

Preparing for ISO 26262

Chris Hills and Günter Glöe have been looking at the draft of the new ISO standard for automotive systems

Functional Safety Management acc. ISO CD 26262

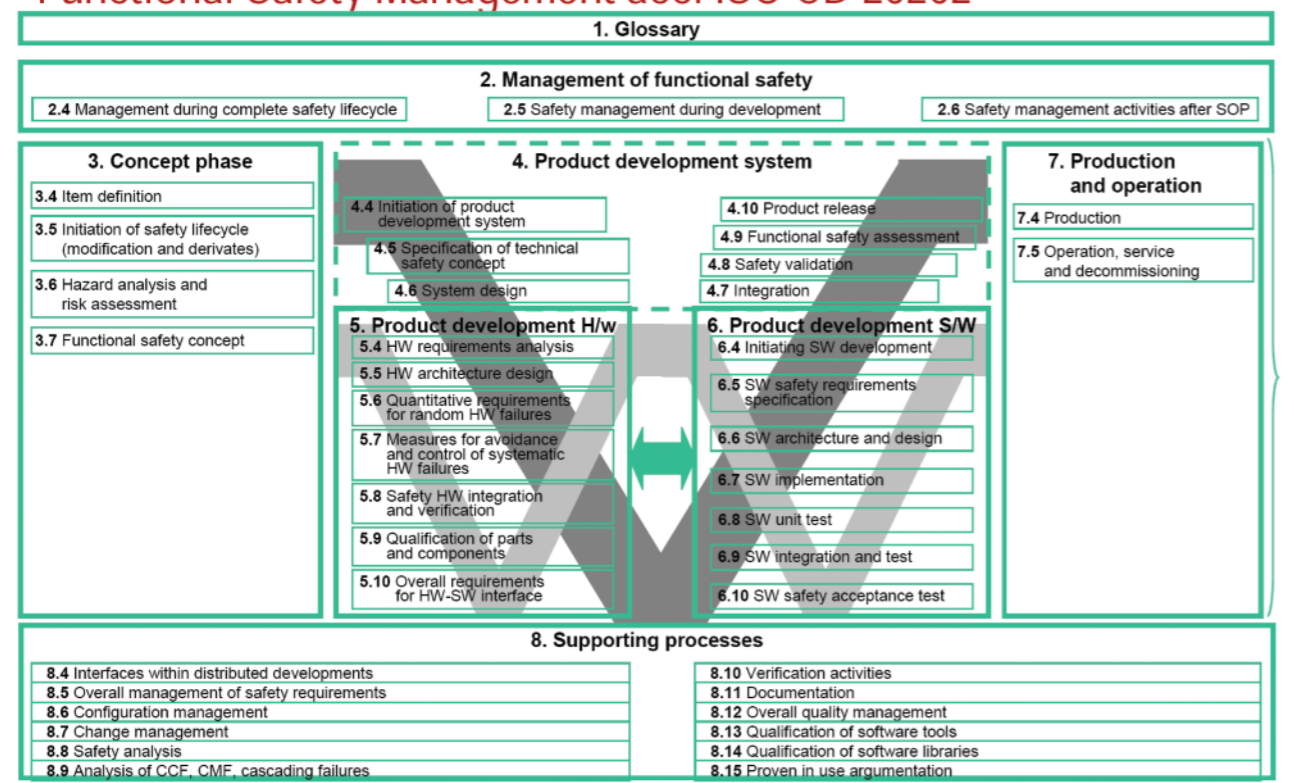


Fig. 1: Overview of ISO 26262

A new standard – ISO/IEC 26262 DIS: Road Vehicles, Functional Safety – is out for discussion through the ISO and national standards bodies. While one expert in the field has suggested that formal ratification is a long way off (“not in my working life-time”) it is still a significant step forward for safety and anyone who is working in systems for the automotive sector should be aware of the standard, its contents and the implications for system development and the product life cycle.

So why do we need a standard? Nobody is knowingly going to build unsafe systems, are they? The argument is the same for the whole area of safety critical systems: a common standard should provide an agreed and objective measure on how safe a system will be in service. As part of this, a standard also provides a standard vocabulary to describe the elements of a system and their relationships.

Starting point
For electrical and electronic systems, the starting point is normally IEC 61508 – Functional safety of electrical, electronic and programmable electronic safety-related systems. This, like all the standards in this area, is a multi-volume document, most parts of which were ratified in 1998. Within 61508 a key element is the concept of safety integrity level (SIL). SILs range from SIL1 (lowest) to SIL4 (highest) and are indicators of probability of failure on demand (PFD) with SIL1 being highest PFD (0.1-0.01) and SIL4 lowest (0.0001-0.00001) or, if you prefer, their inverse the risk reduction factor where SIL4 has the highest RRF (10,000-100,000) and SIL1 the lowest.

