

Integrated Safety Systems for Tankfarms

with SIMATIC Safety Integrated



Koen Druyts Account Manager

Siemens n.v./s.a. Industry Solutions IS ST

Nateus Business Park Nieuwe weg,1 B - 2070 Zwijndrecht Belgium

Tel.: +32 2 536 98 95 Mobile: +32 495 59 92 90 Fax: +32 2 536 72 05 mailto: koen.druyts@siemens.com

http://www.siemens.com/tankterminals

Objective of safety engineering

To avoid accidents and damage when a fault occurs and to ensure maximum safety for



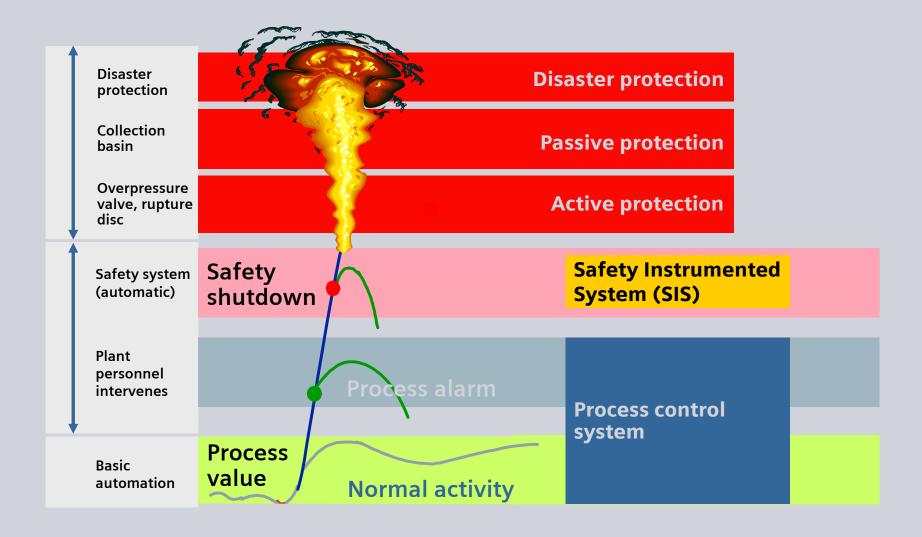
Negligence blamed for Buncefield explosion

A 2006 report by an independent investigation board did not apportion blame, but found <u>that human error and faulty safety equipment</u> were responsible.

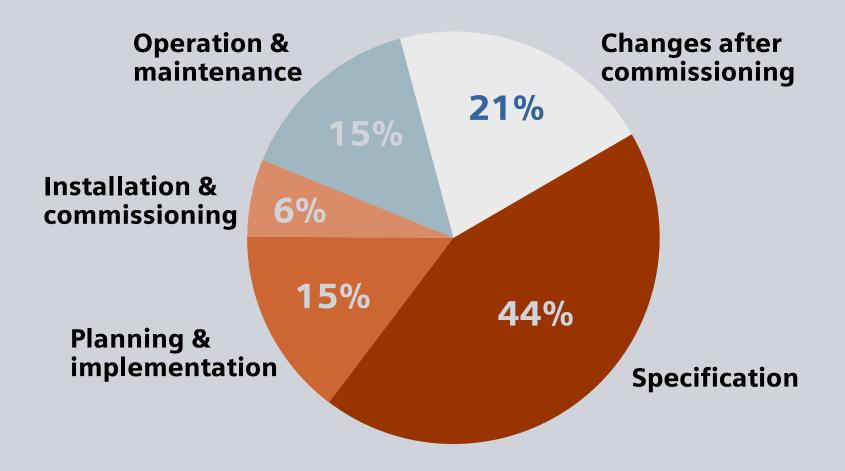
Total UK admitted that 300 tonnes of fuel was spilled after a gauge failed to register that a storage tank was full. But the company argues that it was not liable for damages because it could not reasonably have predicted the spillage would have such devastating consequences.



Safety concept for a plant



Cause of faults in automation systems



Date: 26 September 2008 - TIEMS Workshop Luxemburg - Koen Druyts - Slide 6 -

Risk analysis \rightarrow risk minimization



"Zero risk" is not feasible

Risk Analysis -> HAZOP

Hazard and Operability Analysis (HAZOP)

The Hazard and Operability (HAZOP) study is a widely used formal technique for examining potential safety and operational problems associated with a system.

