

Safety Instrumented Systems (SIS) and Safety Life Cycle

Presented in September 2009

By Jennifer L. Bergstrom

Process Engineering Associates, LLC

Safety Instrumented Systems (SIS) and Safety Life Cycle

Agenda:

- ISA standard that defines Safety Life Cycle
- Safety concepts (including a lot of new acronyms)
- Aspects of the Safety Life Cycle and how to take it from “cradle” to “grave”
- Ways to incorporate SIS into process design

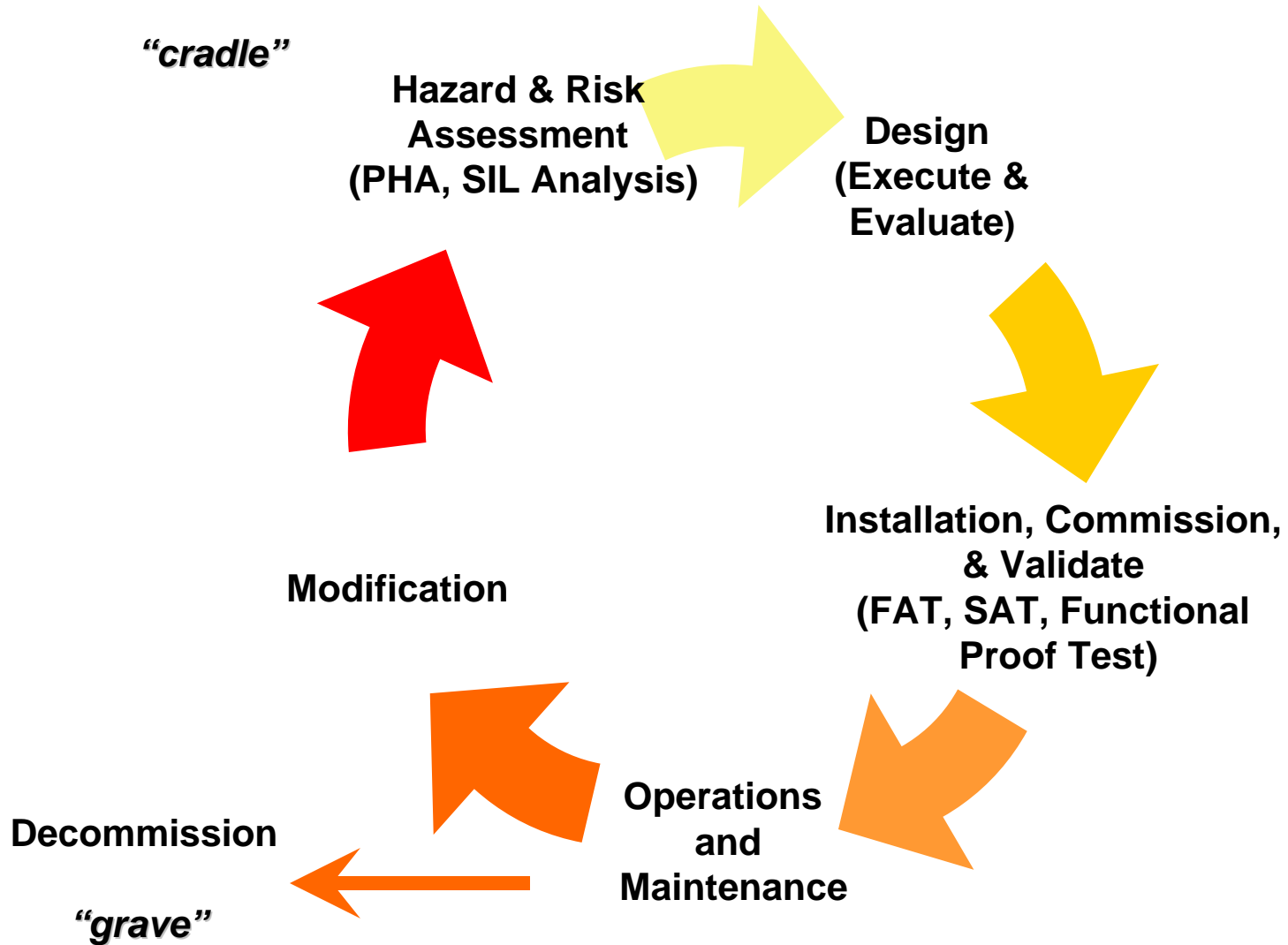
ANSI/ISA 84.00.01-2004 for SIS

- ANSI/ISA 84.00.01-2004 (IEC 61511-Mod) - Application of Safety Instrumented Systems (SIS) for Process Industries :
 - First version in 1996
 - Second version approved in 2004 (only addition was "Grandfather Clause")
 - OSHA recognizes this standard as a RAGAGEP
 - Defines all steps that encompass the Safety Life Cycle
 - Defines a Safety Instrumented System (SIS)

Safety Life Cycle

- Concepts (safety acronyms):
 - Safety Life Cycle
 - Safety Instrumented System (SIS)
 - Safety Integrity Level (SIL)