Other sectors have developed their own standards based on 61508, for

example the nuclear industry has 60880, 61513 and 62138 and the railway industry uses 50128. Now the automotive industry, including automotive manufacturers and national research centres from Austria, France, Germany, Italy, Japan, Sweden, the UK, and the USA, has created 26262. Ten volumes make up the standard (Table 1), which is designed for safety-related systems that include one or more electrical or electronic systems and that are installed in series production passenger cars with a maximum gross weight up to 3500kg. Since the standard is focussed on series production cars, it includes, as part seven, requirements for the production of systems, something not found in 61508, which is aimed more at industrial equipment and process plant, which are normally one-off or very low numbers. Production is seen in the context of the automotive safety lifecycle (management, devel-

“One expert in the field has suggested that formal ratification is a long way off (“not in my working life-time”)

ISO 26262 has ten parts

- ISO 26262-1: — Road vehicles – Functional Safety — Part one: Vocabulary
- ISO 26262-1: — Road vehicles – Functional Safety — Part two: Management of functional safety
- ISO 26262-3: — Road vehicles – Functional Safety — Part three: Concept phase
- ISO 26262-4: — Road vehicles – Functional Safety — Part four: Product development: system level
- ISO 26262-5: — Road vehicles – Functional Safety — Part five: Product development: hardware level
- ISO 26262-6: — Road vehicles – Functional Safety — Part six: Product development: software level
- ISO 26262-7: — Road vehicles – Functional Safety — Part seven: Production and operation
- ISO 26262-8: — Road vehicles – Functional Safety — Part eight: Supporting processes
- ISO 26262-9: — Road vehicles – Functional Safety — Part nine: ASIL-oriented and safety-oriented analyses
- ISO 26262-10: — Road vehicles – Functional Safety — Part ten: Guideline on ISO 26262

Table 1: 26262 structure

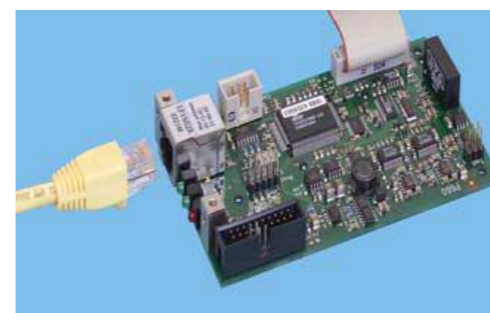
Continued on page 22

Automated Programmable Power Supplies



33 models with different Voltage and Current ranges up to 6kwatts. We can design and configure turnkey systems to your specification.

- *Very Low Ripple
- * 3 phase, PFC
- *Easy Master/Slave
- * Output On/Off Button
- *Excellent dynamic response on load changes



Various program options : RS232,IEEE488,Analogue Inputs.

Ethernet Interface with integrated sequencer. Car battery simulation, Repetitive testing, Automotive applications. Possibility to create loops, subroutines,ramps etc. Works as PLC for stand-alone automation.

150w to 6k Watt Modular Power Supplies

www.safety-power.com Tel: 01252 515565 New 2007 catalogue now available



Enquiry No: 8

- Initiation of product development at the software level
- Specification of software safety requirements
- Software architectural design
- Software unit design and implementation
- Software unit testing
- Software integration and testing
- Verification of software safety requirements

Table 2: Product development - Software

opment, production, operation, service and decommissioning).

SILs
The standard has set up a different ap-

proach to SILs, using instead ASILs (automotive safety integrity levels). To make the difference clear, ASILs run from A (lowest) to D (highest) and there is no one-to-one matching be-

tween 61508 SILs and 26262 ASILs. The approximate correspondence between SILs and ASILs is that ASIL A is approximately SIL1, ASIL B is approximately SIL2 and ASIL C falls between SIL2 and SIL3 and ASIL D is approximately SIL3. There is no equivalent in 26262 to SIL4.

Development model

Parts three to six in the standard cover the development process, from concept (part three), through system level (part four), hardware development (part five) and software development (part six). The standard uses a V model for system development with hardware and software development also following their own V models. Table 2 shows the phases recommended for software development. For each phase of the development (clause in the standard) there is a standard structure of objectives, general, inputs, requirements and recommendations, and work products (which normally form the inputs to the next phase). It is the requirements and recommendations that are the core of the standard. An example from part six is:

- 5.4.8: The criteria to be considered when selecting a suitable modelling or programming language are:
 - a) an unambiguous definition; Example syntax and semantics of the language
 - b) the support for embedded real time software and runtime error handling; and
 - c) the support for modularity, ab-

straction and structured constructs.

