Safety Instrumented System Engineering Capabilities

The Right Balance of Industry, Technology and Project Management Expertise

Managing risk with global standards

Companies that correctly plan for and manage the operational risks inherent to industrial processes avoid exposure to production outages, equipment damage, environmental incidents, injury to personnel and loss of life.

International standards for the evaluation and design of safety functions have been developed. The IEC 61511standard is aimed directly at total process plant operations and covers the whole lifecycle of the safety system from concept to operation, maintenance, function testing, through to decommissioning.

Emerson Process Management offers the total solutions to provide the certified hardware, software, and engineering services needed to meet the requirements of the safety system lifecycle, helping you to analyze the risk associated with each loop or Safety Implement Function (SIF).

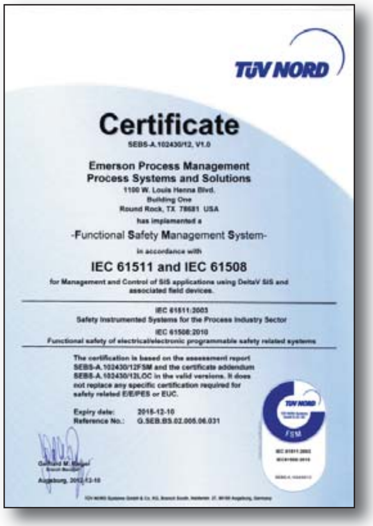
Certified safety process

Emerson utilizes a Functional Safety Management System as defined by the IEC 61511 standard.

This TÜV certified system covers:

- Management of functional safety
- Safety lifecycle structure/ planning
- Verification
- Design and engineering of SIS to decommissioning

Emerson's certified function safety experts utilize this process and their expertise with the latest safety technologies and proven practices to help you define and implement a safety system that is consistent with the most stringent demands for protection, risk reduction and reliability.



TÜV NORD

Certificate

SEBS-A.102430/12, V1.0

Emerson Process Management
Process Systems and Solutions
1100 W. Louis Henna Blvd.
Building One
Round Rock, TX 78681 USA

has implemented a

-Functional Safety Management System-

in accordance with

IEC 61511 and IEC 61508

for Management and Control of SIS applications using DeltaV SIS and associated field devices.

IEC 61511:2003
Safety Instrumented Systems for the Process Industry Sector
IEC 61508:2010
Functional safety of electrical/electronic programmable safety related systems

The certification is based on the assessment report SEBS-A.102430/12FSM and the certificate addendum SEBS-A.102430/12LOC in the valid versions. It does not replace any specific certification required for safety related E/E/PES or EUC.

Expiry date: 2015-12-10
Reference No.: G.SEB.BS.02.005.06.031

Gerhard M. Rieger

Augsburg, 2012-12-10

Certified safety experts

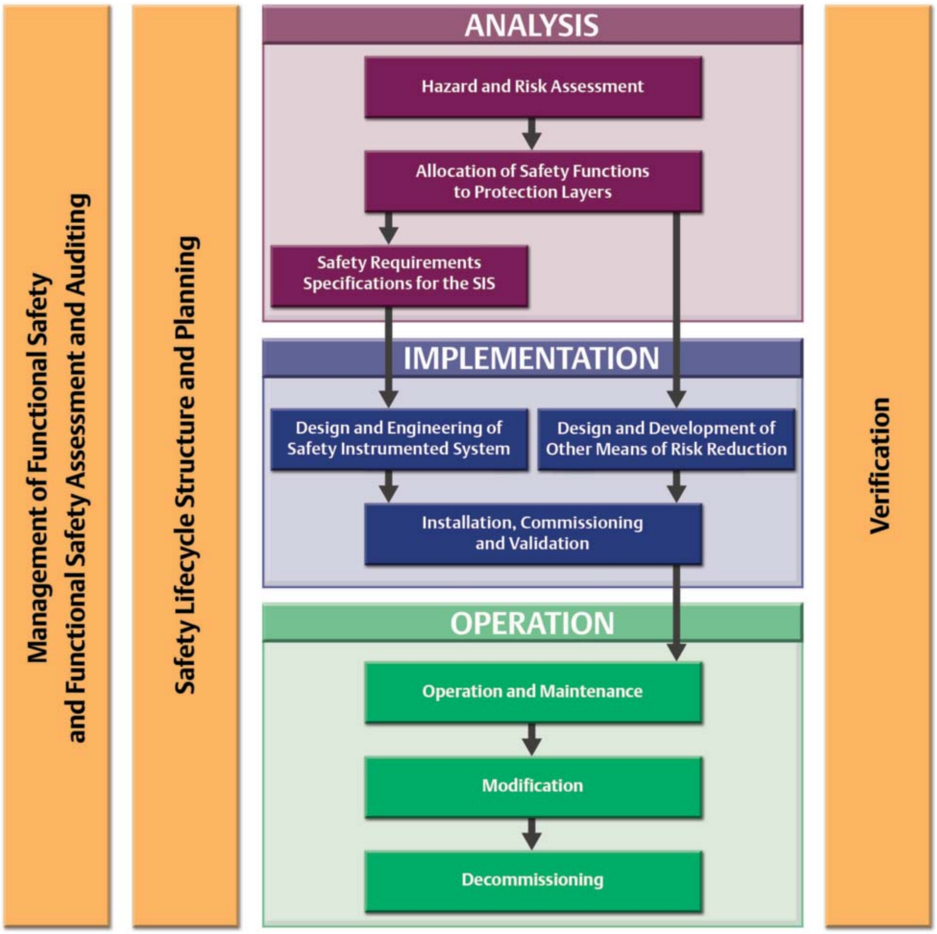
Emerson has committed the resources to become the first safety systems provider to develop TÜV-certified procedures in alignment with IEC 61511. In additon, all employees involved with safety system engineering and development are required to complete extensive safety training and Emerson Certification.

