An Overview of ISA 84 Standard for Safety Instrumented Systems (SIS) and the Safety Life Cycle

Presented in July 2015

By Jennifer L. Bergstrom

Process Engineering Associates, LLC

PROCESS ENGINEERING ASSOCIATES, LLC
"Excellence in Applied Chemical Engineering"

ISA 84 Safety Instrumented Systems and the Safety Life Cycle

Agenda:

- Safety components, acronyms, and definitions
- ANSI/ISA 84.00.01 Standard for Safety Instrumented Systems
- Safety Life Cycle
- Incorporating safety systems into process design
- Workshop

PROCESS
ENGINEERING ASSOCIATES, LLC
"Excellence in Applied Chemical Engineering"

Components, Acronyms, and Definitions

- Components:
  - Safety Instrumented Function (SIF)
  - Safety Instrumented System (SIS)
  - Safety Integrity Level (SIL)
  - Safety Requirement Specification (SRS)
  - Safety Life Cycle
  - Independent Protection Layer (IPL)

PROCESS
ENGINEERING ASSOCIATES, LLC
"Excellence in Applied Chemical Engineering"

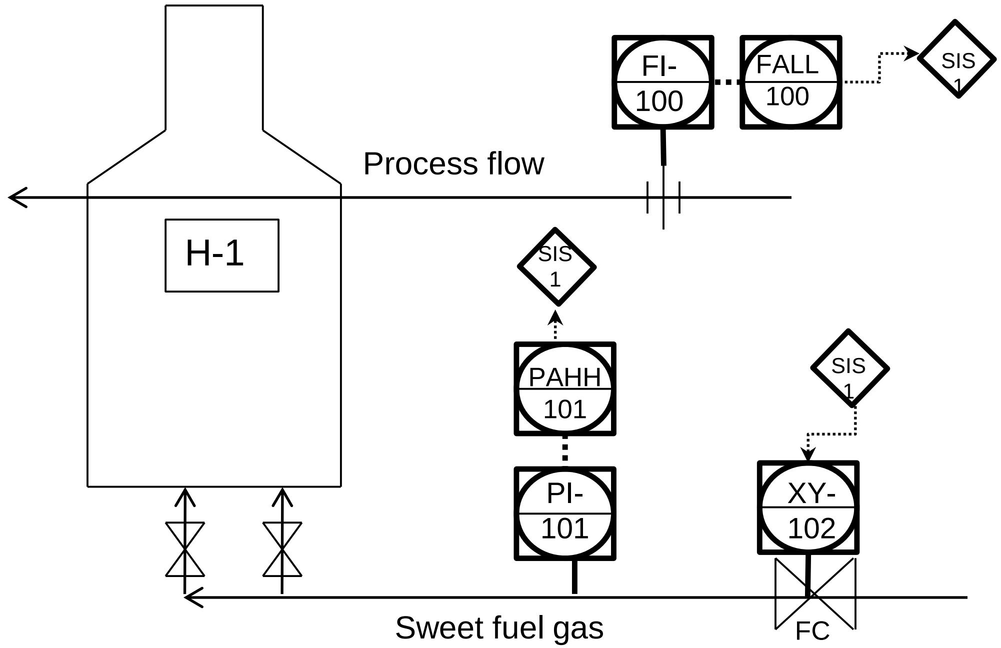
Components, Acronyms, and Descriptions

- SIF – Safety Instrumented Function
  - Individual interlock or automatic trip function that is designed to alleviate or minimize an undesired hazard, as determined in the PHA/HAZOP and the SIL Selection/LOPA
  - Includes all instrumentation in the interlock function, from the sensor and transmitter through the control system all the way to the final element (e.g., isolation valve)

PROCESS ENGINEERING ASSOCIATES, LLC
"Excellence in Applied Chemical Engineering"

Components, Acronyms, and Descriptions

- SIS – Safety Instrumented System
  - A critical system that consists of one or more automatic Safety Instrumented Functions (SIFs) or interlocks
    - Example: Fired Heater burner management system (BMS)



PROCESS ENGINEERING ASSOCIATES, LLC
"Excellence in Applied Chemical Engineering"

Components, Acronyms, and Definitions

- SIL – Safety Integrity Level

  Risk reduction levels:

SIL	RRF	PFD (1/RRF)
0	0-10	$\geq 10^{-1}$
1	>10 to ≤100	$\geq 10^{-2}$ to $<10^{-1}$
2	>100 to ≤1000	$\geq 10^{-3}$ to $<10^{-2}$
3	>1000 to ≤10,000	$\geq 10^{-4}$ to $<10^{-3}$
4	>10,000 to ≤100,000	$\geq 10^{-5}$ to $<10^{-4}$

PROCESS
ENGINEERING ASSOCIATES, LLC
"Excellence in Applied Chemical Engineering"

Components, Acronyms, and Definitions

- SIL – Safety Integrity Level
  - Level of risk reduction that a SIF must achieve
    - Target / Required SIL – amount of risk reduction determined as a need during PHA / HAZOP and then the level is determined during a simplified SIL Selection or elaborate LOPA (Layer of Protection Analysis)
    - Achieved / Verified SIL – calculated risk reduction utilizing Markov equations and includes all components of the interlock to determine the level of risk reduction (RRF) or 1/PFD (Probability of Failure on Demand)

PROCESS ENGINEERING ASSOCIATES, LLC
"Excellence in Applied Chemical Engineering"

Components, Acronyms, and Definitions

- SIL – Safety Integrity Level

  Levels of risk:

  - SIL 0 (none) – tolerable risk
  - SIL 1 – minimal risk
    - 95% of all SIL-rated interlocks
  - SIL 2 – medium risk
    - Less than 5% of all SIL-rated interlocks
  - SIL 3 – high risk
    - Less than 1% of all SIL-rated interlocks (typically found in the nuclear industry or off-shore platforms)
  - SIL 4 – highest risk (not likely in petroleum or chemical industry)

PROCESS ENGINEERING ASSOCIATES, LLC
"Excellence in Applied Chemical Engineering"

Components, Acronyms, and Definitions

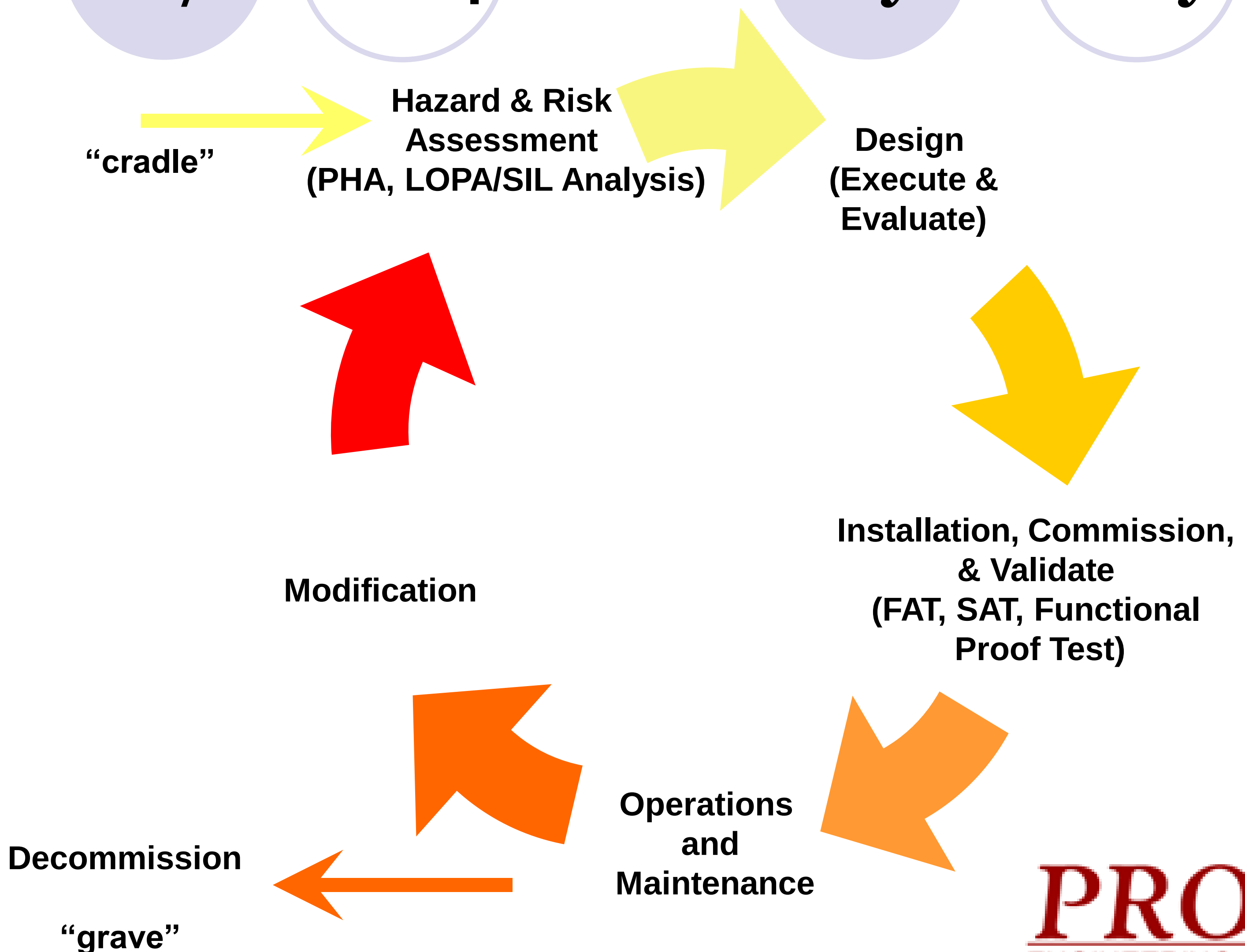
- SRS – Safety Requirement Specification
  - Document containing detailed SIS interlock information
- Safety Life Cycle –
  - Activity designed to include all phases of the life of a SIF and SIS
    - *KEY NOTE*: It's not enough to just ***install*** a SIS. It must be properly designed and maintained so it is available when the need arises!!!
  - ANSI/ISA 84 and Safety Life Cycle were developed to guide a safety system from the Risk Assessment "cradle" to the Decommissioning "grave".