A HAZOP study is usually carried out by a team, headed by a chairman and a secretary, who have experience both in the use of the HAZOP technique and the system under investigation.

International safety standards





Commission Electrotechnique Internationale International Electrotechnical Commission Международная Электротехническая Комиссия



IEC 61508 serves as the basic standard and basis for safety standardization.

It covers all areas where electrical, electronic or PLC systems are used to realize safety-related protection functions.



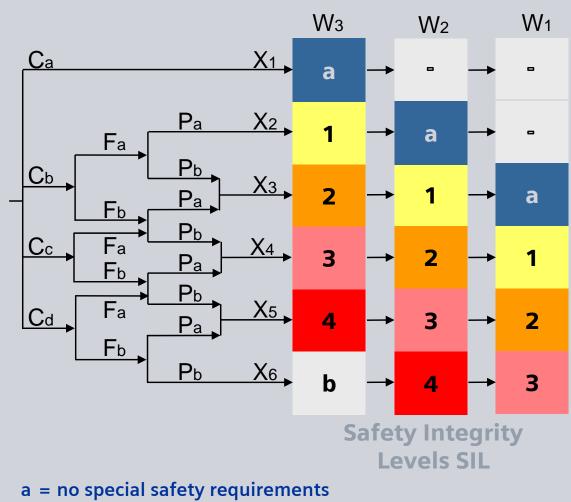
Commission Electrotechnique Internationale International Electrotechnical Commission Международная Электротехначеская Компосия



There are sector-specific standards based on IEC 61508, such as IEC 51511 for the process industry or IEC 61513 for the nuclear industry These sector standards are important for planners and operators of corresponding plants.

Evaluation of risk to define the SIL risk chart Safety Integrity Level

SIEMENS



b = individual safety system insufficient

Effect

- Ca Minor injury
- **Cb** Major, irreversible injury or death of one person
- Cc Death of several persons
- Cd Death of very many persons

Frequency and duration

- Fa Seldom to often
- Fb Frequent to constant

Danger prevention

- Pa Possible under cert. circum.
- Pb Nearly impossible

Probability of occurrence

- W1 Very low
- W2 Low
- W3 Relatively high

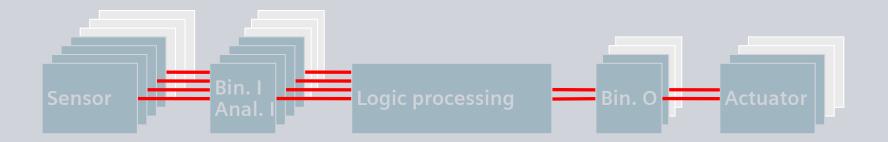
Target Safety Integrity Levels

Safety Integrity Level	Probability of failure on demand (PFD) per year (Demand mode of operation)	Risk Reduction Factor = 1/PFD
SIL 4	>=10 ⁻⁵ to <10 ⁻⁴	100000 to 10000
SIL 3	>=10 ⁻⁴ to <10 ⁻³	10000 to 1000
SIL 2	>=10 ⁻³ to <10 ⁻²	1000 to 100
SIL 1	>=10 ⁻² to <10 ⁻¹	100 to 10

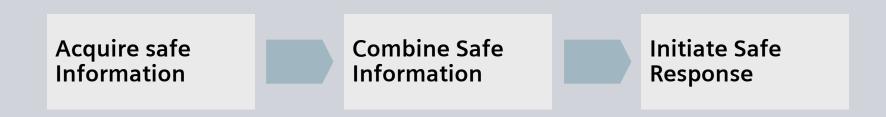
SIL: A performance criteria of a SIS, among other things, describes the probability of failure on demand.

Safety Functions IEC 61508

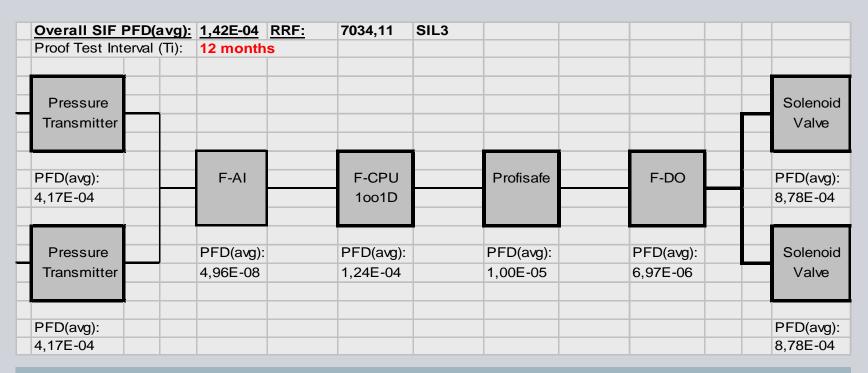
Considering the complete safety functionality of loops acc. to IEC 61508:



