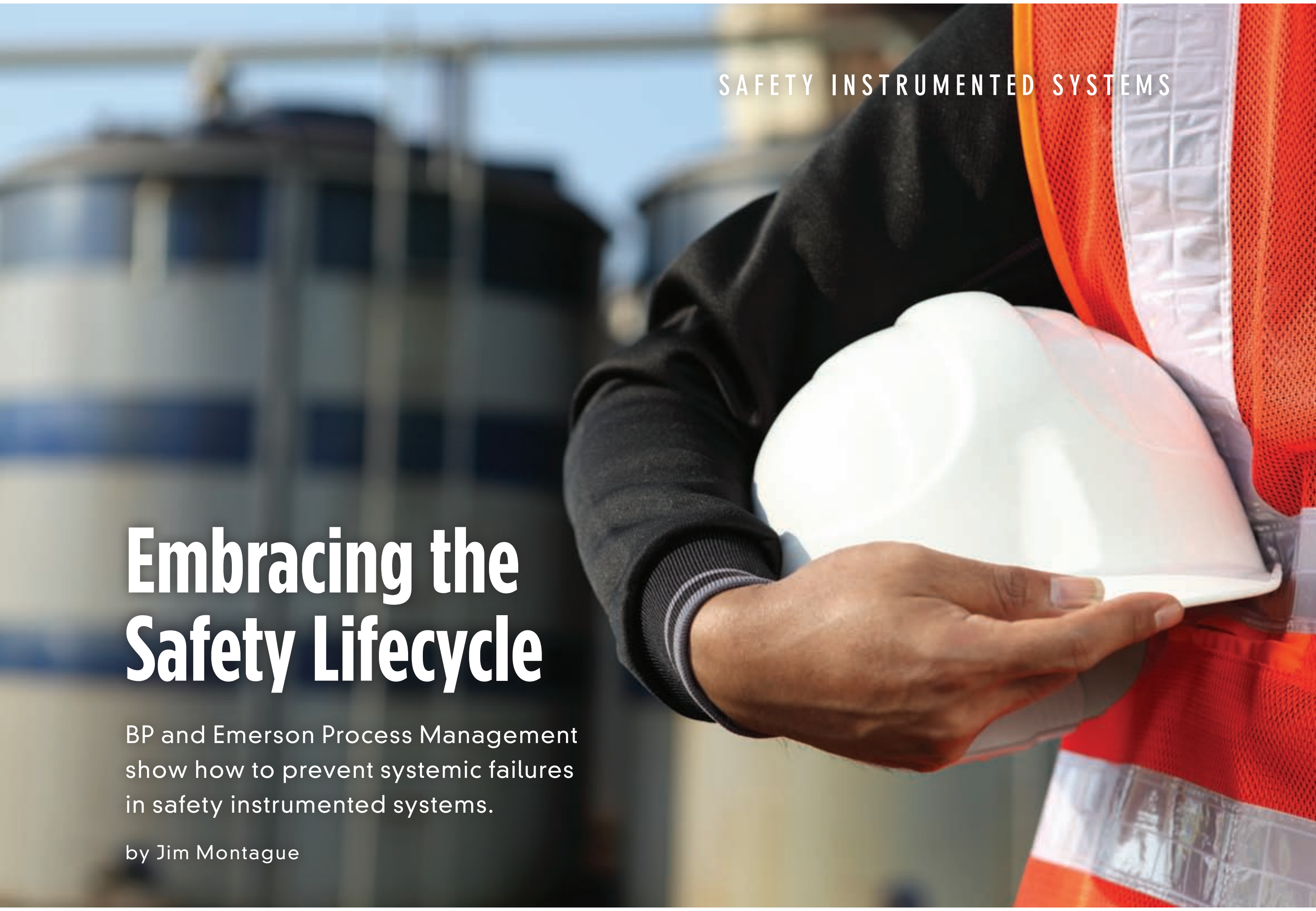
CONTROL



SAFETY INSTRUMENTED SYSTEMS

Embracing the Safety Lifecycle

BP and Emerson Process Management show how to prevent systemic failures in safety instrumented systems.

by Jim Montague

Having a safety instrumented system (SIS) doesn't make process control applications safe. Adopting it intelligently and managing it vigilantly makes them safe.