Many of our engineers and technologists have also completed a rigorous competency qualification for system design engineers known as the Certified Functional Safety Expert (CFSE) exam. This certification requires a minimum amount of experience in Safety Instrumented Systems (SIS), as well as successful completion of a comprehensive examination.

DeltaV SIS

EMERSON™
Process Management

Scalable Safety Lifecycle Management


Management of Functional Safety and Functional Safety Assessment and Auditing
Safety Lifecycle Structure and Planning
ANALYSIS
Hazard and Risk Assessment
Allocation of Safety Functions to Protection Layers
Safety Requirements Specifications for the SIS
IMPLEMENTATION
Design and Engineering of Safety Instrumented System
Design and Development of Other Means of Risk Reduction
Installation, Commissioning and Validation
OPERATION
Operation and Maintenance
Modification
Decommissioning
Verification

Reducing failures from the start

A good design that adheres to IEC 61511 will reduce safety incidents caused by hardware or systematic failures in a safety system. Having a team, whose processes are certified to follow IEC 61511—involved early in the project—will ensure that systematic faults, caused by poor specifications or poor engineering, are reduced or eliminated altogether.

According to the Health and Safty Executive (HSE) 80% of all SIS-related failures occur before startup. Omissions in the design of a safety loop or Safety Instrumented Functions (SIF) could remain undiscovered until an incident occurs. A majority of incidents are preventable is a systemic risk-based approach is implemented.

Scalable safety lifecycle approach

Different processes require different levels of safety support so from Front End Engineering Design onward, Emerson can support you in the different phases of a lifecycle.

Conceptual Process Design and Front End Engineering

These are the critical considerations that are typically taken into account during this early process.

- **Application Standards**—these are the standards the project will follow such as IEC, ISA, company and other standards.

- **Conceptual Architecture**—once the standards are defined and training has been completed, conceptual design requirements are considered.

- **Process Requirements**—a critical step in the discovery of vital process information and the assignment of work.

- **Configuration**—the discussion of who will be doing what scope of work, and how it will all be tested and verified yields a Safety Verification Plan.

- **Safety Requirements Specification (SRS) document**—the philosophy, operation, and functionality of your SIS is recorded in the SRS. The SRS also specifies the safety requirements standards to help you follow IEC 61511 best practices.

The SRS should contain information that will form the basis of the design. This includes: things like desired proof test intervals, acceptable mean time to failure, process safety time,, hardware fault tolerance and diagnostics. It should also include process requirements, like maintenance bypass, start-up bypass, resets, and HMI interactions.

Detailed Design/Build

The breadth of Emerson's process technology and expertise means that you have a single source for all your safety project needs, integrated to ensure compatibility.

SIS Detailed Design

Detailed Design and Engineering deals with the software and hardware Detailed Design—turning the Conceptual Design into something that can be efficiently and unambiguously coded and tested.

SIS Build, Integration and FAT

SIS Build, Integration and Factory Acceptance Testing (FAT) deals with the coding of the software, building the hardware, and testing these before delivery.

Installation and Start-up

SIS Installation and Commissioning

During this phase, the system is delivered to the site, installed (possibly tested), commissioned and then validated.

SIS Safety Validation

In validation we exercise every function defined in the Safety Requirements Specification to ensure that the whole system works as it should. This is a test of every part of the system, from the sensors, through the logic solvers, to the final elements. Only once this has been completed can the plant start up.

Provision of Functional Safety

SIS Operations and Maintenance

Operations and Maintenance deals with managing the SIS throughout its life and ensuring that the required level of risk reduction is achieved. This is usually achieved by partial or full testing. A full test of a safety function is known as a proof test—this ensures that the SIF operates as efficiently as it did when the plant was first validated prior to start-up.

During this phase the demand rate and component failure rates will be logged and periodically compared with the assumptions made during the design of the SIS to ensure that those assumptions were valid.