Each safety function always comprises the entire chain, from the collection and processing of information to the intended action



Simplified SIL Calculation SIL of a Safety Instrumented Function (SIF)



Overall SIF PFDavg = (PFDPT * PFDPT) + PFDAI + PFDCPU + PFDCom + PFDDO + (PFDValve * PFDValve)

For Sensors and actors evaluation: Pressure transmitter: MTTF = 600 years Failure rate (λ) = 1 / MTTF (mean time to failure) For SIF IEC61508 specifies: $\lambda_d = (\lambda_{du}, \lambda_{dd}) = \lambda/2$ Dangerous failure rate λ_d = half of the total failure rate (λ)

 $PFDavg = I^{D}t/2$

RRF (Risk Reduction Factor) = 1/PFDavg

SIEMENS



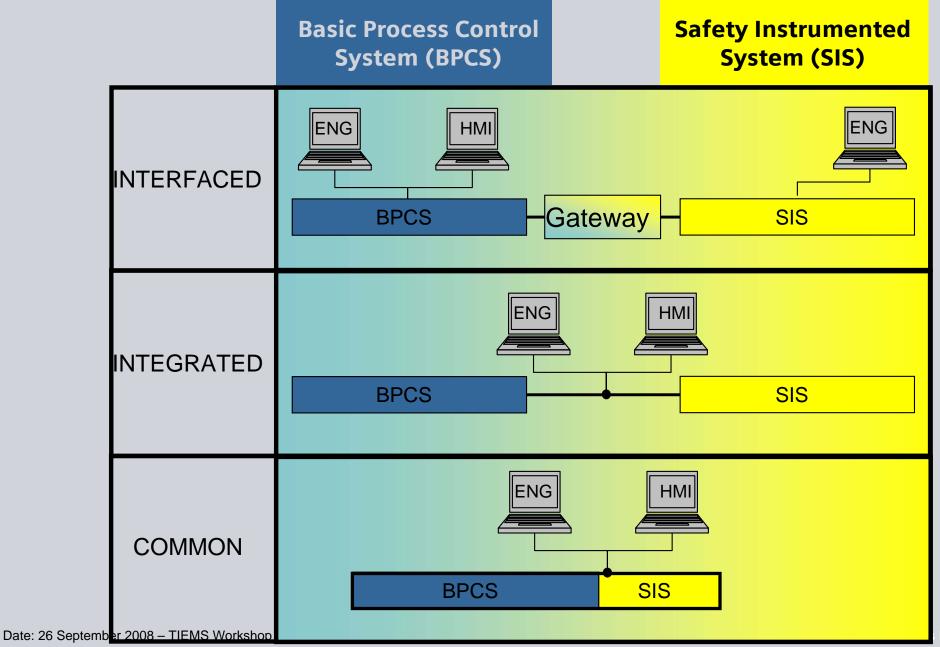
Integrated Control & Safety



Date: 26 September 2008 - TIEMS Workshop Luxemburg - Koen Druyts - Slide 14 -

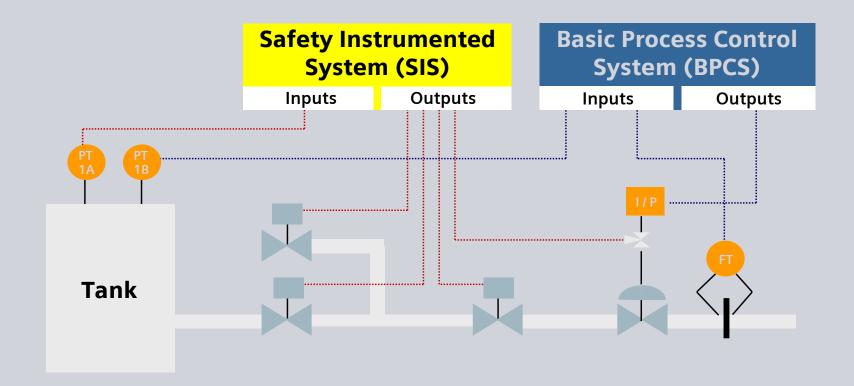
© Siemens AG 2008, All Rights Reserved

The "Right" Level of Integration

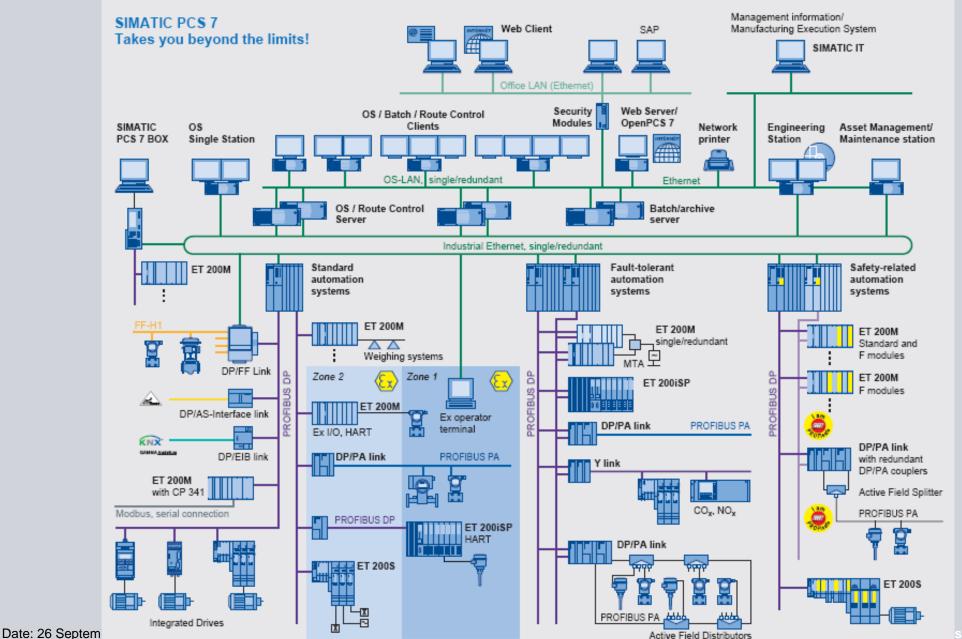


Safety Instrumented System (SIS)

SIS: A combination of sensors, logic units (e.g. controllers) and actuators which detect abnormal operating conditions and AUTOMATICALLY switch the plant to a safe state.