ANSI/ISA 84.00.01 Standard for SIS

- ANSI/ISA 84.00.01 - Application of Safety Instrumented Systems (SIS) for Process Industries :
  - Follows IEC 61511
  - First version in 1996
  - Second version approved in 2004 (included a "Grandfather Clause")
  - OSHA recognizes this standard as a RAGAGEP
  - Defines Safety Instrumented System (SIS)
  - Defines all phases required in Safety Life Cycle

PROCESS ENGINEERING ASSOCIATES, LLC
"Excellence in Applied Chemical Engineering"

ANSI/ISA 84 and Safety Life Cycle



PROCESS ENGINEERING ASSOCIATES, LLC
"Excellence in Applied Chemical Engineering"

Why SIS and Safety Life Cycle?

- Accidents/Incidents can and do occur, so in order to help minimize the frequency and/or severity -
- Safety Instrumented Systems and Safety Life Cycle are designed to minimize risk
- But if the Safety Life Cycle is stopped, this could occur…

PROCESS
ENGINEERING ASSOCIATES, LLC
"Excellence in Applied Chemical Engineering"

BP Refinery - Texas City

PROCESS
ENGINEERING ASSOCIATES, LLC
"Excellence in Applied Chemical Engineering"

Why SIS and Safety Life Cycle?

- 15 fatalities and 180 injuries that day in 2005
- Resulted in multitude of citations with a hefty fine of $21MM
- 2009 – Follow-up FTA inspection was conducted and $87MM fine was given; most of the FTAs related to PSVs and SIS

Why SIS and Safety Life Cycle?

- Due to public concern over the severity of the 2005 BP Texas City incident, OSHA initiated NEP (National Emphasis Program) inspections in petroleum refineries across the country in 2007
  - OSHA included SIS analysis in the NEP dynamic list for refineries (due to SIS and instrumentation failures considered as contributing causes of the BP incident)
  - OSHA more recently initiated a nationwide NEP directive for chemical facilities with PSM-covered chemicals in late 2011

Why SIS and Safety Life Cycle?

