

The human machine interface

For more than 100 years **DEUTA** has been developing and producing dependable components for safety systems in the railway sector, while considering the entire life-cycle of a product

Clients with safety requirements can expect the company to supervise projects all the way through from development, production and commissioning to a full after-sales service.

The safety of people is the focal point of DEUTA's product development. Its reliable components deliver safety functions up to a safety integrity level (SIL) 4 - an offering that is becoming increasingly important.

An SIL product is required when the issue of 'functional safety' comes into play. This is an area concerned with technical solutions to safety-related functions, in order to avoid damage to people and the environment. These safety-triggered reactions should also function when the monitoring circuit malfunctions due to, for example the drop-out of a relay.

The area of 'functional safety' is therefore very large, and DEUTA innovations cover the complete SIL-spectrum of vehicle velocity measurement, recording and visualisation.

IconTrust® can be trusted

Especially applicable in the field of visualisation Dr. Rudolf Ganz, managing director of DEUTA-WERKE and his team have developed *IconTrust®*, a patented electronic safety circuit for human machine interfaces, which by means of a simple, innovative 'fingerprint' comparison monitors the correctness of display data. In addition, the technology enables safe data entry using touch-based operator panels.

Because drivers of modern (high speed) trains carry a large burden of responsibility for passengers, cargo and the expensive rail system itself, and operational errors can have serious consequences, organisational and technical measures must be taken which ensure that the data displayed to the driver is correct at all times, ensuring that the decisions he or she takes are optimal.

Human-machine interface

Today, PC driven TFT display units are also increasingly used in the safety-relevant area of human-machine interfaces in trains. The PC technology used has economical and ergonomic advantages in that several functional and comfort elements can be integrated in one user-friendly device, thus saving

construction space. The disadvantage is that potential failure modes can stay undiscovered, leading to the display of wrong data and consequently an operation error. Examples are a failure in the graphic memory, the graphic controller or its software, which results in a frozen display or a data corruption. The driver will not notice the display failure as long as he or she has 'one' displayed graphic, which appears plausible. Since the driver cannot validate this in real-time while driving, but has to rely on it at all times and in all conditions, a cockpit display is therefore safety critical.

Many applications require - in line with the certification process - a corresponding verification and assessment process together with appropriate technical measures taken to achieve a defined SIL.

In fact, a random survey of current approaches shows that these measures do not go far enough as they reveal or avoid only parts of the error sources in the units. For example, errors in the graphics memory, graphics controller or its software, which may cause the screen to freeze or color shift, in the majority of cases remain hidden. Also potential errors of the central processor unit, which computes the data and finally generates the graphical representation, have to be

reviewed.

DEUTA has been producing HMI terminals for railway vehicles for around 20 years and in *IconTrust®* it has developed a safe multifunction terminal.

Other kinds of technical approaches have existed for SIL-compliant terminals. These were classed as extremely cost intensive as every change of application software is accompanied by a complex modification process and requires verification.

IconTrust® ensures that the displayed data is verifiably up-to-date and correct, without the actual application for the display of information needing to be subjected to SIL verification. Because of this independence, the circuit has a multitude of uses without the extensive post-qualification and documented evidence of conformity usually associated with product and process modification.

Hitachi project

An HMI display with *IconTrust®* is assessed and certified according to SIL 2 to be used in the UK on a Hitachi rail vehicle combined with a Hitachi European Vital Computer (EVC). In this project *IconTrust®* can simultaneously and independently, monitor more than 30 areas, including overlapping areas. When anomalies occur, a corresponding





be used in other types of display. There is increasing discussion about SIL2 for large control centre displays or projector systems. Other industries have conveyed an interest as in principle, the solution is of use wherever safe display and safe operation is needed.

Even in cases where the customer relies on PC technology but not on the proven DEUTA technology, the application can be ported to a PC compatible platform and then upgraded and backed-up with IconTrust®.

Safety Management Group

Complete SIL systems consisting of sensors, controller and actuators (e.g. human machine interfaces) are becoming more and more important in future. In order to ensure a safety integrity level, DEUTA customers are supported by a Safety Management Group. Several development engineers have been trained to become safety engineers and, additionally, safety managers have been appointed to manage communications with assessors. This is also in response to the requirements of the new CENELEC standard DIN EN 50128. The system characteristic is variable and ranges from simple product combinations to high-end safety solutions. Multi-Function Recorders REDBOXsafe, Sensors, e.g. the axle-mounted sensor DF 16 and analogue indicators e.g. the ESG 14 rounding-off the SIL system with safe systems.

*For more information contact Dr. Rudolf Ganz, managing director DEUTA-WERKE.
Tel: +49 (0) 2202 958 100
www.deuta.com*

safety reaction is triggered. For every individual area, in every image refresh cycle the displayed image is analysed and compared with the value of the respective input signal. The patent pending system ensures the information is demonstrably up-to-date and correct without the actual application for displaying the information being subject to a verification procedure. Because of this independence IconTrust® enjoys almost limitless applicability.

The safety case of SIL approval with IconTrust® technology is independent of the operating system, software development tools or hardware configuration. It is even possible to reuse existing application software modules and upgrade it to a 'SIL equipment'. The result is an economic advantage in retrofit projects with new SIL requirements.

The lifetime of a project of typically 15-30 years is much longer than any availability of electronic components. Due

to obsolescence, the processor/chipsets have to be changed several times. The effect on projects with SIL requirements is significantly reduced by IconTrust® technology because processor, chipsets, etc. do not have to be defined in the safety case.

IconTrust® can be used as a Panel PC, a TFT monitor or projector. In the control room of train supervision systems, large TFT screens are used that display track, train and signalling information. An ongoing discussion about the safety relevance of this information may result in SIL levels >0 requirements in the future. To achieve this IconTrust® can also be integrated as an add-on or design-in into existing devices. It can be a step in change of paradigm towards SIL >0 approved control centres.

The use of IconTrust® boards is not limited to human-machine interfaces and, with minor modification, they can