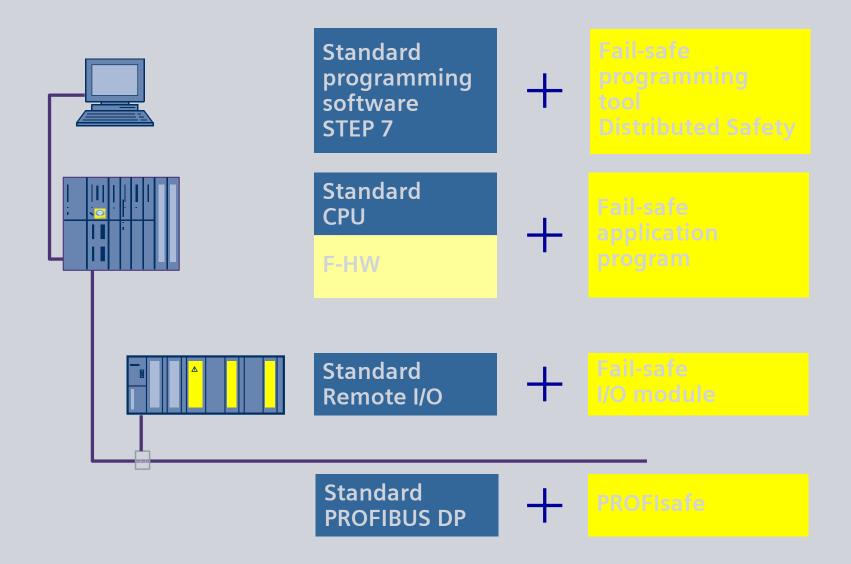


Overview totally integrated solution with PCS7



SIMATIC Safety Integrated The Concept

SIEMENS



Safety Integrated for Process Automation



Common controller platform for process control and process safety

One hardware for all

One engineering system for process control and process safety application

Reduces training and uses the available knowledge

User-friendly display of process safety information in PCS 7

Automatic integration of process safety diagnostics into the operator interface

Direct communication between DCS and SIS