- ANSI/ISA 84.00.01 - Application of Safety Instrumented Systems (SIS) for Process Industries:
  - OSHA recognizes this standard as RAGAGEP (Recognized and Generally Accepted Good Engineering Practice) and has considered it to be within the scope of OSHA 1910.119 PSM regulation under Mechanical Integrity (MI)

PROCESS ENGINEERING ASSOCIATES, LLC
"Excellence in Applied Chemical Engineering"

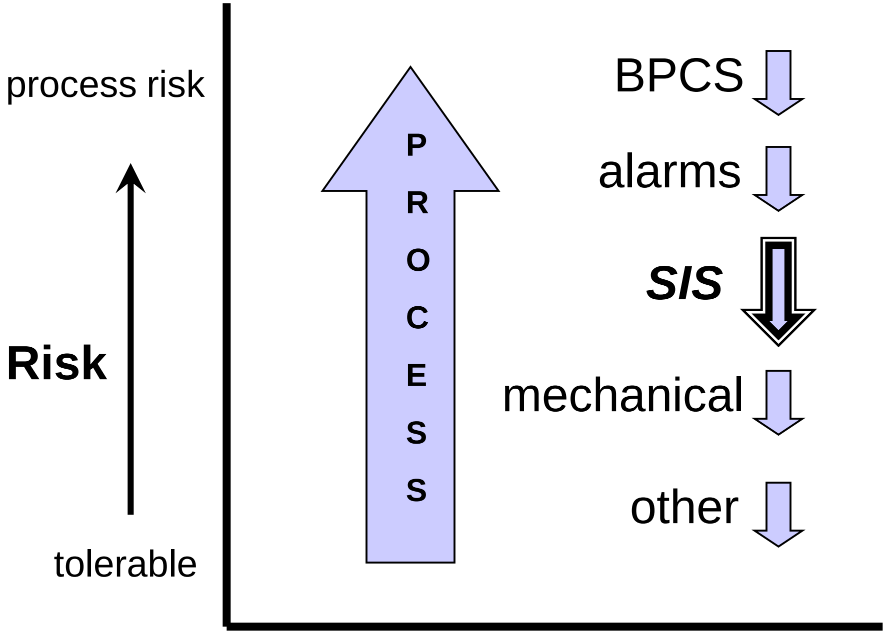
Protection Layers

- IPL – Independent Protection Layer
  - Protective items, when used alone or in combination with diverse types, that are meant to reduce risk to personnel, the environment, or property
    - Examples: BPCS (control system), alarms and operator response, SIS, physical devices (PSVs, dual seals, dikes, flares, deluges, etc.), and other human mitigation (emergency response)

PROCESS
ENGINEERING ASSOCIATES, LLC
"Excellence in Applied Chemical Engineering"

