


SIEMENS

Ingenuity for life

A woman with blonde hair, wearing a yellow dress and a patterned headband, is holding a young child in her arms. The child is wearing an orange dress and purple shorts. They are in a field of yellow flowers under a bright, sunny sky. Three yellow balloons are attached to a string held by the child. The scene is bright and cheerful, with a lens flare effect from the sun.

Maximum Process Safety through Tank Overfill Prevention

[siemens.com/process-safety](https://www.siemens.com/process-safety)

Over the years there have been a number of high profile losses of primary containment at fuel storage facilities. Perhaps the most notable incident in recent times was the Buncefield explosion in the UK back in 2005. The consequences of this incident were considerable but, given different circumstances, it could have been much worse. If the explosion had occurred at a time when more people were present fatalities would have been likely. Still there were significant injuries and extensive damage to the environment, the site and adjacent buildings. Significant financial costs incurred because of the damage, lost production, fines and reputational loss.

The report of the Buncefield incident led to a number of recommendations, including the need for independent, dependable Tank Overfill Prevention systems for fuel storage sites. These recommendations further stated that these systems should be considered as safety related systems and risk assessed, furthermore implemented, operated and maintained in accordance with the requirements of the best practice functional safety standard IEC 61511.

These recommendations have also been adopted in the USA in the latest version of the API 2350 standard.

In line with best practice these systems are expected to be separate and independent from the associated tank gauging and control systems and also to be automatic, so as not to require any interventions from the operator.

Application requirements

Ensuring safety when storing and transferring hydrocarbons is of the utmost importance. Any mistake can jeopardize people, facilities, the environment and operations.

The Tank Overfill Prevention system should reliably detect an overfill situation in the tank in order to take action to stop the overfilling (e.g. by closing a valve to stop the flow into the tank). The system also has to have an alarm function for the operators.

Distributed versus Centralized

Tank Overfill Prevention can be applied to a single tank, a small group of tanks or a large tank farm such as those found at large ports and fuel depots. The automation and safety must be capable of being easily distributed because those tank farms are often spread over large and hazardous areas.

There are various strategies that can be employed. For example:

- Each tank can be hard wired to a central control room.
- Controllers can be centrally located but with remote I/O to each tank or group of tanks.
- Controllers and I/O can be distributed to each tank or group of tanks.

It can be helpful to combine control and safety into the same logic solver, while maintaining performance and functional independence, especially when adapting distribution control and safety strategies it often reduces the number of logic solvers required. (Note that in order to meet the requirements of IEC 61511 it is important that the system can provide the necessary separation to ensure that control cannot affect the safety instrumented functions).



Automation and safety within tank farms must be capable of being easily distributed.



The Siemens Offering

For more than 25 years now, Siemens has been a reliable industrial partner providing first-class automation and safety products and solutions in a wide range of sectors offering significant benefits to end users and also to system integrators. Siemens also offers lifecycle services for all phases of the safety instrumented system lifecycle.

Siemens has a flexible, cost effective, dependable solution for Tank Overfill Prevention. Siemens process instruments can be used to measure the level in the tank. However, the SIMATIC SIS logic solver is also compatible with a wide range of sensors from other manufacturers.

- By combining the SIMATIC failsafe range of safety PLCs, with suitable sensors and valves, it can be used for SIFs with SIL requirements up to SIL 3.
- The SIMATIC ET 200M I/O stations can be widely distributed and offer a wide range of I/O types – both standard and failsafe.
- The SIMATIC ET 200iSP I/O stations can be installed directly in Ex Zone 1. Three fail-safe modules are available for digital input, digital output and analogue input up to SIL 3 for use up to Zone 1 or 21. This means an Ex barrier is not required which reduces costs and simplifies the SIL calculation.
- Safety lifecycle tools help make the configuration of the system straightforward and help to reduce the possibility of systematic errors in the design of the application logic and the operator interface.

Siemens Safety Concepts

Flexible Modular Redundancy

With Flexible Modular Redundancy (FMR), Siemens offers an innovative concept for implementing cost-effective, scalable, safety solutions. Optimal hardware fault-tolerance levels can be implemented to meet the exact requirements for the application in terms of both safety and availability.

Advanced HMI

The SIMATIC PCS 7 HMI is user-friendly and helps ensure safe and secure operation of the Tank Overfill Prevention system. Operators can monitor all aspects of the performance and have complete control through operator views, including the SIMATIC Safety Matrix Viewer, to supervise and intervene as necessary. Comprehensive alarm handling helps the operator manage abnormal situations and the in-built diagnostic capability helps ensure maximum availability.