Less engineering work

Date: 26 September 2008 - TIEMS Workshop Luxemburg - Koen Druyts - Slide 19 -



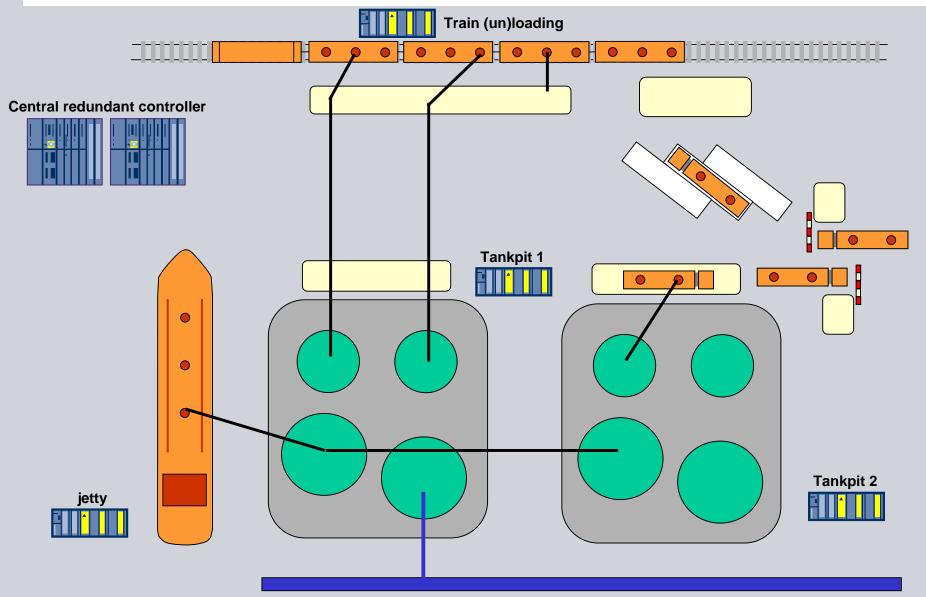
Flexible Modular Redundancy



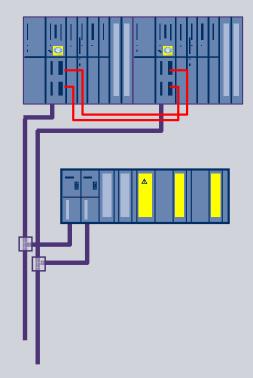
Date: 26 September 2008 - TIEMS Workshop Luxemburg - Koen Druyts - Slide 20 -

© Siemens AG 2008, All Rights Reserved

Typical Tank Farm Lay-out Simplified concept distributed I/O

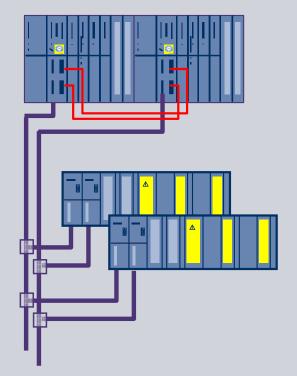


Flexible Modular Redundancy (FMR)



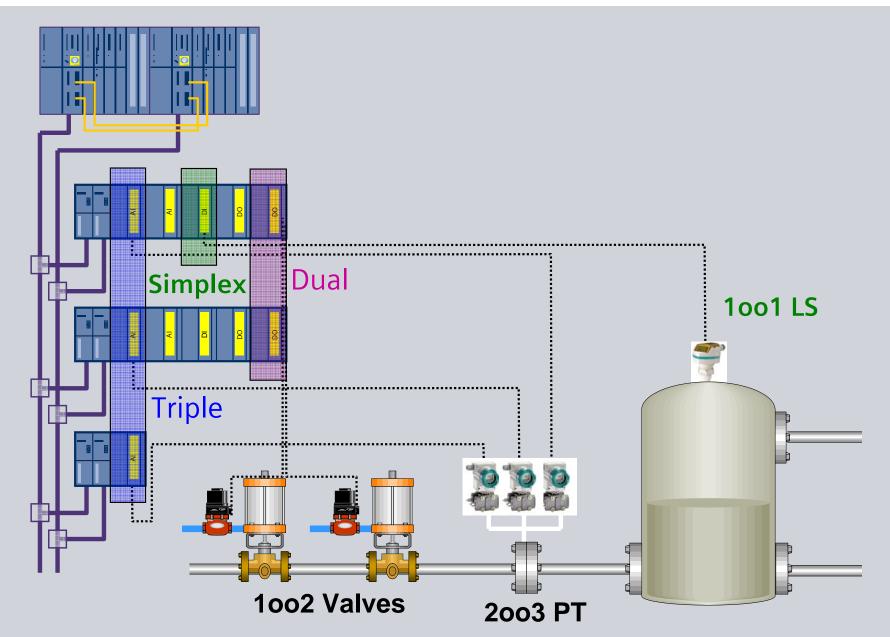
- Redundant S7-400FH
- Redundant PROFIBUS DP
- Switched I/O ET 200M

