Setting the Standard for Automation™

Safety Transmitter / Logic Solver Hybrids

Standards
Certification
Education & Training
Publishing
Conferences & Exhibits

Traditional Pressure Sensor Portfolio

Process Transmitter

Trip Alarm or Trip Module

Process Switch

Safety Transmitter-Switch

Process Pressure Transmitter

- Widely accepted for BPCS and safety control, alarm and interlock (SCAI)
  - Supplies an analog 4 to 20 mA output
  - Comes with or without local indication
- Interface/Integration
  - Coupled with a central or distributed logic solver
  - Attention must be paid to set-up and proof testing
- SIL capable
  - Up to SIL 2 (SC3)
  - Prior use and certified versions used in SIS
  - Newer versions address legacy issue of frozen impulse

Process Switch

- Widely used in plants for safety control, alarm and interlock (SCAI)
  - Supplies SPDT Form C output
  - No indication

- Interface/Integration
  - Supplies discrete input to logic solver or coupled directly final elements
  - Attention must be paid to set up and proof testing
- SIL capable
  - Prior use and certified versions are available
  - SIL achievement is sometimes a stretch
  - No diagnostic coverage

Trip Alarm or Trip Module

- Widely used in plants for safety control, alarm and interlock (SCAI)
  - Supplies an analog or digital outputs
  - With or without local indication

- Interface/Integration
  - Needs additional environmental or hazardous area protection
  - Attention must be paid to set-up and proof testing
- SIL capable
  - Process relays and fault relays must be wired in series
  - (i.e. you must monitor the diagnostic output)

Hybrid Transmitter-Switch

- Emerging “niche” technology for safety control, alarm and interlock (SCAI)
  - Combines functions of transmitter and trip alarm
  - Comes with local indication
- Interface/Integration
  - Coupled with logic solver or powered externally
  - Programmable logic for set-up

- SIL capable
  - SIL 2 (SC3)
  - Prior use and certified versions used in SIS
  - Automatic self-diagnostics

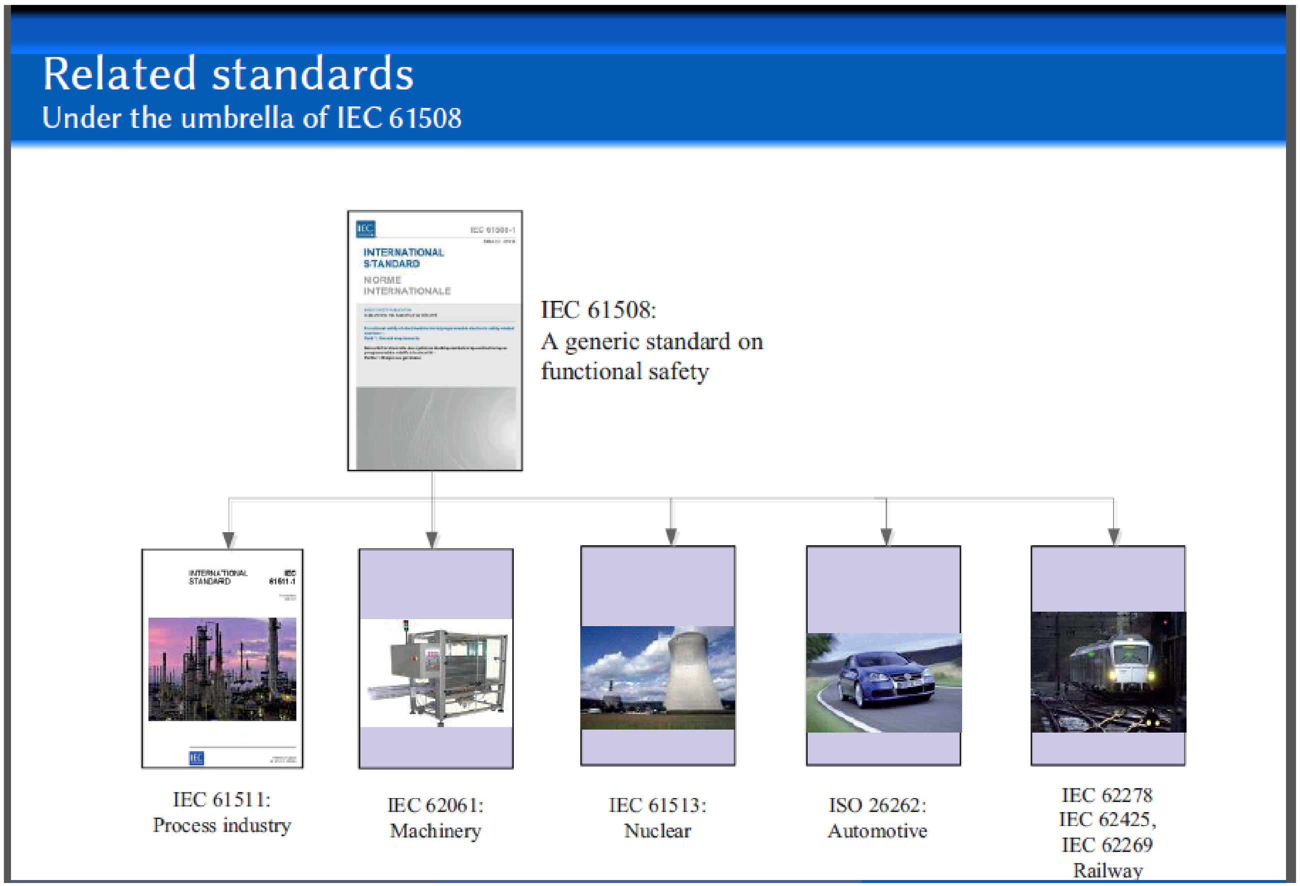
Value Proposition of Hybrids

- Cost effective
  - ✓ 3 in 1 in one footprint
  - ✓ Lower unit price point & lower total cost
- Reduces complexity
  - ✓ Simplified integration
  - ✓ Standalone hardware & software
- SIL capable
  - ✓ Certified for use in SIL 2 (SC3)
  - ✓ Robust diagnostics

