White Paper

# Rösberg Engineering: Functional Safety Management in the Process Industry

Edited by on 12. Jul. 2017

Treating the cause and not the symptoms For plant owners in the process industry, cutting corners on safety to reduce costs can be a very expensive mistake. One dramatic example is the oil spill in the Gulf of Mexico, which was a direct consequence of the explosion on the oil platform Deepwater Horizon. One of the main factors that contributed to the explosion was the sealing of the bore hole: despite warnings from experts, a cheaper solution was adopted that involved a higher risk of escaping gas. In retrospect, this would have been a negligible investment compared to the damages paid to the US government, which ran into of billions of dollars in double figures. Not to mention the damage to the company image, or the appalling effects on the environment and on people that cannot be quantified. Thus in plant construction, whether for the chemical industry, for firing technology or for incineration systems, systematic hazard assessment is essential.

Not only may false economies prove to be expensive in many different ways – they can also lead to legal consequences. There are clear legal requirements regarding the implementation of functional safety measures: in Germany, for instance the Industrial Safety Regulation (Betriebssicherheitsverordnung, BetrSichV) obliges operators of plants requiring compulsory monitoring to ensure the safety and protect the health of their employees. It lays down clear guidelines on hazard assessment and protective measures, and explicitly names the elements of infringements and criminal offences. Nevertheless, for reasons of

cost many safety measures are not implemented at all, or are only implemented half-heartedly. Other stumbling-blocks are a lack of knowledge on the topic of functional safety, or confusion about finding one's way through the complex "jungle" of standards and guidelines. Here, establishing a Functional Safety Management (FSM) system can help not only to avoid major safety risks, but on a "smaller" scale can reduce downtimes, meaning it pays off doubly. But let us consider one point at a time.**Implementing functional safety in practice**What exactly is FSM? It is a systematic procedure that can help to avoid potential failures even at the stage of plant planning and development. The failures that occur in a plant can be generally divided into two groups: stochastic and systematic. Stochastic failures occur by chance and are not able to be prevented beforehand. One example is the unforeseeable failure of an electric component. If something like this occurs it is a case of minimizing the damage that could be caused by malfunction, and ensuring sufficient safety in advance by redundancy concepts. Whereas stochastic failures occur randomly and cannot be prevented in advance, systematic failures can be recognized beforehand and their consequences are foreseeable. For instance, an error in the instructions for inspecting a protection system results in an inspection that is wrongly carried out. Thus the intended function of the protective system is not ensured and as a result there may be damage to the plant, to the environment and, in the worst case, to people.Systematic failures of this kind therefore need to be anticipated and avoided. A study by the Health and Safety Executive (HSE) demonstrates that this is worth doing. In Great Britain the HSE regulates major areas of health and safety at work. The study investigated 34 accidents that caused substantial damage, and came to the conclusion that more than 60 percent of these failures were built into the plant before it was commissioned (**Fig. 1**). Around 25 percent of failures arose through installations or changes made after commissioning. Only 15 percent of the failures that occurred had a stochastic cause.**How can a Functional Safety Management System help?**The main cause of systematic failures is generally: people. Thus it is important to support people during the planning and implementation stage, in order to avoid these errors – which are mainly down to the management – as effectively as possible. This is where FSM systems help. They are based on legal regulations, guidelines and standards. An FSM system is built on the "safety life cycle" as defined in DIN EN 61511. **Fig. 2** shows all the stages of hazard and risk assessment, from planning to commissioning and ending with decommissioning. Right at the beginning, people responsible for each of the total of eight phases are defined in a safety plan. In each of these phases the FSM system uses two main instruments: process definition (left-hand bar: Management and Evaluation of Functional Safety) and control of whether the process definitions are actually adhered to (right-hand bar:

Verification).**Process definition and control**Process definitions are created for each individual phase of the safety life cycle. For each phase the hazard level is also defined. That in turn influences who should perform verification. Where the hazard level is low, this can be done by employees within the company, but the higher the hazard level, the more independently the verification must be conducted, and for extremely dangerous processes the “four eyes” principle applies. The question of who is allowed to verify which processes is decided not only by independence, but also by competence. Both specialist qualification and professional experience in the particular area play an important role here.Style sheets similar to quality management sheets are used for control. With these specially prepared lists, potential causes of failure can be systematically checked. When compiling these checklists for a particular plant, specifications from various standards can mainly be used. Individual adaptations are only necessary in a few cases. The aim of the catalogues of questions in these style sheets is to eliminate all possibilities for different interpretation as to whether, and how, tasks have been carried out. **Fig. 3** shows an example of an excerpt from a style sheet for phase 1 of the safety life cycle for verification of the task concerned. After each phase a hk is made of whether all tasks have been performed in compliance with the rules. Only then will the Safety Manager give his “all clear” for the next step.
**Making work easier and improving safety at work**Dipl.-Ing. (FH) ***Andre Günther*** (**Fig. 4**) works as Product Manager for Functional Safety at **Rösberg Engineering GmbH**. He adds: “Increasing safety is often thought to mean doing without freedom and flexibility. This is exactly what FSM is not trying to achieve. A well-set-up FSM system helps users to develop the best and safest solution as simply as possible.” He and his colleagues support plant constructors and operators in all tasks involving functional safety and also help with the integration of an FSM system. Plant operators who have previously installed a quality management system according to DIN EN ISO 9001 are already part of the way there. Günther explains: “The departments and their employees are then already accustomed to defined processes and the use of style sheets. And individual processes are already in place, such as e.g. steering and document revision.” The Rösberg team help with the integration of QM and FSM systems by defining relevant interfaces. Aber auch in anderen Fällen unterstützen sie natürlich beim Aufsetzen eines FSM: from comprehensive advice and document preparation to the final rollout. Rösberg’s employees have the necessary qualifications and also the professional experience required by the relevant standards. Among other things, the enterprise has developed its own style sheets verified by the TÜV (German safety and standards institution). These can be made available to the customer after consultation. Günthers sums up: “Although the legal requirement for functional safety is clear, many people still hesitate to adopt an FSM system.

By providing services in this area, we want to help lower the inhibition threshold so that implementation becomes straightforward, feasible and preventative – and people are not forced to learn from their mistakes when it is too late.”***Rösberg Engineering GmbH****Founded in Karlsruhe in 1962, offers tailored automation solutions created by around 100 employees working at five locations in Germany and China. Their scope includes basic and detail engineering for the automation of process and production plants. Rösberg also has extensive project planning and application experience in the use of all usual brands of programmable logic controllers (PLCs).Many companies also put their trust in Rösberg for the configuration, delivery and commissioning of distributed control systems, as a manufacturer-neutral system integrator.In the area of information technology, Rösberg has enjoyed international success for more than 25 years now with its I&C-CAE system ProDOK. With LiveDOK NG, Rösberg presents a system which offers efficient access to electronic plant documentation, and ensures maintenance and consistency of documentation over the whole life cycle of the plant. The app LiveDOK.mobile enables online/offline access to plant documentation on mobile devices, including Ex-Zone access. Plant Assist Manager (PAM) supports the user in documenting and carrying out optimized workflows. Under the name “Plant Solutions”, ProDOK, LiveDOK and PAM support not only the engineering, construction and modification of plants, but also continue to support the plant throughout its operative phase. All software products are now in the “Next Generation” (NG), meaning that they use state-of-the-art technology and offer many possibilities for visualization, modularization, databases and cloud applications.***The Authors**