- Redundant S7-400FH
- Redundant PROFIBUS DP
- Redundant I/O ET 200M



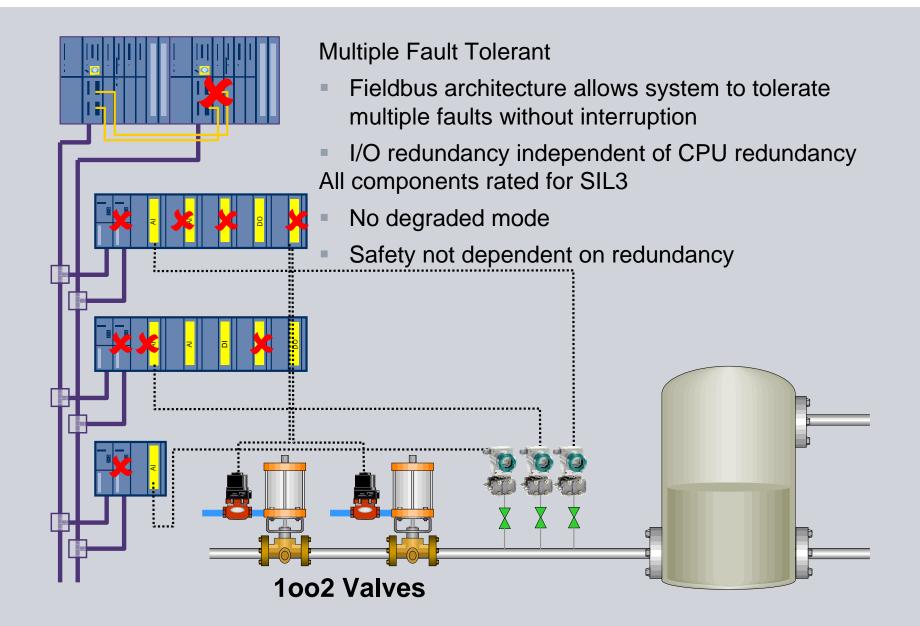
- Redundant S7-400FH
- Redundant PROFIBUS DP
- Redundant, switched I/O ET 200M

Flexible Modular Redundancy (FMR)



Date: 26 September 2008 - TIEMS Workshop Luxemburg - Koen Druyts - Slide 23 -

Flexible Modular Redundancy (FMR)



Flexible Modular Redundancy (FMR)

Safety Integrity Level up to SIL 3 with one controller

- Highest Safety Integrity Level
- **Highest Flexibility**
 - Separate or combine safety and standard application in one CPU
 - Use redundancy for safety only where it is needed
 - Parallel use of PROFIsafe on PROFIBUS

Highest Availability through Multiple Fault Tolerance

- Architecture allows system to tolerate multiple faults
- IO redundancy independent of CPU redundancy
- IO and device redundancy can be matched to maximize availability

Cost reducing

- Use redundancy only where you need it for safety or availability
- Parallel use of PROFIsafe on PROFIBUS

Date: 26 September 2008 - TIEMS Workshop Luxemburg - Koen Druyts - Slide 25 -



Safety Lifecycle Engineering



Date: 26 September 2008 - TIEMS Workshop Luxemburg - Koen Druyts - Slide 26 -

The IEC 61511(ISA S84) Safety Lifecycle

The different phases of the safety Lifecycle

- Analysis Phase
 - Identification of Hazards and Risks
 - Development of the Safety Requirement Specification for the Safety Instrumented System
 - Allocation of Safety Function to Protective Layers

Realization Phase

- Design and Engineering of Safety Instrumented System
- Design and Development of other Means of Risk Reduction
- Installation, Commissioning & Validation
- Operation Phase
 - Operation & Maintenance
 - Modification
 - Decommissioning







The Realization Phase with the Safety Matrix

Configuration of the Safety Functions with the Cause & Effects Method

Automatic TÜVcertified Creation of the Safety Logic from the Cause & Effect matrix