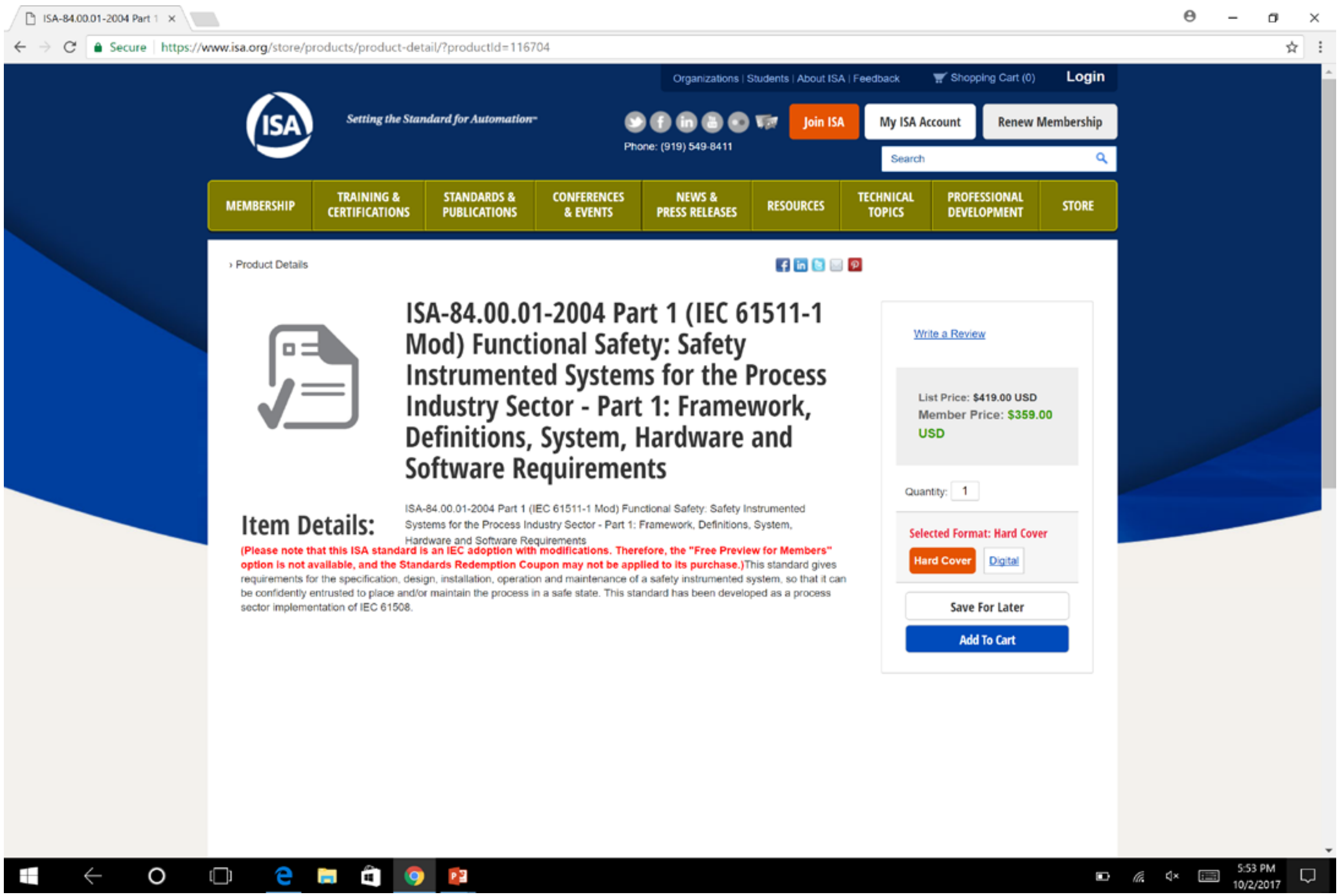
Functional Safety Standards increasingly inform selections

- What are the functional safety standards against which these sensor devices are measured?
  - Qualitative and quantitative assessment

IEC Standards for the Process and Other Industries



ISA 84.00.01-2004



IEC 61508

- “Functional safety is a concept applicable across all industry sectors. It is fundamental to the enabling of complex technology used for safety-related systems. It provides the assurance that the safety-related systems will offer the necessary risk reduction required to achieve safety for the equipment.”

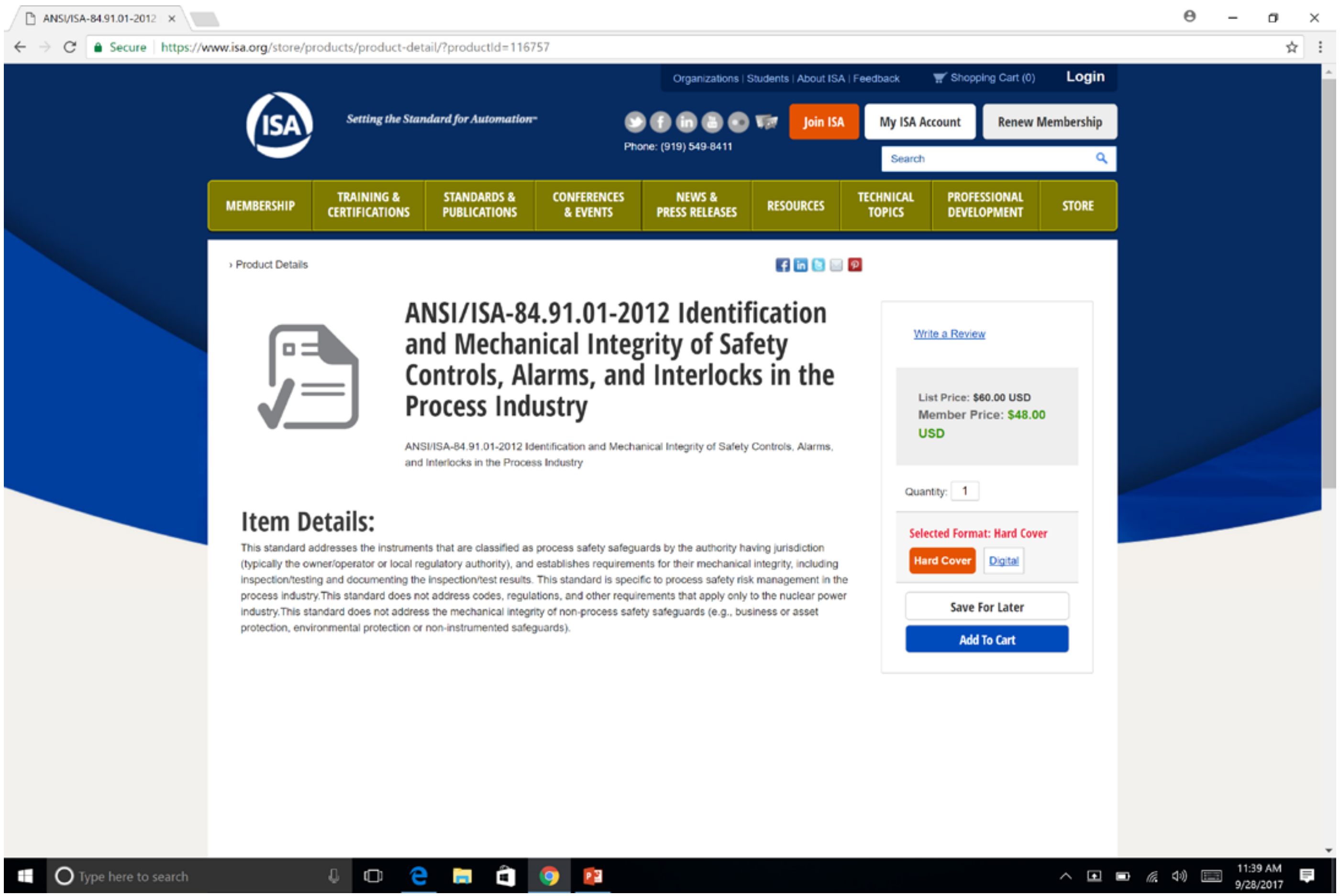
IEC

IEC 61508

- Functional safety relies on **active systems**. The following are two examples of functional safety:
  - The detection of smoke by sensors and the ensuing intelligent activation of a fire suppression system; or,
  - The activation of a level switch in a tank containing a flammable liquid, when a potentially dangerous level has been reached, which causes a valve to be closed to prevent further liquid entering the tank and thereby preventing the liquid in the tank from overflowing.

