauses of IEC61508 to the rigour and content required by a SIL 2 integrity requirement [11].

Given that each DPPS™ is based on the same core hardware and software for every installation, with configurations to be tailored to the unique layout of each facility, every installation of DPPS™ that has followed the IEC61508 techniques and measures, will satisfy the functional safety and RAMS requirements of SIL 2. It should be noted that a further bonus of the core approval approach is avoiding the need for assessments of each installation for bespoke systems.

References

1. BS EN 50126-1:2017 Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS); December 2017

2. IEC61508 Functional safety of electrical / electronic / programmable electronic safety-related systems, Edition 2; April 2010

3. 53918rnh03 Issue 1 DPPS Development Safety Plan; Lloyd's Register; March 2014

4. David J. Smith, Kenneth G. L. Simpson; The Safety Critical Systems Handbook A Straightforward Guide to Functional Safety: IEC 61508 (2010 Edition), IEC 61511 (2015 Edition) and Related Guidance 5th Edition - January 15, 2020

5. Rainer Faller; Project experience with IEC 61508 and its consequences; Safety Science 42(5) : 405-422; June 2004

6. Safety Manual for ZG-Smart DPPS; ZoneGreen; March 2022

7. Concept and Requirement Specification for ZG-Smart DPPS; ZoneGreen; September 2021

8. Julie Beugin, Dominique Renaux, Laurent Cauffries; A SIL quantification approach based on an operating situation model for safety evaluation in complex guided transportation systems; Reliability Engineering & System Safety 92(12) : 1686-1700; December 2007

9. T1020 Safety Integrity Assessment Of A Rail Depot Personnel Protection System (DPPS), Issue 1.0; Technis; July 2021

10. F1454_105_A Gap Analysis Report against IEC61508 SIL#2 For ZoneGreen Ltd, Rev A; Wilde Analysis Limited; July 2021

11. Hardware & Software V&V Report for ZG-Smart DPPS; ZoneGreen; March 2022