Easy Configuration without special Programming Knowledge

		Matrix - Tools W	_	no SM_ISA_N\Plant ESD]	-														∎× ∎×
				MATRIX	Effect Description	Feed pump	Feed block valve	Feed block valve	Hopper Feed block valve	Tank Drain block valve	ESD shutdown	Tank relief valve						_	
All Groups				Select	Output Tag	PM_100*	BV_100A*	BV_100B*	BV_200 #OUT_TO_AREA1 #OUT_TO_AREA2 #OUT_TO_AREA3	BV_300	#ESD	SV_100*							
					Action	Shutdown	Close	Close	\searrow	Open		OPEN							
Input Tag	Func	Limit/Trip	EngUnit	Cause Description	Num	1	2	3	4	5	6	7	8	9	10	11	12	13	14
PS_100		FALSE		Feed Pump High Pressure Switch	1	Ν													
LSH_100		TRUE		Tank_100 Level switch high	2	2S	S	S	R	2N									
LSL_200		TRUE		Hopper_200 Level switch Low	3		Ν	Ν	2S										
PSH_200		TRUE		Hopper_200 High Pressure	4		Ν	Ν	V										
PT_100		H 38.00	PSIG	Feed pressure	5	S	S	S											
LT_100		H 50.00	Feet	Tank Level	6	2S	N	Ν		2N									
PT_101 PT_102 PT_103	Vote	U 3.0	_	Tank Pressure	7				N	2N		s							
LT_200		H 50.00	Ft	Hopper Level	8				2S	Т	apk	Pre	Pee	ure	>	clos	201	Hor	per F
TS_101 TS_102 TS_103	AND	FALSE FALSE FALSE		Tank_100 High Temperature switch	9							35				010			
∢ Ready																			

The Operation Phase with Safety Matrix

Operation and Maintenance

- Online View
- Support Operation functions like Bypass, Reset and Override
- Sequence of Event Recording
- First Alarm Display

Safety Lifecycle Management Tool

- Integrated Version Tracking
- Integrated Documentation of Operator Manipulations
- Integrated Documentation of Changes

							_	SN	1 D	emo/@SM_	De	mo)/SN	_	en en
SIMA		SA			ATRIX	Effect Description	dun	valve		Hopper Feed block valve	Tank Drain block valve	ESD shutdown	ę	_	
Ack Cause	ACK Drivers			/iew iags	View Status	ffect	Feed pump	eed b	Feed block	oppel	ank D	SD	ank n		
Clear FirstOut	Bypass	Vie Eve		lear vents	Select	Values E	RUE F		TRUE F		TRUE T				
All Groups						Output Tag	PM_100* T			AREA1 AREA2 AREA2	BV_300 T)0*		
Ioput Tag	Values	Func	Limit(Trin	Engl Init	Cause Description	an Action	Shutdown				n Open		2 OPEN	8	c
Input Tag	Values	Func	Limit/Trip	EngUnit	Cause Description	nu Action	Z - Shutdowr	2 Close		close notify notify hotify	open 2	6	2 OPEN	8	ç
PS_100	FALSE	Func	FALSE	EngUnit	Feed Pump High Pressure Switch	Num 1	1 N	2	3	4	5	6		8	E.
PS_100 LSH_100	FALSE FALSE	Func	FALSE TRUE	EngUnit	Feed Pump High Pressure Switch Tank_100 Level switch high	Num 1 2	1	2 S	3 S	4 R	•••••••	6		8	<u>e</u>
PS_100 LSH_100 LSL_200	FALSE FALSE FALSE	Func	FALSE TRUE TRUE		Feed Pump High Pressure Switch Tank_100 Level switch high Hopper_200 Level switch Low	Num 1 2 3	1 N	2 S N	3 S N	4 R 2S	5	6		8	с
PS_100 LSH_100 LSL_200 PSH_200	FALSE FALSE FALSE FALSE	Func	FALSE TRUE TRUE TRUE		Feed Pump High Pressure Switch Tank_100 Level switch high Hopper_200 Level switch Low Hopper_200 High Pressure	Num 1 2 3 4	1 N 2S	2 S N N	3 S N N	4 R	5	6		8	c
PS_100 LSH_100 LSL_200 PSH_200 PT_100	FALSE FALSE FALSE FALSE 0.0	Func	FALSE TRUE TRUE TRUE H 38.00	PSIG	Feed Pump High Pressure Switch Tank_100 Level switch high Hopper_200 Level switch Low Hopper_200 High Pressure Feed pressure	Num 1 2 3 4 5	1 2S S	2 S N S	3 S N N S	4 R 2S	5 2N	6		8	c
PS_100 LSH_100 LSL_200 PSH_200 PT_100 LT_100	FALSE FALSE FALSE FALSE 0.0 0.0	Func	FALSE TRUE TRUE TRUE H 38.00 H 50.00		Feed Pump High Pressure Switch Tank_100 Level switch high Hopper_200 Level switch Low Hopper_200 High Pressure	Num 1 2 3 4	1 2S S	2 S N N	3 S N N S	4 R 2S	5	6		8	ç
PS_100 LSH_100 LSL_200 PSH_200 PT_100	FALSE FALSE FALSE 0.0 0.0 0.0	Func Vote	FALSE TRUE TRUE TRUE H 38.00	PSIG	Feed Pump High Pressure Switch Tank_100 Level switch high Hopper_200 Level switch Low Hopper_200 High Pressure Feed pressure	Num 1 2 3 4 5	1 2S S	2 S N S	3 S N N S	4 R 2S	5 2N	6		8	e
PS_100 LSH_100 LSL_200 PSH_200 PT_100 LT_100 PT_101 PT_102	FALSE FALSE FALSE FALSE 0.0 0.0 0.0 0.0 0.0	Vote	FALSE TRUE TRUE TRUE H 38.00 H 50.00 H 26.00	PSIG Feet	Feed Pump High Pressure Switch Tank_100 Level switch high Hopper_200 Level switch Low Hopper_200 High Pressure Feed pressure Tank Level	Num 2 3 4 5 6	1 2S S	2 S N S	3 S N N S	4 R 2S V	5 2N 2N	6	7	8	C.