IEC

ANSI/ISA 84.91.01-2012



ANSI/ISA 84.91.01 (2012)

Introduction

This standard establishes a procedure to identify the process safety functions that utilize instrumentation to maintain safe operation in the process industry. In this standard, these functions are implemented by safety controls, alarms, and interlocks.

Mechanical integrity and maintenance are important elements in process safety risk management. In this standard, provisions for mechanical integrity and maintenance apply to safety controls, alarms, and interlocks.

Basic Concepts of ANSI/ISA 84.91.01 (2012)

- Identify process safety functions that utilize instrumentation in order to maintain safe operation.
- Identification of safety control, alarms and interlocks (SCAI)
- Focused on mechanical integrity and maintenance being the key to managing process risk.

Instrumented Safeguards

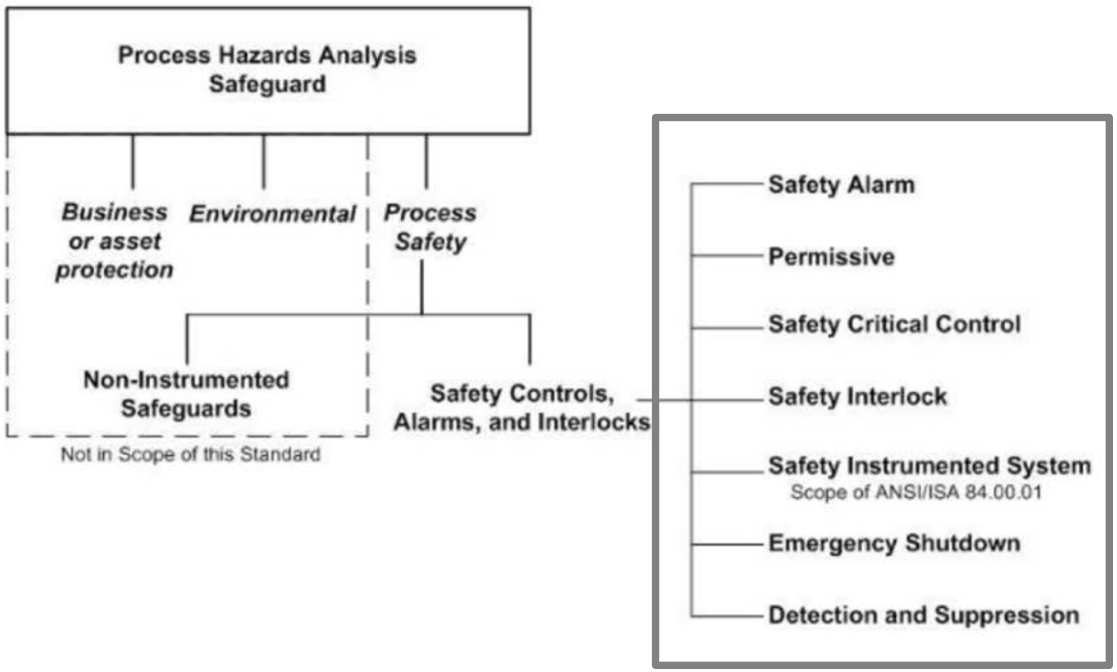


Figure 1 – Safety controls, alarms, and interlocks relationship to the process hazards analysis (PHA)

4 Procedure

Recommended Reading

sis-tech.com/wp-content/uploads/2013/09/PSP-published-SCAI.pdf

Safety controls, alarms, and interlocks as IPLs

Angela E. Summers, Ph.D., P.E.

SIS-TECH Solutions

12621 Featherwood Dr. Suite 120,

Houston, TX 77034

Keywords: safety controls, alarms, interlocks, SIS, BPCS, process control, layers of protection analysis

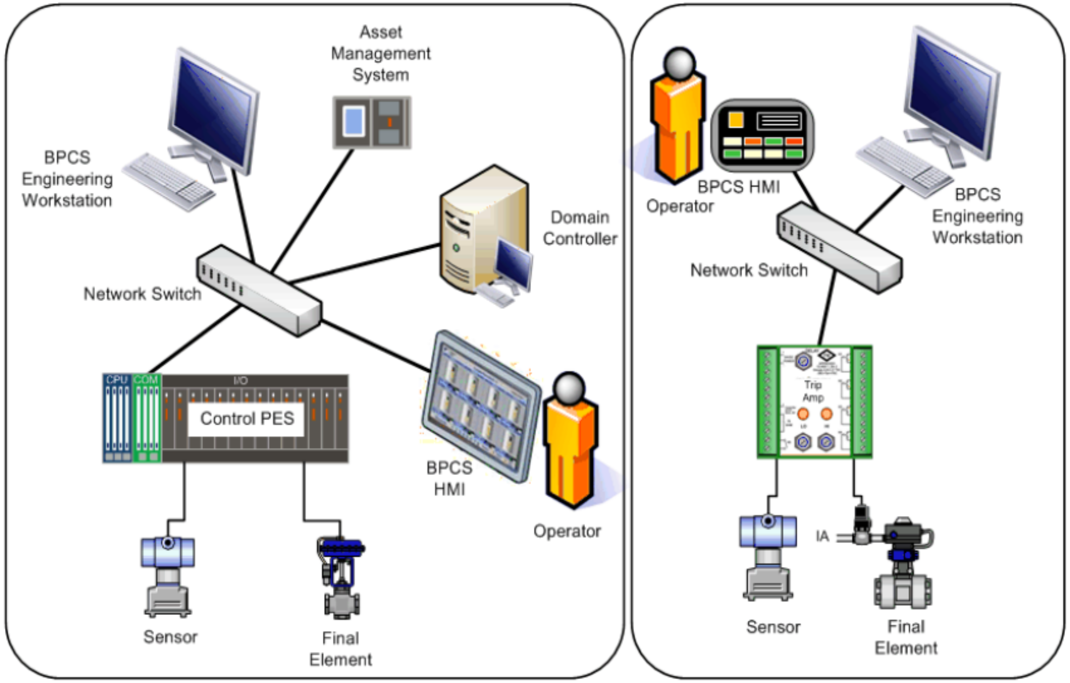
Abstract

Layers of Protection Analysis (LOPA) evaluates the sequence of events that first initiate and then propagate to a hazardous event. This semi-quantitative risk assessment technique can expose the role that automation plays in causing initiating events and in responding to the resulting abnormal operation. Automation that is specifically designed to achieve or maintain a safe state of a process in response to a hazardous event is now referred to as safety controls, alarms, and interlocks (SCAI).

Guidelines for Initiating Events and Independent Protection Layers addresses four basic types of SCAI: safety controls, safety alarms, safety interlocks, and safety instrumented systems (SIS).