Integrated Control and Safety

The innovative Siemens safety concept allows the user to choose the appropriate level of integration between the Tank Overfill Prevention system and the Basic Process Control System (BPCS). If physical separation of the BPCS and the Tank Overfill Prevention system is not dictated by the application standard being used, then a common architecture, where the functionality of both BPCS and Tank Overfill Prevention system can co-exist in the same controller, may be beneficial. This can bring a reduction in space requirements, scope of hardware and wiring, and assembly, installation and engineering overheads and can therefore result in significant cost savings over the entire lifecycle of the plant. This common architecture still achieves the necessary logical separation to meet the requirements of independence as dictated by functional safety standards like the IEC 61511.

Safety Integrated Fieldbus Technology

The PROFIsafe application profile allows secure safety-related communication between the automation system and the process I/O via both PROFIBUS and PROFINET. PROFIsafe complies with functional safety standards and requirements up to SIL 3. Where appropriate, these can be used in the hazardous area and can be distributed across the whole tank farm. Options exist for star, line or ring network configurations. Physical media can be either copper or fibre.

Application engineering

Siemens provides the option of tried and tested TÜV certified F-block library blocks in S7 F systems which allow the application to be configured using standard blocks. An attractive alternative is to use a cause and effects based approach with the SIMATIC Safety Matrix. This is a TÜV-certified Safety Lifecycle Management tool for safety applications up to SIL 3 in accordance with IEC 61508. SIMATIC Safety Matrix can be used in all phases of the safety lifecycle for documenting, programming and monitoring of the system. The SIMATIC Safety Matrix safety lifecycle tool is ideally suited to processes in which defined states demand specific safety responses. SIMATIC Safety Matrix makes configuring safety logic easier, more convenient and faster.



Security

Since Tank Overfill Prevention systems are often found on high hazard sites so it is particularly important that such systems are adequately protected against security threats.

Siemens has developed an extremely effective holistic security concept to help protect plants using the SIMATIC PCS 7 process control system, which links a wide range of security measures that are continuously monitored and upgraded. This defense-in-depth concept operates on three levels:

- Plant security prevents unauthorized persons from gaining physical access to critical components
- Network security protects production against unauthorized access from office environments and the Internet
- System integrity prevents unauthorized modifications to process automation

Individual components such as the S7-400 CPUs are hardened against cyber threats. The Siemens SIMATIC PCS 7 process control system is certified by TÜV SÜD as conforming to the security standards IEC 62443-3-3 and also to IEC 62443-4-1 for the general development process for automation and drive technology products.

Solution Delivery

Where appropriate, Siemens can provide a fully engineered solution using in-house expertise and resources. However, it is also possible to use Solution Partners to meet the growing demand in the area of safety engineering. Our PCS 7 Safety Specialist Solution Partners offer professional services for all relevant safety aspects including:

- Know-how concerning the safety lifecycle of IEC 61511
- Knowledge of safety engineering with S7 F Systems and SIMATIC Safety Matrix
- Comprehensive experience in projects with safety applications in the process industry

Safety Lifecycle Services

With Safety Lifecycle Services, Siemens provides the necessary expertise for safety verification and validation providing tools and methods that exclude systematic errors in all project phases. This is all the more important since errors in an early project phase are often costly and time-consuming to correct at a later date.

The following service modules are available:

- Process Hazard Analysis and safety assessment
- Management, evaluation of “functional safety” and audits
- Configuration and planning of the SLC (Safety Plan)
- Assignment of the safety functions to the protection levels
- Safety Requirement Specification (SRS)
- Verification and validation (e.g. SIL verification, hardware/software audit)
- Modification
- Security in all phases of the lifecycle
- Training

Benefits

Increased Safety and System Availability

- Safety certified equipment for high availability and safety
- Higher system availability achieved without the need for external diagnostic devices
- Easier troubleshooting
- Integrated safety life-cycle tools available
- Flexible redundancy schemes to meet your safety and availability targets

Improved Operations and Maintenance

- Advanced local HMI options
- Greater operational flexibility
- Extensive system diagnostics provide efficient maintenance
- Embedded alarm management
- Reduced maintenance costs
- Integrated historian

Reduced Risk and Complexity

- Scalable to fit all of your fired processes
- Easier compliance with standards and codes
- Integrated security features

Subject to change without prior notice
PDPA-B10323-00-7600
FL 0917 1. INP 2 EN
Printed in Germany
© 11.2017, Siemens AG

The information provided in this flyer contains descriptions or characteristics of performance which in case of actual use do

not always apply as described or which may change as a result of further development of the products. An obligation to provide the respective characteristics shall only exist if expressly agreed in the terms of contract. Availability and technical specifications are subject to change without prior notice. All product designations may be trademarks or product names of Siemens AG or supplier companies whose use by third parties for their own purposes could violate the rights of the owners.

Security information

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions only form one element of such a concept. For more information about industrial security, please visit <http://siemens.com/industrialsecurity>.