PRODUCT DESIGN SCOTLAND

A NETWORK OF technology SCOTLAND

PRODUCT DESIGN SCOTLAND TOOLKIT

17 FUNCTIONAL SAFETY STANDARDS AND CONSIDERATIONS DURING THE DESIGN CYCLE

WITH MAGE CONTROL SYSTEMS

IN PARTNERSHIP WITH

filament · product design · The Glasgow School of Art · wideblue making technology happen · SCINTILLA · systolic product development

4c · University of Glasgow Adam Smith Business School · ENIGMA PEOPLE SOLUTIONS · MAGE CONTROL SYSTEMS · NMIS National Manufacturing Institute Scotland · DMEM Delivering Total Engineering · University of Strathclyde Glasgow · UKRI Innovate UK KTN

ABOUT US

With a long tradition of innovation, entrepreneurship and commercialisation, the product design sector is one of Scotland's key industries. Through advances in technology, designers are providing innovative products across a number of global markets, including healthcare, energy, communications and mobility. Integration of these technologies into viable, efficient and commercially attractive products is key, and the partnership between technology and product design is becoming ever more important.

Product Design Scotland, managed by Technology Scotland, the representative body for Scotland's Enabling Technologies Sector, has been established to support the product and industrial design sector in Scotland. The network aims to be the focal point for the community, raising awareness of the critical importance of design to future growth and competitiveness and creating a thriving, collaborative network to drive innovation.

By working with companies and organisations across Scotland, we support the sector through:

- Promoting the value of strategic design to government and industry
- Raising the profile of Scotland's product/ industrial design sector
- Increasing visibility of those operating within relevant supply chains
- Improving competitiveness through collaboration and knowledge exchange
- Creating new networks to shape the future of design in Scotland.

TOPIC INTRODUCTION

During the development of any new engineering system design the design team must consider a multitude of different factors. Apart from designing a product which meets all the functional and aesthetic requirements functional safety must be considered as a priority, as the product will have to comply with international standards to comply with the ALARP (as low as reasonably practical) principle.

Different sectors and legislative bodies have different levels of safety defined by a multitude of differing standards therefore this document will provide an introduction on a sample of these and give guidance on the general principles of navigating and integration of functional safety into engineering designs.

KEY DESIGN METHODOLOGIES

Fundamentally functional safety should be considered throughout the complete design cycle and also be considered in manufacturing and tooling as these can also critically affect functional safety. The following are some of the steps to undertaking and implementing functional safety analysis and design:

- Top level **risk register** should contain a broad overview of potential areas for concern within any design

- During requirements capture and system design applicable standards should be studied to analyse appropriate safety levels for the equipment for the particular industry sector and also any overarching safety standards.

- When the design is underway a failure modes, effects and criticality analysis (FMECA) can be undertaken. This ensures that the design has been analysed for sunny and rainy-day failure modes, and what implications these have for on safety. It also will help define how these potential failures are mitigated and the mitigations recorded in the design data pack.

- During manufacture and test the equipment should undergo tolerance and stress testing to make sure that appropriate safety mitigations in the design function as intended and that the equipment meets specification.

EXAMPLES OF AREAS OF CONCERN IN FUNCTIONAL SAFETY

- Electrical safety (an example of a standard here would be the low voltage directive)
- Explosion risk (an example of this would be ATEX)
- Moving parts causing harm (Directive 2006/42/EC - new machinery directive)
- Eye damage
- Hearing damage
- Loss of life/multiple lives
- EMC radiated and susceptibility
- Functional Safety (IEC 61-508)
- Software and algorithmic integrity (DO-178C)

STANDARDS AND HOW THEY CAN BE MAPPED ACROSS SECTORS

In engineering design and manufacture there are multiple sectors with differing standards. Methodologies and the desired requirements are often common between these differing standards but have to attain differing levels within them, making it sometimes confusing what is needed. So were should a new designer, entrepreneur begin when considering functional safety?

IEC 61-508 is an international standard which has a good overview of functional safety which could be considered appropriate for all industries. This is certainly the case if utilised as a generic framework document that outlines best practice in functional safety. The document outlines two key areas being:

- A process engineering framework to best implement a “safety lifecycle” which ties in well with the systems engineering process which is applicable to the rest of the design

- A statistical approach to look at likelihood of a failure mode against the level of consequence of failure

Overall IEC 61-508 is a very good place to understand functional safety and there are a range of derivative standards that are industry specific and often split functional safety into software, electronics and mechanical design.

At its core 4 SIL levels are defined with level 4 being the most onerous and each SIL level having an associated statistical probability of failure.

When the safety assessment is undertaken, SIL (Safety Integrity Levels) will be defined for the system and components within the system based on the overall target provided by the safety case analysis.

A good example of standards to compare with IEC 61-508 in the software domain would be DO-178C (Aero) ISO26262 (Automotive) these standards use similar methodologies but differ in a number of key areas (including terminology) so it is essential that the appropriate standard be understood. The two standards define safety integrity levels using different levels and terminology. The terms SIL, DAL(development assurance levels) and ASIL will be encountered and should be thoroughly understood by the engineer undertaking the work. These levels can be roughly mapped as follows but the engineer should as always be aware the devil is in the detail.

Safety integrity level	**Aero DO-178C DAL**	**Automotive ISO26262 ASIL**	**Rail CENELEC EN 50126/8/9 SSIL**	**Space ECSS-Q-ST-80C CAT**	**Industrial IEC 61-508 SIL**
Low	DAL E	N/A	N/A	CAT E	N/A
	DAL D	ASIL A	SIL 1	CAT D	SIL 1
Medium	DAL C	ASIL B or C	SIL 2	CAT C	SIL 2
	DAL B	ASIL D	SIL 3	CAT B	SIL3
High	DAL A	None	SIL 4	CAT A	SIL4

MAGE
CONTROL SYSTEMS

MAGE CONTROL SYSTEMS PROFILE

Serving as one of Scotland's largest product design houses, Mage Control Systems is the one-stop shop for bringing innovative ideas to fruition.

The company's core capabilities in complex embedded control systems design, advanced algorithm development, power electronics, IoT & sensing solutions and safety-critical software development is what sets Mage apart from the rest. Simply put – we understand how electronics, software and mechanical modelling work together to meet complex challenges that demand embedded control system solutions.

Mage has a strong history that includes extensive experience within its leadership team stemming from the aerospace & defence sector. The company's capabilities uniquely develop and enhance designs across a wide range of industry sectors, harnessing the reliable and robust practices utilised in the aerospace & defence sector.

Working across a range of industry sectors, Mage Control Systems Ltd.'s expertise and technologies have been developed and honed to sharpen core skills and know-how around:

- products that require to operate in unpredictable and harsh environments (e.g., deep sea, extreme high and low temperatures, at altitude, under shock and vibration).

- highly effective cost engineering coupled with high power density solution designs – value and performance is optimised whilst reducing size and weight.

- successful development of products that not only drive and control precise, complex movement but can also enable essential feedback by utilising intelligent sensing technology.

- consistent performance in meeting stringent requirements for safety-critical designs and needs for military and defence standards etc.

- development of safe, end-user human-interface controlled equipment and sensing/monitoring technology.

- development of complex BUS architectures including RS422, CAN BUS, Ethernet, Ethercat and wireless technologies.

WANT TO KNOW MORE?

PRODUCT DESIGN SCOTLAND'S FULL TOOLKIT SERIES IS AVAILABLE HERE.

CORPORATE SPONSOR

SCINTILLA