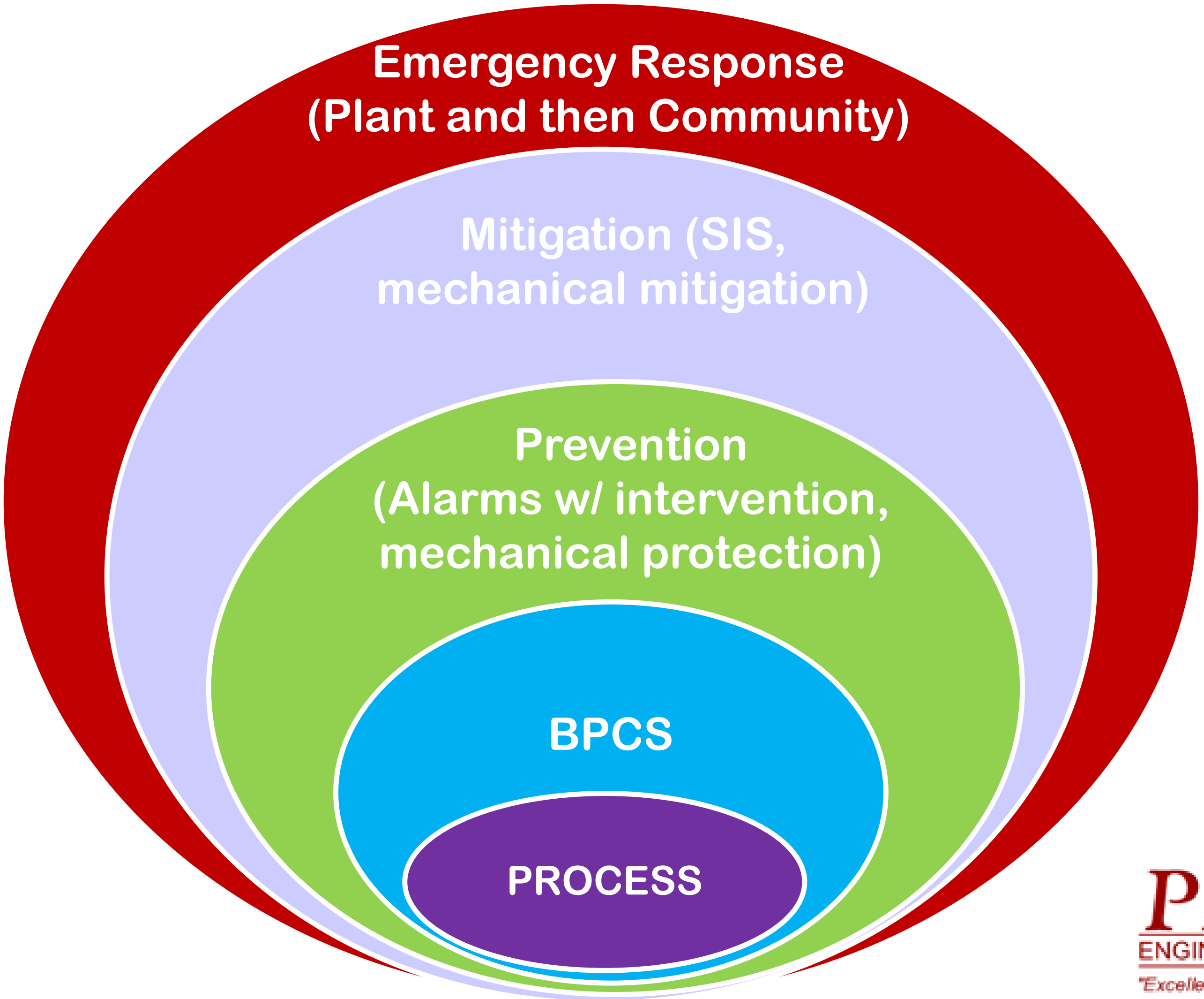
Protection Layers

- Process Hazards/Risk and IPLs (ups and downs)



PROCESS ENGINEERING ASSOCIATES, LLC
"Excellence in Applied Chemical Engineering"

Protection Layers



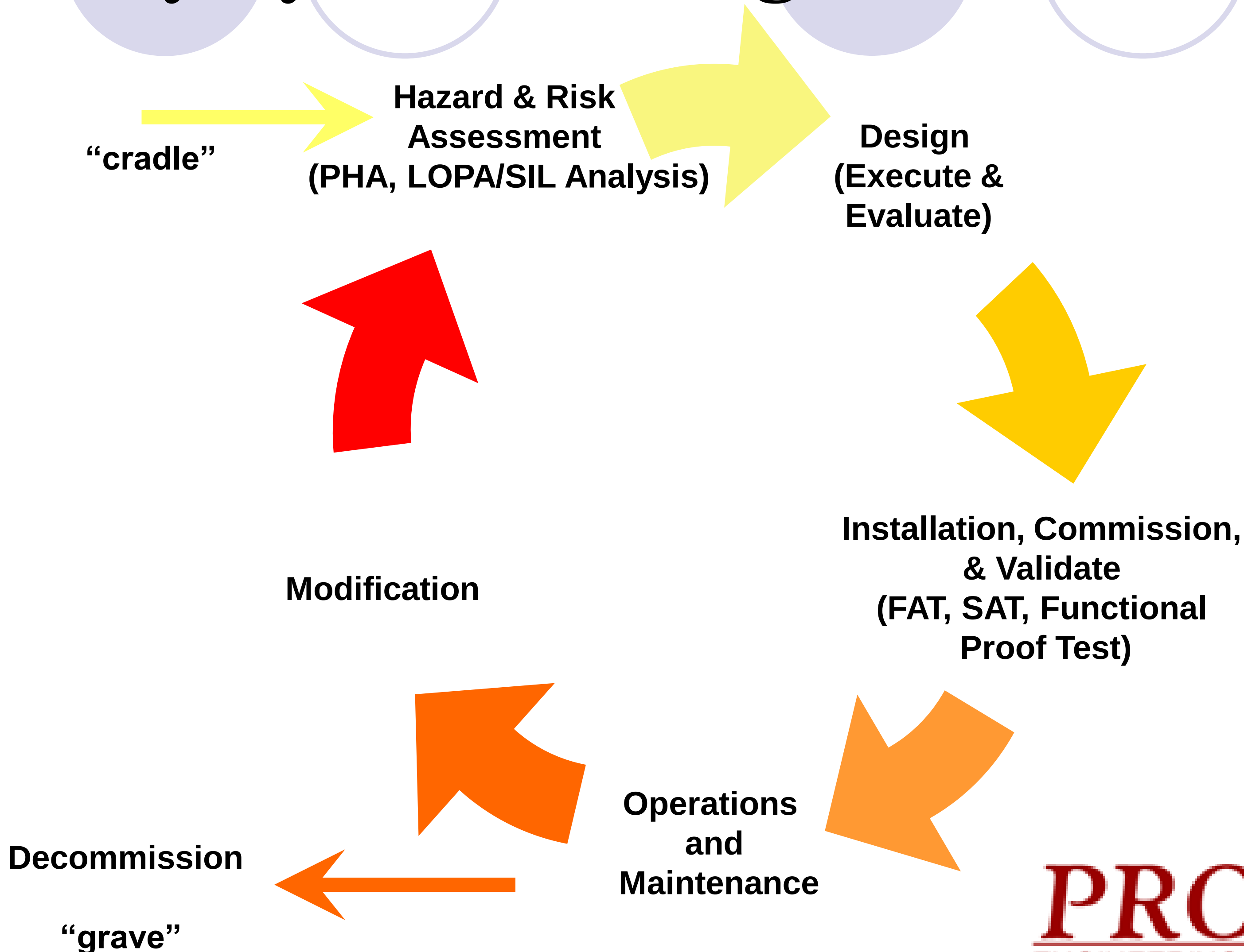
PROCESS ENGINEERING ASSOCIATES, LLC
"Excellence in Applied Chemical Engineering"