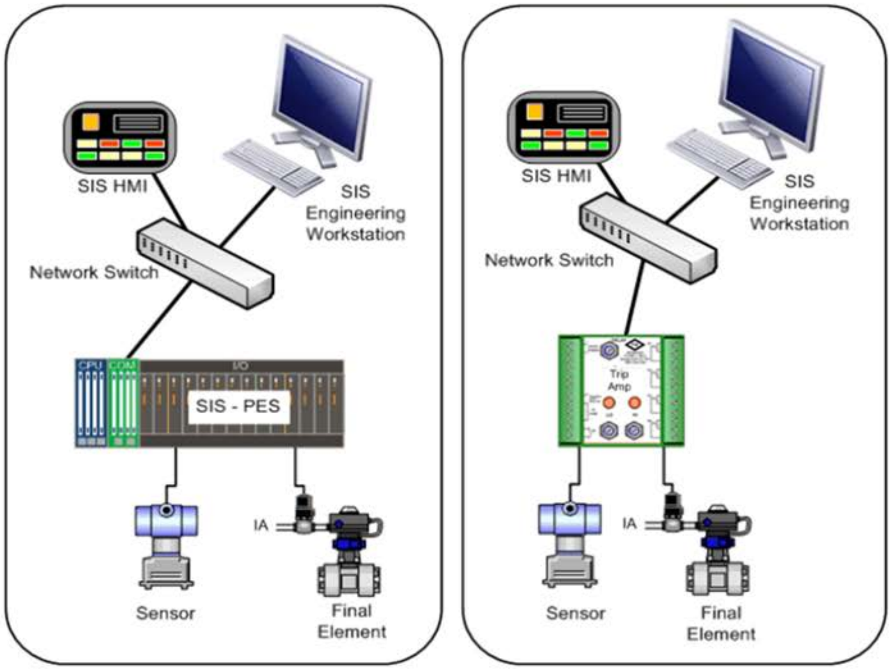
How SCAI is Implemented

Figure 3 ***Examples of BPCS using PES and Trip Amplifier Technology***



Recommended Reading

Figure 4 ***Examples of SIS using PES and Trip Amplifier Technology***



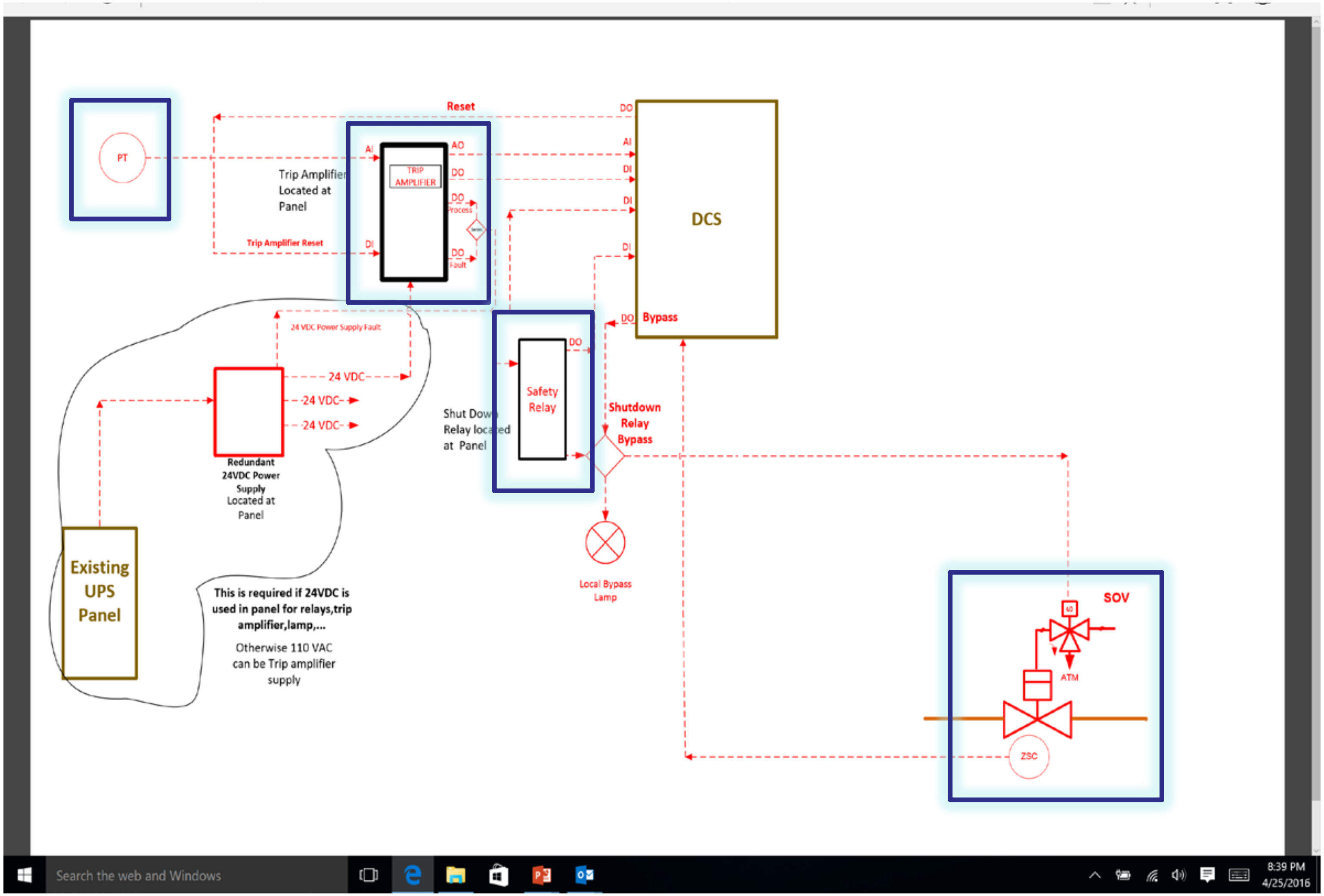
Angela says…

- ”When considering the use of BPCS for SCAI, the first thing to remember is that risk reduction is not free. Getting an order of magnitude risk reduction from the BPCS is hard. The independence and reliability requirements impose rigorous design and management practices, focusing on eliminating single points of failure and human error.”