Modification and Updating

SIS Modification

Modification and Updating leads us back into the analysis phase. Any modification requires redesign, and this means that a safety analysis must be performed. Decommissioning might be considered a special type of modification—careful planning and execution are required. Hazards must be managed until they are no longer present.

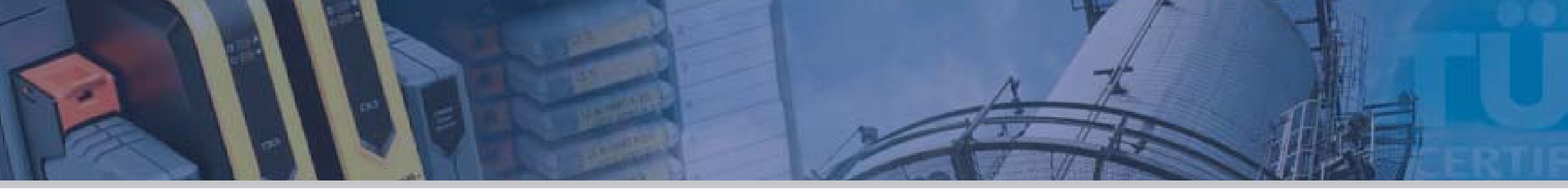
Verification and Documentation

Verification—demonstrating for each phase of the relevant safety life cycle by analysis and/or tests, that, for specific inputs, the outputs meet in all respects the objectives and requirements set for the specific phase.

Validation—demonstrating that the Safety Instrumented Function(s) and Safety Instrumented System(s) under consideration after installation meets in all respects the Safety Requirements Specification.

Safety Lifecycle Capabilities

- Identify potential hazards
- Allocate safety functions to layer of protection
- Determine if SIS is required
- Identify levels of tolerable risk and select target SILs
- Produce Safety Requirements Specification for SIS
- Select technology, architecture, and proof test philosophy
- Verify target SIL for each Safety Instrumented Function
- Detailed design of: SIS field devices, SIS logic solvers, SIS software
- Design verification—verify SIL targets have been met for each SIF
- Produce installation, test, and commissioning documentation—logic solver and field devices
- Produce operations and maintenance documentation—logic solver and field devices
- Logic solver hardware build and verification
- SIS configuration and safety function testing
- Verification of as-built functionality
- Produce as-shipped documentation
- Install SIS field devices
- Install SIS logic solvers
- Integrate SIS into BPCS as required
- Verify installation
- Commission SIS
- Validate SIS
- Complete Function Safety Assessment
- Operate and maintain SIS in accordance with documented procedures
- Perform proof tests as defined in the design to verify operation of the SIS
- Check assumptions: Demand rate and dangerous failure rate used in design vs actual
- Assess scope of modification (e.g. change a parameter or update configuration)
- If change does not affect safety case then make change, and complete all required verification and change management activities
- If change is significant then repeat the Safety Lifecycle, starting at Step 1, Conceptual Design and Front End Engineering

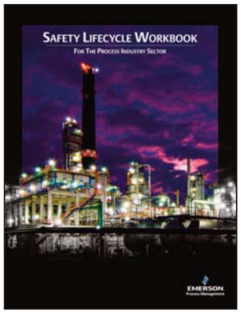


Our TÜV-approved processes provides a documented verification that each process step
was completed throughout all phases of the safety lifecycle. Each step of the design and engineering process is reviewed and documented to confirm that compliance to IEC 61511 mandatory clauses have been accomplished.

Globally balanced capabilities

When time is of the essence, when failure is not an option, and when you need the best total approach, call Emerson. Whether your project is large or small, brand new or a modernization project, you can depend on Emerson. Our balance of industry, technology and project management expertise is proven in the many successful projects we have delivered around the globe. To read more about these successes, visit **www.EmersonProcess.com/ home/news**.

We recommend the following:



Safety Lifecycle Workbook for the Process Industry Sector

DeltaV SIS™ for Process Safety Systems
Smart, Modern Safety System—for the Life of Your Plant
TÜV
DeltaV SIS
EMERSON
Process Management

DeltaV SIS™ for Process Safety Systems
Smart, Modern Safety System—
for the Life of Your Plant

Emerson Process Management
1100 W. Louis Henna Blvd., Bldg I
Round Rock, TX 78681-7430

www.DeltaVSIS.com

The contents of this publication are presented for informational purposes only, and while every effort has been made to ensure their accuracy, they are not to be construed as warrantees or guarantees, express or implied, regarding the products or services described herein or their use or applicability. All sales are governed by our terms and conditions, which are available on request. We reserve the right to modify or improve the design or specification of such products at any time without notice. For Emerson Process Management trademarks and service marks, go to http://www.emersonprocess.com/home/news/resources/marks.pdf

DeltaV SIS

EMERSON™
Process Management