 - Safety Instrumented Function (SIF)
 - Safety Requirement Specification (SRS)

Safety Life Cycle



Safety Life Cycle

- Definition: "An engineering process designed to achieve a risk-based level of safety with performance criteria that allow versatile technologies and optimal design solutions." -exida
- In other words, the cycle is meant to guide a safety system from the Risk Assessment "cradle" to the Decommissioning "grave".

Why Safety Life Cycle?

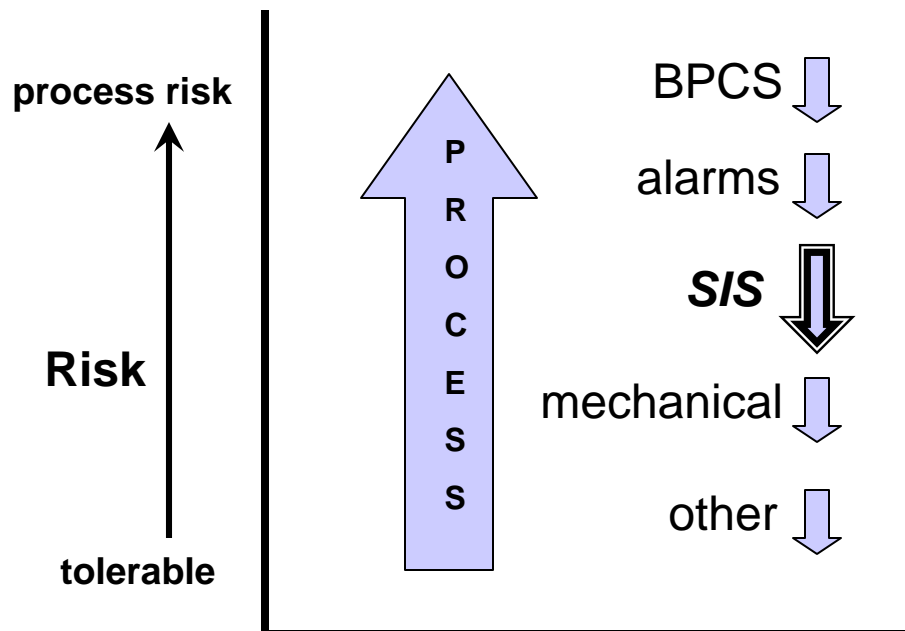
- Accidents can and do occur, so in order to help minimize the frequency and/or severity.....
- Safety Instrumented Systems and Safety Life Cycle were designed to minimize risk

Protection Layers

- SIS is used as a protection layer between the hazards of the process and the public (the worse the potential hazard, the more layers required for prevention/protection)
- Examples:
 - BPCS (control system), alarms and operator response, SIS, physical devices (PSV's, dikes, flares, deluges, etc.), and other human mitigation (emergency response)