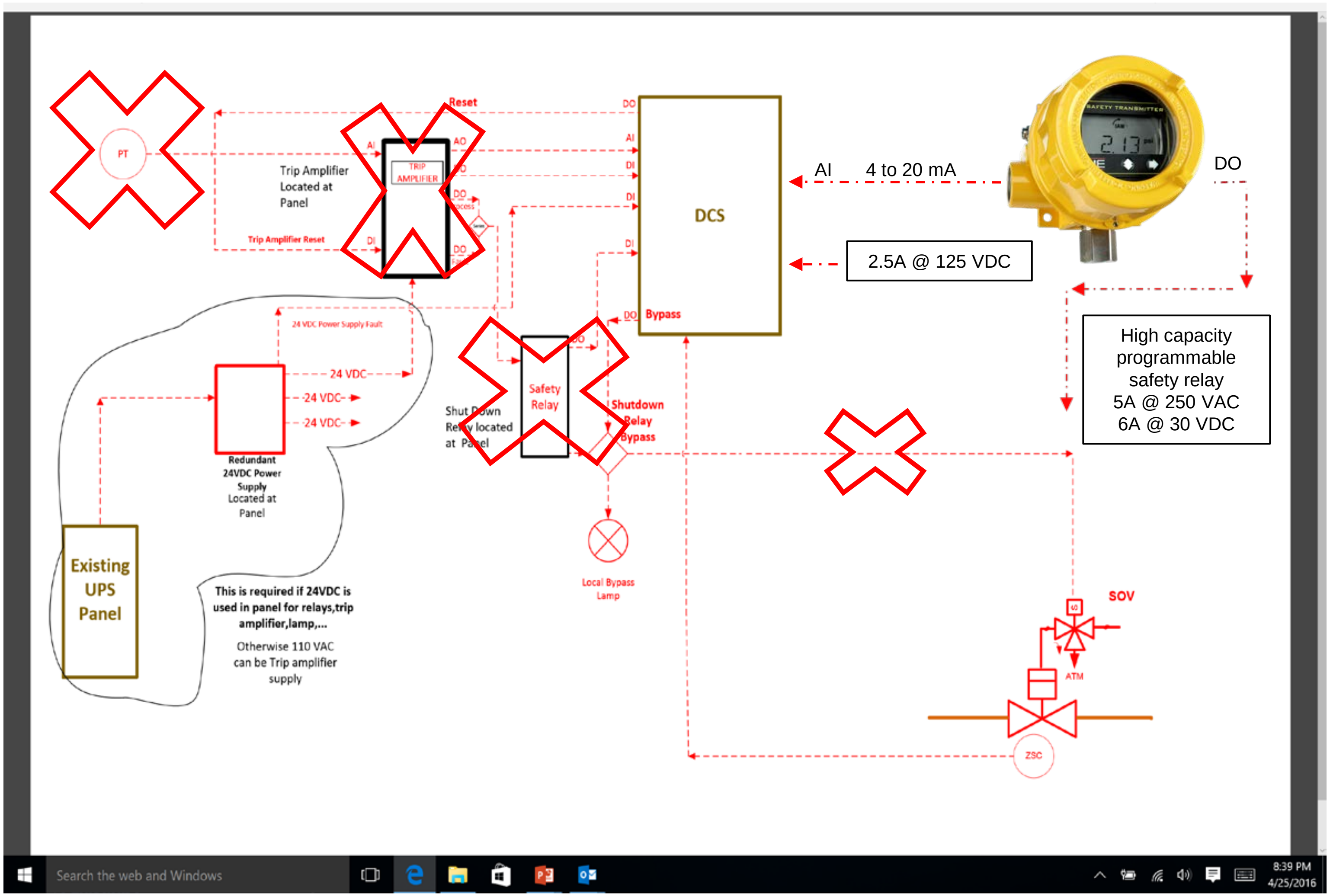
Angela says…

- ”When claiming more than one order of magnitude (risk reduction) from a single controller in a scenario, the controller must be designed and managed as a SIS in accordance with IEC 61511.”

Distributed SIS: Traditional Recipe



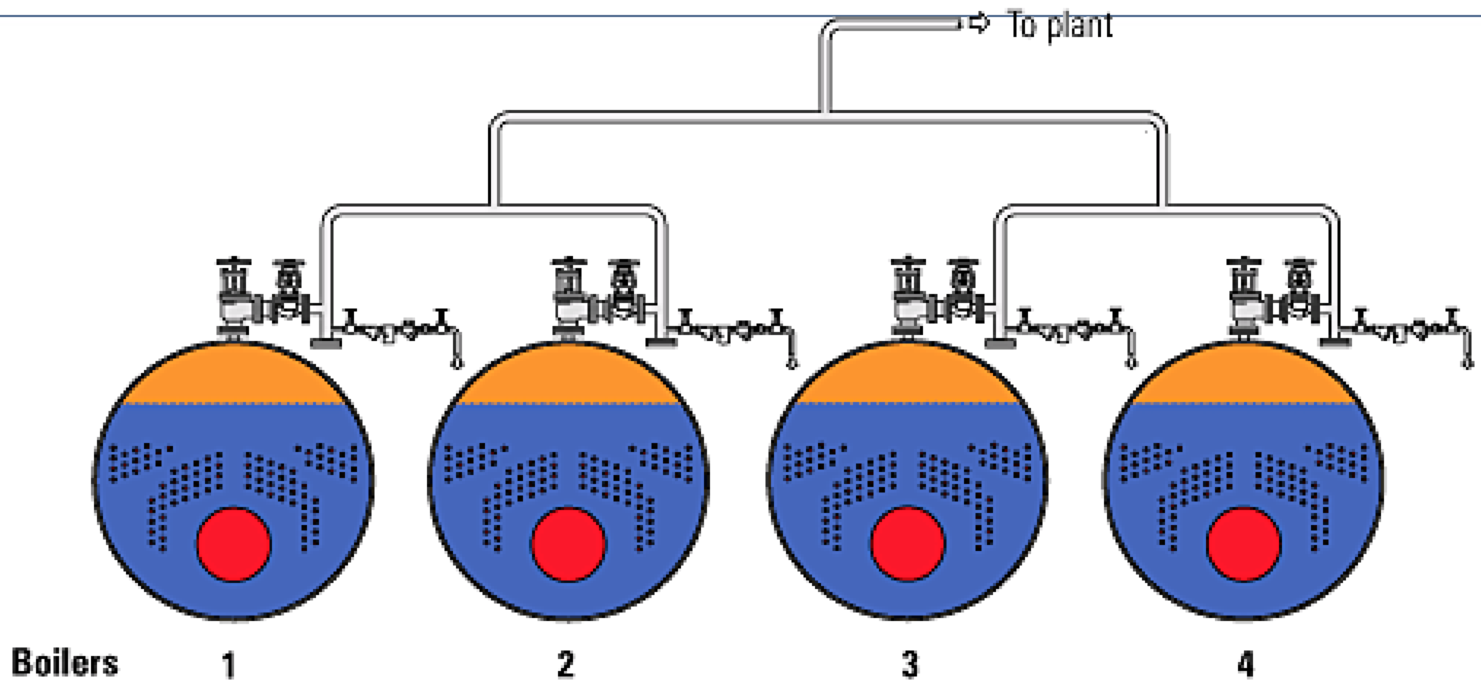
Distributed SIS: applying the "hybrid" in SIS



Functional Safety context

- Target SIL
- PFD avg
- Risk Reduction (RRF)

Theoretical Safety Instrumented Function (SIF)



The “High Pressure Protection” SIF measures steam pressure in the boiler output header and opens a vent valve if the pressure exceeds the setpoint.

Sensors

- Sensors are either certified process transmitters or a certified “hybrid of a transmitter & switch
- Clean service
- MTTR=24 hours
- Proof Test Interval = 12 months
- Proof Test Coverage = 100%
- Process outputs are assumed to fail to safe states.

Logic Solver

- Generic SIL 2 or SIL 3 Logic Solver
- MTTR = 24 hours
- Proof Test Interval = 60 months
- PT Coverage = 100%.