Protection Layers / SIFs / SISs

- Safety systems/interlocks are a vital protection layer between the hazards of the process and the public when inherent design is not enough
- Safety Systems are added to the process design to minimize these risks to a tolerable level or ALARP (As Low As Reasonably Practical)

PROCESS
ENGINEERING ASSOCIATES, LLC
"Excellence in Applied Chemical Engineering"

Safety Systems Design



PROCESS ENGINEERING ASSOCIATES, LLC
"Excellence in Applied Chemical Engineering"

Safety Systems Design

- SIF/SIS is added to a design during the "cradle" stage or PHA as a safeguard to mitigate or minimize a hazard
- Each SIF is assigned a Safety Integrity Level (SIL) during the SIL Analysis or LOPA risk assessment
  - SIL 0 – lowest risk
  - SIL 4 – highest risk
- Each incremental SIL must be more reliable and available to operate when required (thus installation and maintenance costs increase)

PROCESS
ENGINEERING ASSOCIATES, LLC
"Excellence in Applied Chemical Engineering"

Safety Systems Design

- Requirements when designing SIS:
  - Separation:
    - Instrumentation – interlock instrumentation CAN NOT be part of control logic
    - Safety Control System – requires safety logic solver that segregates its inputs and outputs
  - Robust equipment options:
    - Examples:
      - Honeywell ST3000 Safety transmitter with HART 6.0
      - MAXON MM/MA series safety isolation valves
      - DeltaV Redundant SLS

PROCESS ENGINEERING ASSOCIATES, LLC
"Excellence in Applied Chemical Engineering"

Safety Systems Design

- Reliability and availability can also be achieved by:
  - Architecture
    - Using redundancy and voting logic of the initiators, safety control system, and/or final elements (e.g., 1oo2, 2oo3 required to achieve safe state)
  - Installation – per manufacturer's guidelines
  - Testing / Validation and Replacement – both at initial startup as well as at specified testing intervals or after any modification (i.e., via PSSR)

Safety Systems Design

- When designing or modifying a SIS, keep in mind there are two types of failures:
  - Safe Failures
  - Dangerous Failures
- Safe Failures are the desired failure
  - Initiated (actual event)
  - Spurious (false – undesired but still safe)
- Dangerous failures are not desired
  - Inhibited (bypassed)
  - Dangerous operation (doesn’t trip when needed)

PROCESS
ENGINEERING ASSOCIATES, LLC
"Excellence in Applied Chemical Engineering"

Safety Systems Design – Voting Logic

- How to design for safe failures without dangerous failures or with minimal spurious trips?