Summary



Date: 26 September 2008 - TIEMS Workshop Luxemburg - Koen Druyts - Slide 30 -

© Siemens AG 2008, All Rights Reserved

Process Safety and Totally Integrated Automation

Integrated Control & Safety

- Best Integration into the distributed control system PCS 7
- Less training and easy handling due using same tools
- Less hardware due using same CPU for standard and safety

Flexible Modular Redundancy

- Save money by mix and match to meet the goals of the application
- Highest availability due the multiple fault tolerance

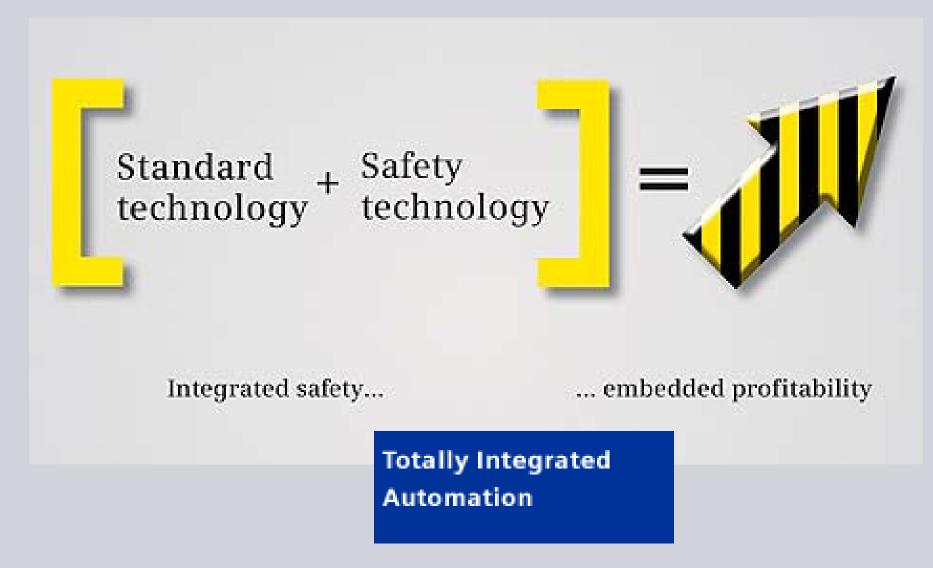
Integrated Safety Fieldbus

- Less wiring due PROFIsafe on PROFIBUS, one cable for the communication safe and non-safe
- Prepared for safety fieldbus instruments

Safety Lifecycle Engineering

Safety Matrix supports the phases of the Safety Lifecyle

Process Safety and Totally Integrated Automation



Date: 26 September 2008 - TIEMS Workshop Luxemburg - Koen Druyts - Slide 32 -

© Siemens AG 2008, All Rights Reserved