Final Element

- Generic, 3-way solenoid
- Bettis G-Series pneumatic spring return actuator
- Fisher Controls Design EZ valve
- MTTR = 24 hours
- Proof Test Interval = 12 months
- PT Coverage = 85%
- No ß factor

Simplified Equation

- PFDavg (SIF) = PFDavg (Sensor Subsystem) + PFDavg (Logic Solver) + PFDavg (Final Element subsystem)

RRF & Achieved SIL (SIL 2 LS)

Table 2 - HIGH PRESSURE PROTECTION SIF, 1oo1D, SIL 2 Logic Solver, Sensor PTI = 12 months

			SAFETY VARIABLE OUTPUTS			LOGIC SOLVER + FE				
Sensor Description	SIF Input	SILac	4 to 20 mA Current	Safety Relay	Photo-MOS w/ IAW®	Logic Solver	Final Element	PFDavg	Risk Reduction Factor	Achieved SIL
Certified Pressure Transmitter										
Honeywell SmartLine ST 800 Hart	4 to 20 mA	2	1.84E-04	N/A	N/A	6.03E-03	4.62E-03	**1.08E-02**	92	1
Honeywell SmartLine ST 700 Basic Hart	4 to 20 mA	2	4.34E-04	N/A	N/A	6.03E-03	4.62E-03	**1.11E-02**	90	1
Honeywell SmartLine ST 700 Standard Hart	4 to 20 mA	2	1.84E-04	N/A	N/A	6.03E-03	4.62E-03	**1.08E-02**	92	1
Rosemount 3051 Device Label SW 1.0.0-1.4.x	4 to 20 mA	2	1.40E-04	N/A	N/A	6.03E-03	4.62E-03	**1.08E-02**	93	1
Rosemount 3051S SW V.7.0+	4 to 20 mA	2	1.75E-04	N/A	N/A	6.03E-03	4.62E-03	**1.08E-02**	92	1
Rosemount 3051S HDS DA2, SW 5.0+	4 to 20 mA	2	1.49E-04	N/A	N/A	6.03E-03	4.62E-03	**1.08E-02**	93	1
Rosemount 3051S HDS DA2, SW 5.0+ (w/ PATC)	4 to 20 mA	2	8.76E-05	N/A	N/A	6.03E-03	4.62E-03	**1.07E-02**	93	1
Yokogawa EJX (A & J Series)	4 to 20 mA	2	1.71E-04	N/A	N/A	6.03E-03	4.62E-03	**1.08E-02**	92	1
Yokogawa EJA (E & J Series)	4 to 20 mA	2	1.71E-04	N/A	N/A	6.03E-03	4.62E-03	**1.08E-02**	92	1
Certified Pressure Transmitter-Switch										
United Electric 2SLP (current output only)	4 to 20 mA	2	2.10E-04	N/A	N/A	6.03E-03	4.62E-03	**1.09E-02**	92	1
United Electric 2SLP (safety relay only)	Safety Relay (5A VAC or VDC)	2	2.10E-04	2.32E-04	N/A	0.00E+00	4.62E-03	**4.85E-03**	206	2
United Electric 2SLP (photo-MOSFET w/ IAW®)	Photo-MOS (30 VDC @ 20mA max)	2	2.10E-04	N/A	2.01E-04	4.24E-03	4.62E-03	**9.06E-03**	110	2

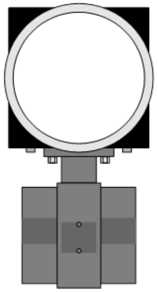
PD PUMP APPLICATION
LOW SIL 2 - TRADITIONAL APPROACH

• Safety PLC

Safety function to trip remote pump on excessive pressure

MCC

- Stainless steel cabinet
- Sub panel
- Associated wiring & programming
- Estimated cost >$20K



Process Transmitter SIL 2

Challenge

Process Safety Time

> 1 sec

PD PUMP APPLICATION
LOW SIL 2 - NEW APPROACH

MCC

High speed/high capacity

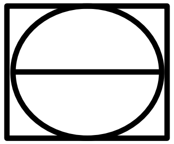
Safety Relay (60 ms)

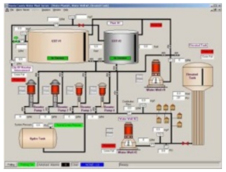
- Start/stop circuit
- No Safety PLC

4 to 20 mA (NAMUR 43 NE Std)

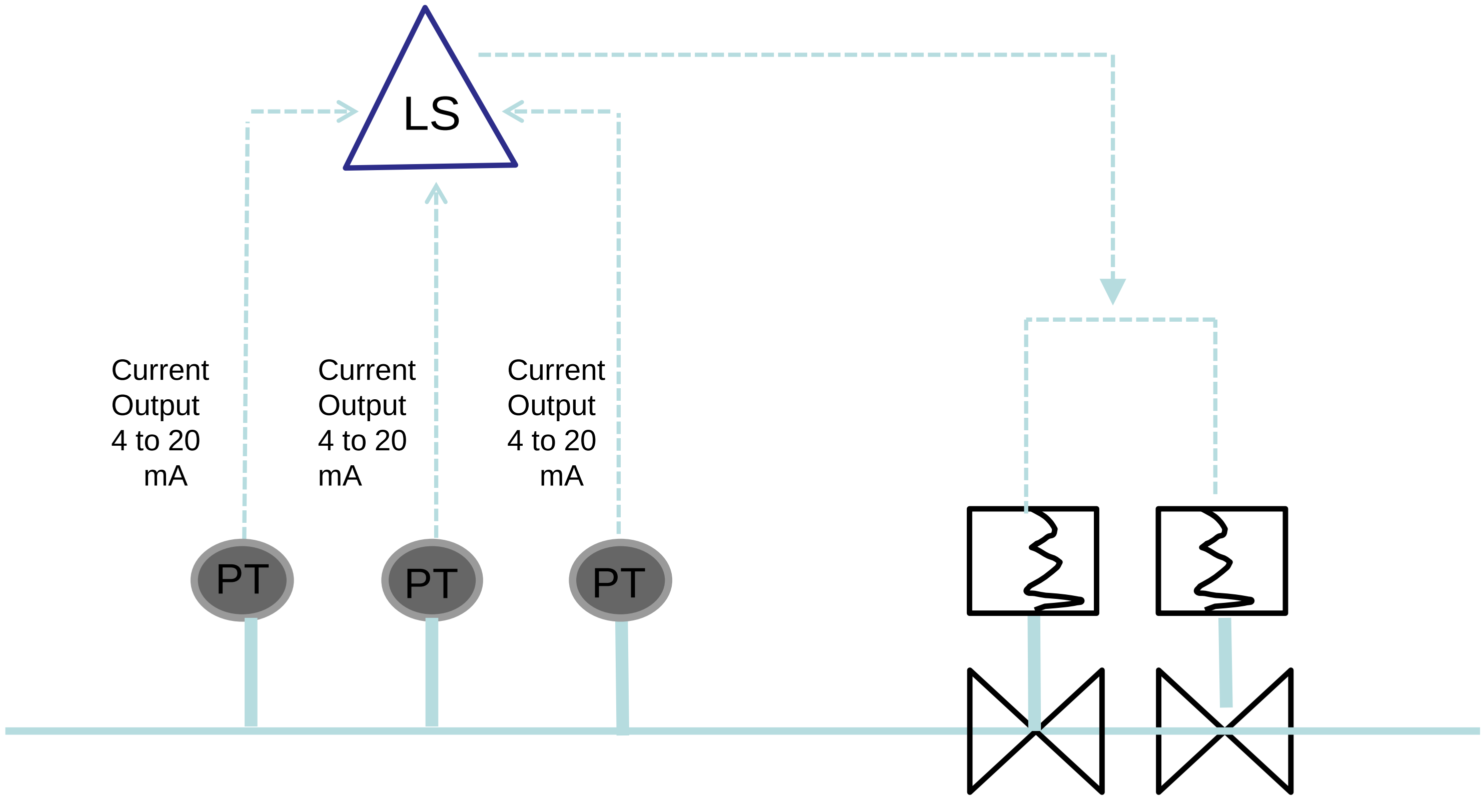
30 VDC @ 20 mA (max)