"All systems fail at some point in time," says Rahul Bhojani, PE, technical authority for downstream at BP (www.bp.com) "SISs can have random or systematic failures. Random failures are usually the result of degraded mechanisms in the hardware, such as corrosion or thermal shocks. Systematic failures are due to human error during the lifecycle of the SIS or process, and so they can occur during any phase of that lifecycle."

Bhojani and Len Laskowski, PE, principal technical consultant at Emerson Process Management's Midwest Engineering Center, presented "Safety Instrumented Systems: Why Do They Fail?" on Oct. 7 at the Emerson Global Users Exchange 2014 in Orlando, Florida.

"The good news is that failures can be learned from and help produce process safety standards, such as OSHA PSM 1910.119, as well as SIS standards, such as ISA 84/IEC 61511, which have evolved over time," explains Bhojani. "Some of these standards have requirements, while others have recommended good practices. Either way, it's important that applicable requirements are understood and followed."

For example, NFPA 86 states that, "In the event of a loss of flame, the burner management system on an oven or furnace shall close the safety shutoff valves to prevent gas from accumulating in the firebox." However, Laskowski reports this earlier version of the standard didn't cover whether users needed to make sure they didn't have a flame before they started. "The answer is yes! This is because a flame detector was once 'stuck on,' the flame went out and didn't trip the burner, and gas accumulated and caused an explosion," says Laskowski. "As a result, NFPA 86 now requires you to verify that no flame is present as part of the safe-start check."

Bhojani adds, "This is why details are so important in managing safety systems. You have to get a lot right in safety instrumented functions (SIFs) to get them to perform properly."

So how can you spot these issues? Bhojani advises taking several essential steps:

- Attend a thorough hazard and operability (HAZOP) study.
- Verify the layers of protection analysis (LOPA) evaluation.
- Have a complete safety requirements specifications (SRS) analysis.
- Install new functioning hardware.
- Install new tested software.
- Conduct regular proof tests.
- Train world-class operators.
- Use engineered trip setpoints or process delay time.

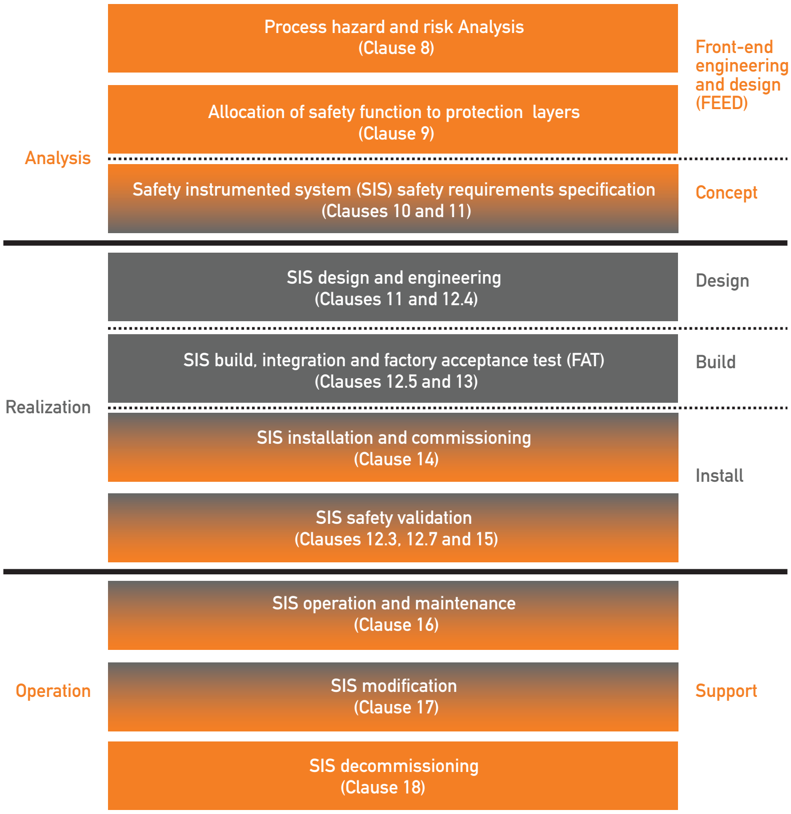
"However, you have to be careful here as well because you can negate a SIF because you haven't selected the right trip setpoint," adds Laskowski, who recommends adopting a three-part safety lifecycle procedure (Figure 1):

- The first part, Analysis, includes performing a process hazard and risk analysis, allocating safety functions to protection layers and drafting the SIS safety requirements specification.
- The second part, Realization, includes designing and engineering the SIS, building, integrating and factory acceptance testing it, installing and commissioning the SIS, and safety-validating it.
- The third part, Operation, includes operating and maintaining the SIS, modifying it as needed, and decommissioning it at the end of its lifecycle.

