Product Certification for ‘SIL’ applications

Safety integrity levels:

Safety Integrity Levels (SIL 1, 2, 3 or 4) are used in safety instrumented systems as a measure of dependability and safety performance.

For CML’s overall approach, refer to the information sheet ‘***The CML approach to functional safety certification’***.

Overview of product certification:

To achieve the SIL, the system designer needs to have verified parameters for all the products that form the system (sensors, controllers and final elements). The purpose of product certification is to establish and verify those parameters, together with the safety manual and functional specification, which should all comply with IEC 61508.

Typically, this certification is relevant to product manufacturers.

A typical programme:

An assessment plan is always created to suit the needs of a client’s particular project. Typically, it will have several stages and may look something like the example over the page. Gaining certification by the most straightforward route is the overall objective, getting there in manageable steps.

The initial stage usually involves information gathering by correspondence or a face to face meeting, as convenient. The information will concern the safety function(s), technologies involved and the design and development process used.

Sometimes there is a choice of compliance routes depending on the information is available. For example, a proven in use approach (known in IEC 61508 as Route 2H and Route 2S) may be possible, rather than an assessment of the realisation lifecycle and all the accompanying design techniques and measures.

At each stage, the client’s documentary evidence is evaluated and an interim report can be issued on completion of each stage. Throughout the process, the client can request more or less support from CML as required. Finally, the evaluation report is completed, checked and the certificate prepared.

Product Certification for 'SIL' applications

Continued…

CLIENT ACTIVITIES	**A TYPCIAL PRODUCT CERTIFICATION PLAN**	*CML ACTIVITIES*
Provide information to CML on safety function(s), technologies, application(s), quality management	***STAGE 1*** **Scope and planning**	*Review product information from client and propose optimal certification plan*
Provide hardware failure analysis (e.g., FMEA) and architecture for review, or circuit diagrams / BOM for CML to create the analysis	***STAGE 2*** **Hardware failure analysis**	*Review or create the hardware failure analysis (e.g., FMEA), define the architecture and any system level reliability model using FMEA data*
Provide hardware development process information, including 61508-2 'techniques and measures'; remediate any compliance gaps if required	***STAGE 3*** **Hardware realisation process, techniques & measures**	*Review conformity of hardware development process (lifecycle) and 61508-2 'techniques and measures'*
Provide software development process information, including 61508-3 'techniques and measures'; remediate any compliance gaps if required	***STAGE 4*** **Software realisation process and techniques**	*Review conformity of software development process (lifecycle) and 61508-3 'techniques and measures'*
Provide functional safety management (FSM) information applicable to the product; remediate any compliance gaps if required	***STAGE 5*** **Functional Safety Management (FSM)**	*Review FSM information applicable to the product, its realisation and manufacture*
Write the safety manual (containing failure data and all other relevant information) and the functional safety specification (if separate)	***STAGE 6*** **Safety manual and published FS specification**	*Review the product safety manual and functional safety specification (if separate)*

Product Certification for 'SIL' applications

Complete any remaining remedial actions	**STAGE 7** **Assessment report**	*Complete the functional safety assessment report (hardware, software and FSM)*
None	**STAGE 8** **Technical check and certification**	*Technical check of report; Draft, review and issue certificate*