- Voting Logic

	Safe	Dangerous
1oo1	good	good
1oo2	good	best
1oo2D	best	better
2oo2	better	good
2oo3	best	better

Best blend of both

(Source: ISA & Exida)

PROCESS ENGINEERING ASSOCIATES, LLC
"Excellence in Applied Chemical Engineering"

Safety Systems Design - SIL Verification

- SIL verification involves multiple Morkov model calculations to determine the achieved SIL range
- Interlock component data used for verification:
  - MTTFS
  - PFD_{avg}
  - RRF (inverse of PFD or 1/PFD)
  - $\beta\%$ (when using multiple components)
  - λ_{du} (undetected dangerous failures)
  - λ_{sp} (safe or spurious failures)

PROCESS ENGINEERING ASSOCIATES, LLC
"Excellence in Applied Chemical Engineering"

Safety Systems Design - SIL Verification

Safety Integrity Level (SIL)	Safety Instrumented System Performance Requirements		
	Safety Availability Required	Average Probability of Failure on Demand (PFDavg)	Risk Reduction Factor (RRF) RRF=1/PFD
1	90.00 – 99.00 %	10^{-1} to 10^{-2}	10 to 100
2	99.00 – 99.90 %	10^{-2} to 10^{-3}	100 to 1,000
3	99.90 – 99.99 %	10^{-3} to 10^{-4}	1,000 to 10,000

PROCESS
ENGINEERING ASSOCIATES, LLC
"Excellence in Applied Chemical Engineering"

Safety Systems Design - SIL Verification

- If the required SIL can not be achieved with the initial design, some options are:
  - More frequent proof testing
  - Add redundancy (i.e., initiating device, control system, final element)
  - Install "smarter" device (i.e., HART smart transmitter or transmitter vs. switch or relay, smart control /isolation valve with diagnostics and feedback and position indication vs. basic control valve)
  - Add other IPL(s)

PROCESS ENGINEERING ASSOCIATES, LLC
"Excellence in Applied Chemical Engineering"

Validation/Functional Proof Testing

- Proof Tests must be performed at the frequency determined during SIL verification (and as stated in the SRS) to validate the reliability of the SIF
  - Many facilities prefer to perform these tests during turnaround, so SIS may be designed to perform between 4-5 year testing frequency
- It should include the following information:
  - Test procedure
  - Date of test and all personnel performing the test
  - Control logic – version # (if available)
  - Results of entire test and any abnormalities found

PROCESS ENGINEERING ASSOCIATES, LLC
"Excellence in Applied Chemical Engineering"

General Concepts to Remember in Design

- Separation from control logic
- Two words in design to achieve lower MTTFS (PFD) or higher RRF to achieve the SIL:
  - Diagnostics, diagnostics, diagnostics,…
  - Redundancy

Transmitters with diagnostics (i.e., HART) can detect problems before going awry or failing, making troubleshooting and repair much easier

- Hence, the desire for transmitters with diagnostics over switches

PROCESS
ENGINEERING ASSOCIATES, LLC
"Excellence in Applied Chemical Engineering"