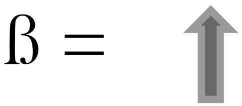
30 VDC @ 20 mA max – universal diagnostics





Hypothetical Illustration Target SIL 3 2oo3





NOT ENOUGH RISK REDUCTION

Recommended Reading

ection Layer

file:///C:/Users/ue/Documents/Hybrid%20Protection%20Layers.pdf

p - UE Mail OWA GoToAssist

An Integrated Approach to Design Hybrid Independent Protection Layers

Henry Johnston
Principal Specialist
Risk and Reliability Management
Genesis North America
Houston, USA

Genebelin Valbuena
Department Head
Risk and Reliability Management
Genesis North America
Houston, USA

Keywords: High Integrity Pressure Protection System (HIPPS), Independent Protection Layer (IPL), Safety Instrumented Systems (SIS), Safety Instrumented Functions (SIF), Safety Integrity Level (SIL), Risk Reduction Factor (RRF), Pressure Relieve Valve (PRV), Pressure Relief Systems, Quantitative Risk Analysis (QRA), Common Cause Failure (CCF), Reliability Analysis, Fault Tree Analysis (FTA).

Abstract

A popular method to assess process risks semi-quantitatively and determine the performance requirements of safeguards which may prevent the materialization of the risk scenario is a fault propagation modeling technique called Layer of Protection Analysis (LOPA). It is popular because it is neither excessively complex nor time consuming, and provides better accuracy than qualitative estimates. The principle behind LOPA is to determine effective safeguards, called independent protection layers (IPL), capable of preventing and/or mitigating the consequence. The safeguards qualify as IPLs only if they are specific, independent, reliable, and auditable [1].

Companies have developed procedures to apply LOPA methodology, pre-establishing possible initiating causes and their likelihoods, as well as IPL types. IPL types are mostly mechanical (pressure relief valves, rupture disks, check valves, restrictive office, mechanical over-speed trip, etc.), or instrument related (control loops, alarms, SIF). IPL type lists are usually restrictive and a combination of mechanical and instrumented systems is not commonly addressed.

Many times, during LOPA exercises, the identified safeguard cannot meet the specificity requirement

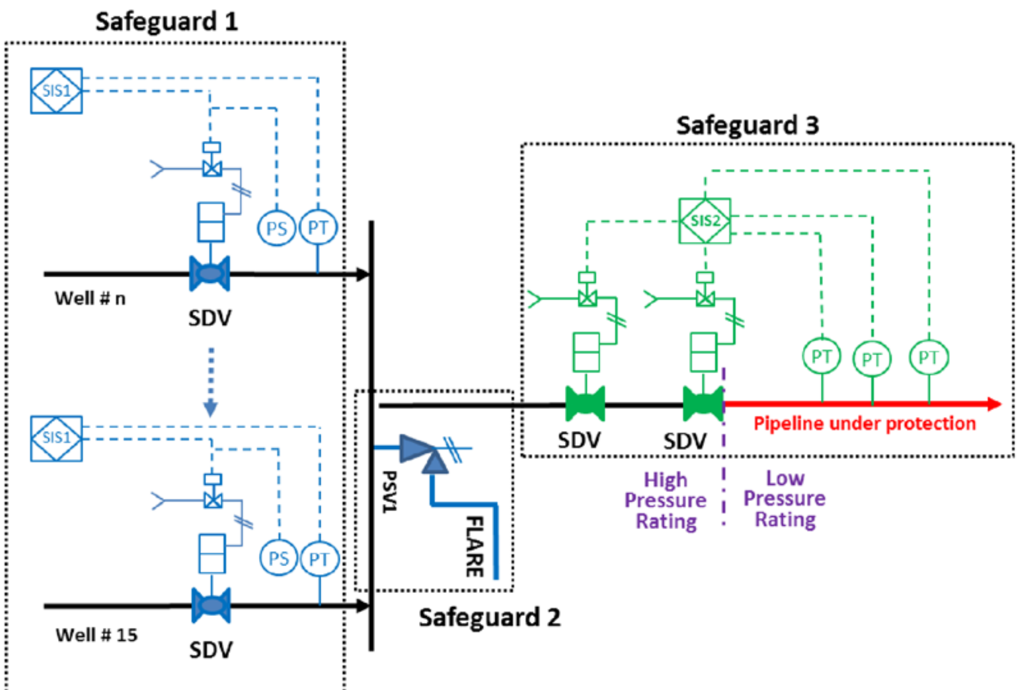
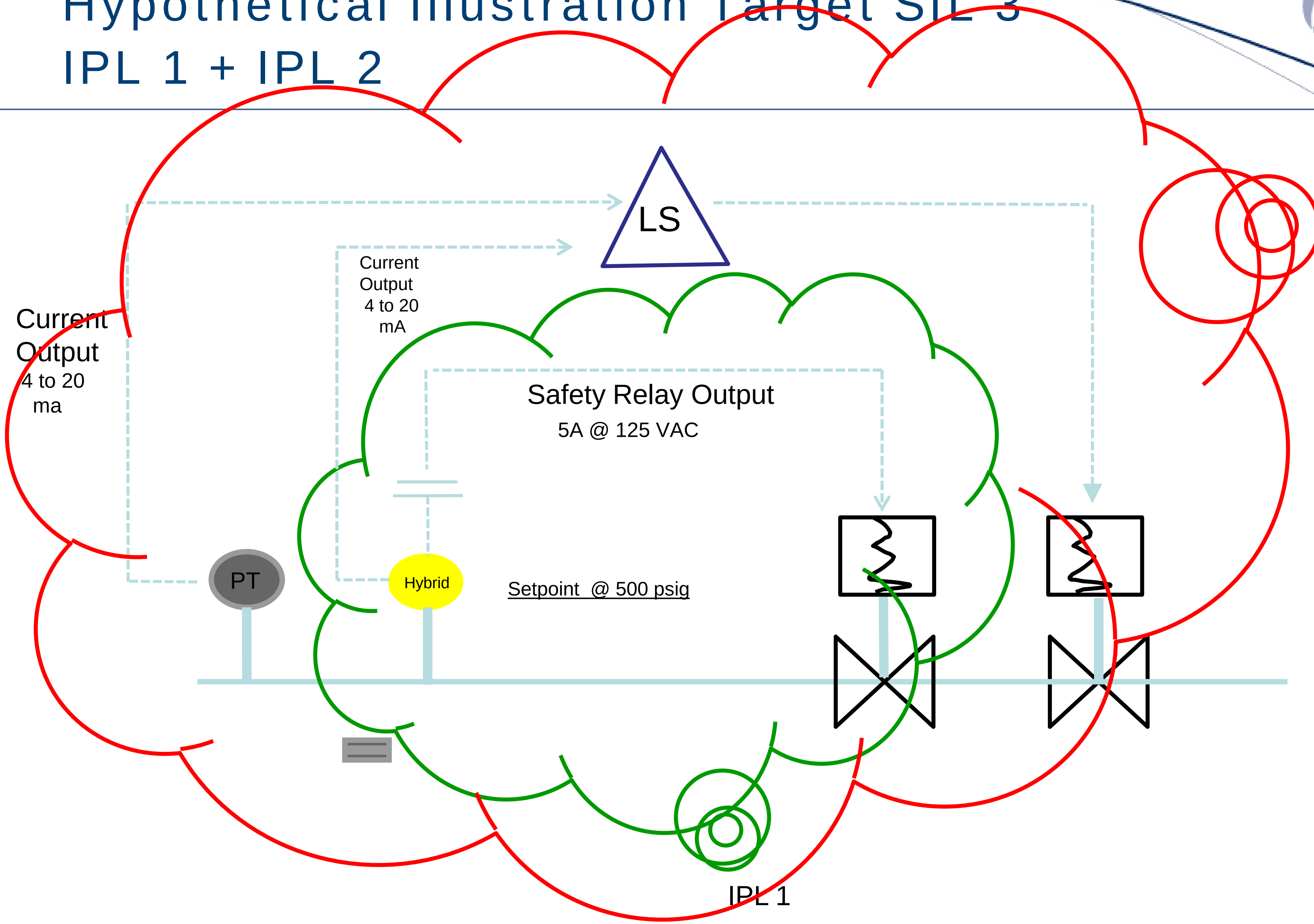