"Unfortunately, safety lifecycles can fail when all initiating causes aren't identified, such as when all fuel sources to BMSs [burner management systems], SRUs [sulfur recovery units] and thermal oxidizers aren't identified," explains Laskowski. "Likewise, during overfills, all inlet lines, not just big ones, need to be identified as closing on high level. Also, loss of utilities like power, steam, cooling water and instrument air can lead to initiation, and need to be identified. Finally, other consequences may have been under or overestimated."

To seek a stable safety lifecycle, Laskowski also suggests that SIS and process applications implement an "interaction matrix," which lists all raw materials, end products and other materials and equipment in a process application on an X-Y axis, and then cross-references their potential interactions with each other (Figure 2). "If two of these materials come in contact they could decompose, polymerize or become flammable," says Laskowski. "After one big explosion, the affected R&D department said it hadn't reported that the two materials involved could possibly explode because they were never supposed to be heated. In fact, they were cooled in this process. However, during start-up or shutdown, they did become heated, and that caused the accident.

"Many independent protection layers [IPLs] aren't as independent as they're described. There are common-cause failures. And many safety


Process hazard and risk Analysis
(Clause 8)
Front-end engineering and design (FEED)
Allocation of safety function to protection layers
(Clause 9)
Analysis
Safety instrumented system (SIS) safety requirements specification
(Clauses 10 and 11)
Concept
SIS design and engineering
(Clauses 11 and 12.4)
Design
SIS build, integration and factory acceptance test (FAT)
(Clauses 12.5 and 13)
Build
Realization
SIS installation and commissioning
(Clause 14)
Install
SIS safety validation
(Clauses 12.3, 12.7 and 15)
SIS operation and maintenance
(Clause 16)
SIS modification
(Clause 17)
Operation
Support
SIS decommissioning
(Clause 18)

WHAT IS THE SAFETY LIFECYCLE?

Figure 1: The procedure for adopting an effective and successful lifecycle for safety instrumented systems (SISs) includes three main steps—analysis, realization and operation—according to the IEC 61511-1 international standard, "Functional Safety–SISs for the Process Industry Sector."

	A	B	C	D	Air	Water	Steam
A	A	C + D			Flammable		Polymerizes
B	C + D	B			Pyrophoric		
C			C				?
D				D		Nerve gas	
Air	Flammable						
Water				Nerve gas			
Steam	Polymerizes		?				
Acid Wash Solution	Polymerizes	?					
Caustic Wash Solution	Polymerizes	?					
High Temp	Polymerizes		?				
Low Temp							
High Pressure							
O-Rings (Viton)	Decomposes						
Humidity		Pyrophoric		Nerve gas			
Carbon Steel	Corrosion	Corrosion	Corrosion	Corrosion			

SAMPLE INTERACTION MATRIX

Figure 2: An interaction matrix lists all raw materials, end products, and other materials and equipment in a process application on an X-Y axis, and then cross-references their potential interactions with each other, such as chemistry A+B leading to C+D.

functions aren't clearly defined and don't completely mitigate their hazards. One research study reported that 44% of failures are engineered into their application's specifications, so this is why the most important task is to validate your LOPA early. Further up in the process stream, the LOPA may not be as stringent and IPLs may not be as valid as they should be, and this little bit of wiggle room can cause some real problems. So users need to look at all possible modes of failure and also do complete testing."

Bhojani adds, "It's difficult to quantify direct project savings, but from a moral perspective, providing employees a safe workplace is the right thing to do, and it's also a legal requirement. Properly designed and operating SISs and other IPLs are fundamental to maintaining a license to operate a facility. This is why proper SIS lifecycle management is required, and must be designed, operated and maintained correctly. This can be best addressed by auditing projects and facilities, and will reduce the user's total cost of ownership. It's better to have fewer, well-managed IPLs than numerous, non-managed IPLs." ■

Eprinted and posted with permission to Emerson Process Management from *Control*
November © 2014 PUTMAN