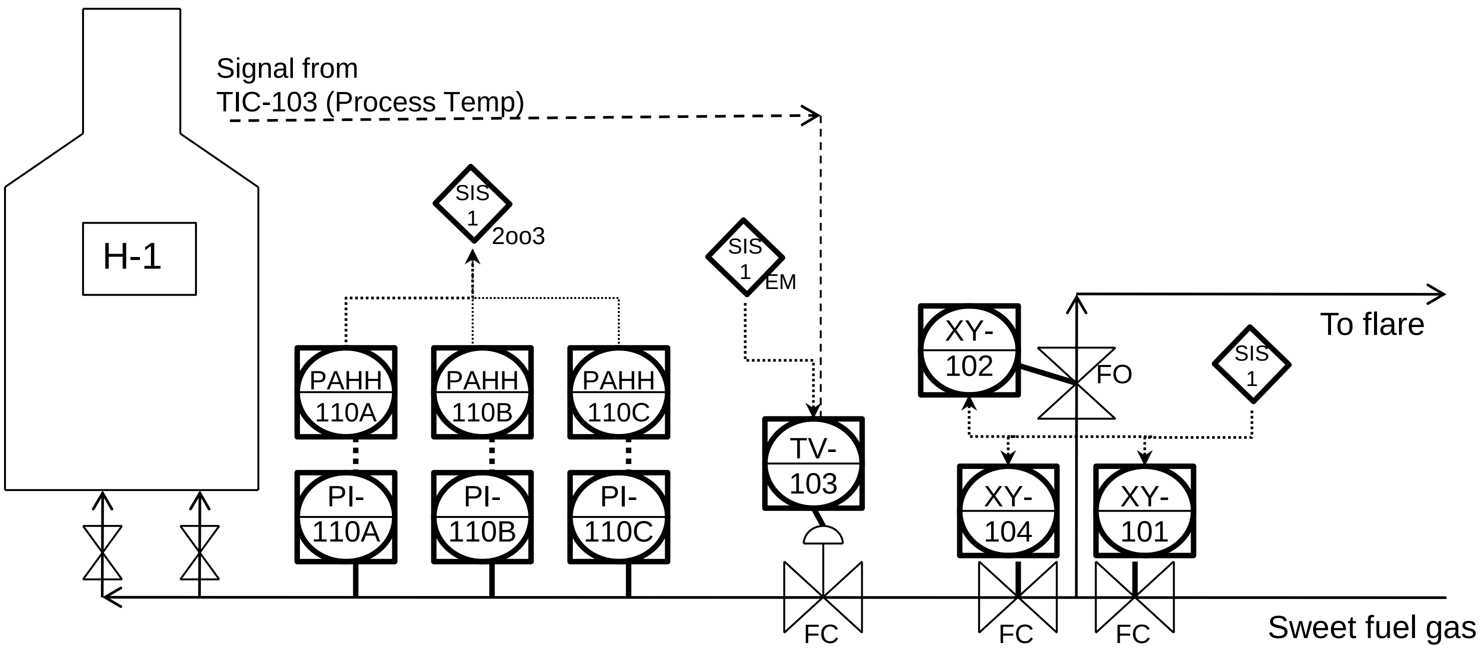
General Concepts to Remember in Design

- If using switch, solenoid, or relay (anything on/off or discrete), verify that it is normally energized during operation (fail safe)
- Use dedicated wiring to each device (as much as possible)
- Minimize common cause failures (i.e., common wires, instrument taps, or same controller or I/O card)
- Mechanical devices are the weakest link in the SIF. They can stick if not moved periodically (i.e., PSVs, valves, switches)
  - To remedy this issue: install dual isolation or modulating valves that can be partially stroked

PROCESS
ENGINEERING ASSOCIATES, LLC
"Excellence in Applied Chemical Engineering"

Workshop – Fired Heater H-1 P&ID

What voting logic/redundancy options are used in this SIF?
(hint: both initiators and final elements)



PROCESS ENGINEERING ASSOCIATES, LLC
"Excellence in Applied Chemical Engineering"

Final Review

- Components
  - IPL
  - SIS
  - SIF
  - SIL
    - Required/ Target SIL
    - Achieved SIL
  - SRS
  - Safety Life Cycle
    - cradle to grave

Final Review

- Design of the SIF/SIS must be capable of achieving the target SIL
- Design of the SIF/SIS should minimize common cause and dangerous failures
- Employer must continue the Safety Life Cycle timelines as determined in the SRS to the keep the SIF reliable and available to reduce risk
  - Functional Proof Test – at a specified interval or after any changes to hardware or software configuration
  - Mission Time – hardware replacement interval
  - Document any modifications to SIS or protection layers (MOC)

PROCESS ENGINEERING ASSOCIATES, LLC
"Excellence in Applied Chemical Engineering"

Introduction to ***PROCESS***

- ***PROCESS*** *Chemical Engineering Services*
  - Process Design (FEL-0, 1, 2, and 3)
  - Process Modeling/Simulation (CHEMCAD/Aspen/HYSYS/etc.)
  - Operations Support
  - Process Safety Services (PHAs, LOPA, SIL Selection, etc.)

- *The* ***PROCESS*** *Competitive Advantage*
  - The Best Process Engineers Available
  - State of the Art Process Engineering Tools
  - Extremely Responsive to Client's Needs
  - Available for Projects Worldwide
  - Only Process Engineering Services
  - Independent
  - On Time
  - Under Budget
  - Competitive Pricing

PROCESS
ENGINEERING ASSOCIATES, LLC
"Excellence in Applied Chemical Engineering"