- Criteria that are not sufficiently addressed by the language itself shall be covered by the corresponding guidelines, or by the development environment.
- Note 1: The selected programming language (such as Ada, C, C++, Java, Assembler or a graphical modelling language) is to fulfil the criteria given in 5.4.6. Usually programming or modelling guidelines are necessary to fulfil these criteria.
- Note 2: Assembly languages can only be used for those parts of the software where the use of high-level programming languages is not appropriate. Examples are low-level software with interfaces to the hardware, interrupt handlers and time-critical algorithms.

It is interesting to note that graphical modelling is acceptable.

Matching ASILs

Within the requirements and recommendations are tables that match requirements to the different ASILs, ranging from "highly recommended for this ASIL", through "recommended for this ASIL" to "no recommendation for or against its usage for this ASIL".

In the standard's Table 9 in part six: Design principles for software unit design and implementation, for example, initialisation of variables is highly recommended for all ASILs. Limited use of pointers is highly recommended for ASIL D, while for ASIL C and ASIL B it is only recommended and for ASIL A there is no recommendation. Table 9 also has a note: "For the C language, (Misra C) covers many of the methods listed in Table 9." A note is only for guidance in understanding, or for clarification of, the associated requirement and shall not be interpreted as a requirement itself.

Industry uptake

One important element in the likely industry uptake of 26262, apart from the already strong support of the automotive manufacturers, is that in parallel to the work on the standard has been the development of Autosar, an open software architecture for automotive applications. The intention is that Autosar will provide a common software infrastructure, with standard interfaces, to make the development of software and systems modular, scalable, transferable and reusable. Autosar starts from software components, each carrying out a specific function. These go through an Au-

“You have until the end of October to look at 26262 if you want to make your views known to the BSI

tosar interface to the Autosar runtime environment, including OS, drivers and so on, and run on the underlying hardware. This approach decouples the applications and their hardware, making it easier, for example, to transfer applications to different hardware or to upgrade applications.

Autosar also presumes a development methodology, which can be easily mapped into the methodology that is defined within the 26262 standard.

Commenting

If you want a copy of the draft standard, you can download it from the BSI web site; although a complete set will set you back £200 unless your organisation is already a BSI member. You have until the end of October to look at 26262 if you want to make your views known to the BSI. ■

Chris Hills is CTO for Phaedrus Systems and a member of the Misra-C panel and Günter Glöe is CTO for Cats Software Tools

Objectives General Inputs to this clause Requirements and recommendations Work products

Table 3: Structure of each clause

automotive electronics

SPECIAL REPORTS
October-November 09 Issue

- Infotainment
- FPGAs
- Flexray, Can and Lin

www.automotive-electronics.co.uk August/September 09

automotive electronics

CODE GENERATION
Choosing the right tools

RESEARCH & DEVELOPMENT
Pay as you drive trial

PREPARING FOR ISO 26262
TESTING MULTIPLE ECUs

INSIDE THE MERCEDES E CLASS

Just think...

Thousands of potential customers could be reading your advert now, instead of ours!

Tel: +44 (0)1582 722460
david@automotive-electronics.co.uk
automotive-electronics.co.uk

maxell INDUSTRIAL AUTOMOTIVE

INDUSTRIAL BATTERIES
HEAT RESISTANT CR BATTERIES
OPERATING TEMPERATURE RANGE FROM -40° UP TO 150°
SUPERIOR LEAK-RESISTANT CHARACTERISTICS
PERFECT FOR TPMS AND ELECTRICAL TOLL EQUIPMENT
DESIGNED LIFE TIME 10 YEARS

OPTICAL COMPONENTS
ULTRA WIDE ANGLE LENS
90° - 190° HORIZONTAL VIEW ANGLE
HIGH WATER AND HEAT RESISTANCE AND ANTI VIBRATION
PERFECT FOR BACK MONITORING SYSTEMS

FUNCTIONAL MATERIALS
ADHESIVE TAPE
MADE SPECIFICALLY FOR AUTOMOTIVE, HOME OR INDUSTRY USE
ELECTRO MAGNETIC SHIELDING AND ELECTRIC RESISTIVITY
HIGH ADHESION WHEN COMPARED WITH OTHER ADHESIVE TAPES

MOULDING SERVICES
MAXELL MOULDING SERVICES
OFFERS PLASTIC INJECTION MOULDING FOR A WIDE RANGE 'ABOVE AND BELOW' THE BONNET
PAD PRINTING AVAILABLE FOR DRIVER CONTROLS
ACCREDITED TO ISO STANDARDS

WWW.MAXELL.EU