Figure 1. Simplified Process Diagram

Hypothetical Illustration Target SIL 3
IPL 1 + IPL 2

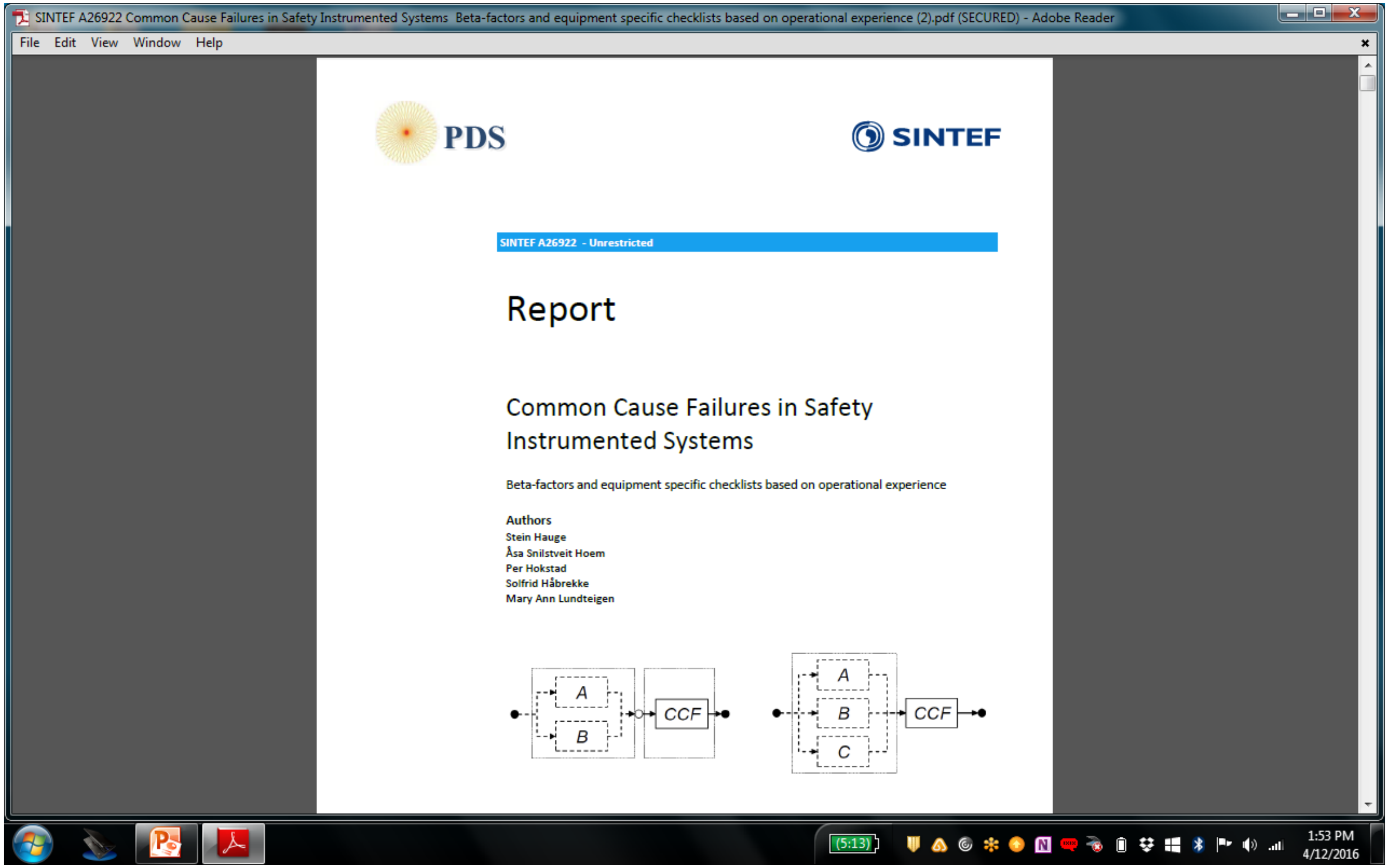


Comparing Attributes (Three SIL 2 Certified Sensors)

Product	Safe Failure Fraction	Safety Accuracy	Fault Detection	Number of Safety Variable Outputs	Enviromental Profile (per IEC 60654-1	MTTR	Input to Output Trip Response Time	IEC 61508
Hybrid Transmitter	98.6%	±3%	6 sec	4	C3	24 hours	~ 60 ms	Edition 2, 2010
Process Transmitter	95%	±2%	30 sec	1	C3	24 hours	N/A	Edition 2, 2010
Trip Alarm	91.4%	±2%	15 minutes	2*	B2	8 hours	256 msec	Edition 2, 2010

* Assumes fault relay is wired in series with process relays for fault monitoring

Can Hybrids Addressing Common Cause ?



Common Cause Failure
Major Equipment Groups

SINTEF A26922 Common Cause Failures in Safety Instrumented Systems Beta-factors and equipment specific checklists based on operational experience (2).pdf (SECURED) - Adobe Reader

File Edit View Window Help

SINTEF

Equipment group	Total population	N_{DU}	$N_{DU,CCF}$	New suggested β	β from PDS 2013 data handbook (for comparison)
ESD/PSD valves (incl. riser ESD valves)	1120	279	68	**12 %**	5 %
Blowdown valves	228	73	17	**12 %**	5 %
Fire dampers	458	44	23	**20 %**	5 %
PSVs	2356	148	32	**11 %**	5 %
Gas detectors (point and line)	2239	74	20	**15 %**	7 %
Fire detectors (flame, smoke and heat)	5921	65	19	**15 %**	7 %
Process transmitters (level, pressure, temperature and flow)	1746	112	32	**15 %**	6 %

Summarizing Benefits of the Hybrid

- Highly distributed SIS
- Where full blow safety systems are cost prohibitive.
- Where ESD and continuous monitoring are needed.
- Where process safety time thresholds cannot be met.
- Where diversity can reduce common cause.
- Where lower unit price points for certified devices are desirable.
- Where lower total cost solutions are imperative.

Thank you for your attention

For more information contact:

- Channing Reis, Director Functional Safety Technologies, United Electric Controls Company, Watertown, MA (USA) 617-899-1132
  creis@ueonline.com