Hazards and Risks in Industry

- Risk – ups and downs –



SIF and SIL

- Safety Instrumented Function (SIF) is designed to minimize process risks to a tolerable level (or ALARP)
- Each SIF is assigned a Safety Integrity Level (SIL) during SIL analysis - risk assessment
 - **SIL 0/none** – lowest risk
 - **SIL 1** – 95% of the SIFs
 - **SIL 2** – 5% of SIFs
 - **SIL 3** – < 1% (not likely in refineries, but possible in off-shore platforms or nuclear)
 - **SIL 4** – highest risk (only seen in nuclear industry)

Safety Integrity Level (SIL)

- Each SIL rating (increasing in number) must be that much more reliable and available at all times (and costs more for upkeep).
- Reliability and availability are achieved by:
 - Design – using proper safety components
 - Installation – per manufacturer's guidelines
 - Testing – both at initial startup as well as at specified intervals or after any modification (i.e., via PSSR)

Design

- Phase where the SIF/SIS is developed to achieve the risk reduction that is determined in the PHA or SIL Analysis (target SIL). Design options can include:
 - Redundancy (initiators, control system, and/or final elements)
 - Type/style of components (transmitter vs. switch or modulating valve vs. on/off chop valve)
- **NOTE:** If a SIS already exists, then analysis of the existing system is done to determine if the target SIL can be achieved with the current design. (“Grandfather Clause”)

Design - Type of Failures

- When designing or modifying a SIS, keep in mind there are two types of failures:
 - Safe Failures - "FAIL SAFE"
 - 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)

Design - Type of Failures

- How do we design for safe failures with minimal spurious trips?

- Voting Logic

	Safe	Dangerous
1001	good	good
1002	good	best
1002D	best	better
2002	better	good
2003	best	better

(Source: ISA & Exida)

Safety Requirement Specification (SRS)

- The design and verification is compiled into a document called the Safety Requirement Specification (SRS)
 - Information included:
 - Intent of each SIF (the hazard that is mitigated)
 - Components of each SIF (sensor, logic solver, final element)
 - Calculations to verify the target (required) SIL can be achieved

SIL Verification

- SIL verification involves multiple equations to determine the achieved SIL.
- Some of the components to verify this include:
 - MTTFS
 - PFD
 - RRF (inverse of PFD or $1/\text{PFD}$)
- NOTE: SIL 1 achieves a RRF of 10 to 100

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 valve with diagnostics and feedback and position indication vs. basic control valve)
 - Add protection layers (independent)

General Concepts to Remember in Design

- Two ways to achieve lower MTTFS (PFD) or higher RRF to achieve the target SIL:
 - Diagnostics, diagnostics, diagnostics,...
 - Redundancy
- Instrumentation with diagnostics is the key!
 - Feedback information can tell you the condition of the instrument and whether it is “ill” and about to fail

General Concepts to Remember in Design

- Transmitter is better than a switch or relay
- 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 – including bridles, 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 double blocks or modulating valves that can be partially stroked

Functional Proof Tests

- Proof Tests must be performed at the frequency stated in the SRS to continue the reliability of the SIF.
- It should include the following information:
 - Test procedure
 - Test all bypasses, all individual initiators, and final elements
 - Results of all steps of the procedure
 - Verification that process has been restored to normal operation
 - Date of test and all personnel performing the test
 - Control logic – version # (if available)
 - Results of entire test and any abnormalities found

Final Review

- Safety Life Cycle
 - Guidelines for a safety system from the Risk Assessment “cradle” to the Decommissioning “grave”.
- SRS
 - It is only a portion of the Safety Life Cycle, but documents and verifies the SIF design
- Employer must also fulfill the SRS timelines as determined in the SRS to keep the SIF reliable and available to reduce risk.
 - Functional Proof Test – at a specified interval
 - Mission Time – replacement interval
 - Document any modifications to SIS or protection layers (MOC)