EDWARD MARSZAL

Kenexis
USA

- ➢ CEO of Kenexis, a technical safety consultancy
- ➢ Has over 25 years of experience in risk analysis and technical safety engineering
- ➢ Former Director of the ISA Safety Division and 20 year veteran of the ISA 84 standards committee for SIS

@emarszal

KENEXIS

Security PHA Review (SPR)

Speaker

- Edward M. Marszal, PE
- President and CEO, Kenexis
- 25 Years Industrial Experience
- Author – *Security PHA Review* and *Systematic SIL Selection*
- Member ISA 84 and former Director of ISA Safety Division
- BS Chemical Engineering, Ohio State University

● Representatives
● Coming Soon
● Kenexis Offices

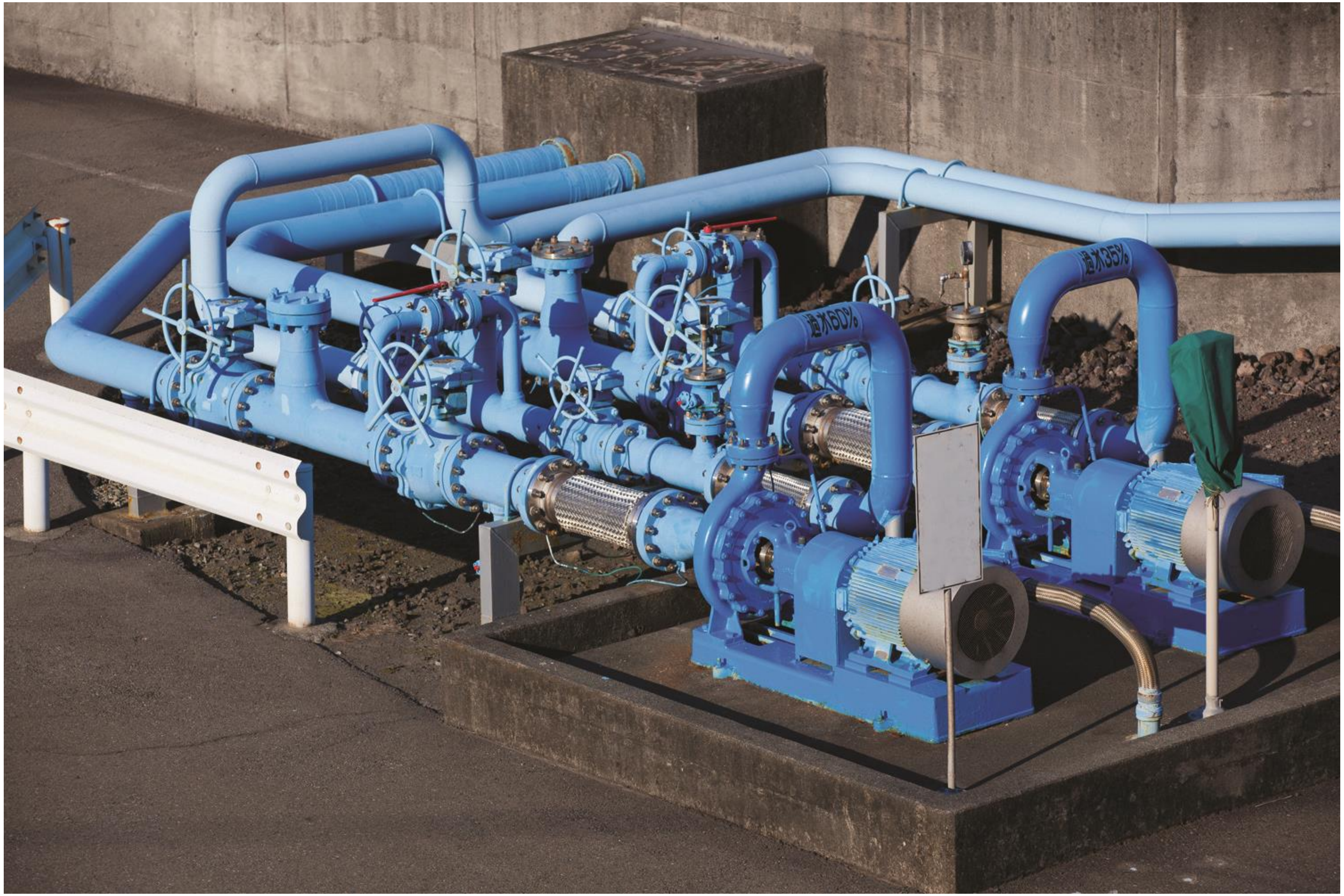
Deep Bench of Experienced Process Safety Engineers & ICS Experts
Analyzed over 1M Safety Instrumented Functions
Performed 1,000s of Process Hazards Analysis
Cybersecurity Assessments of 1,000s of ICS Networks

Introduction

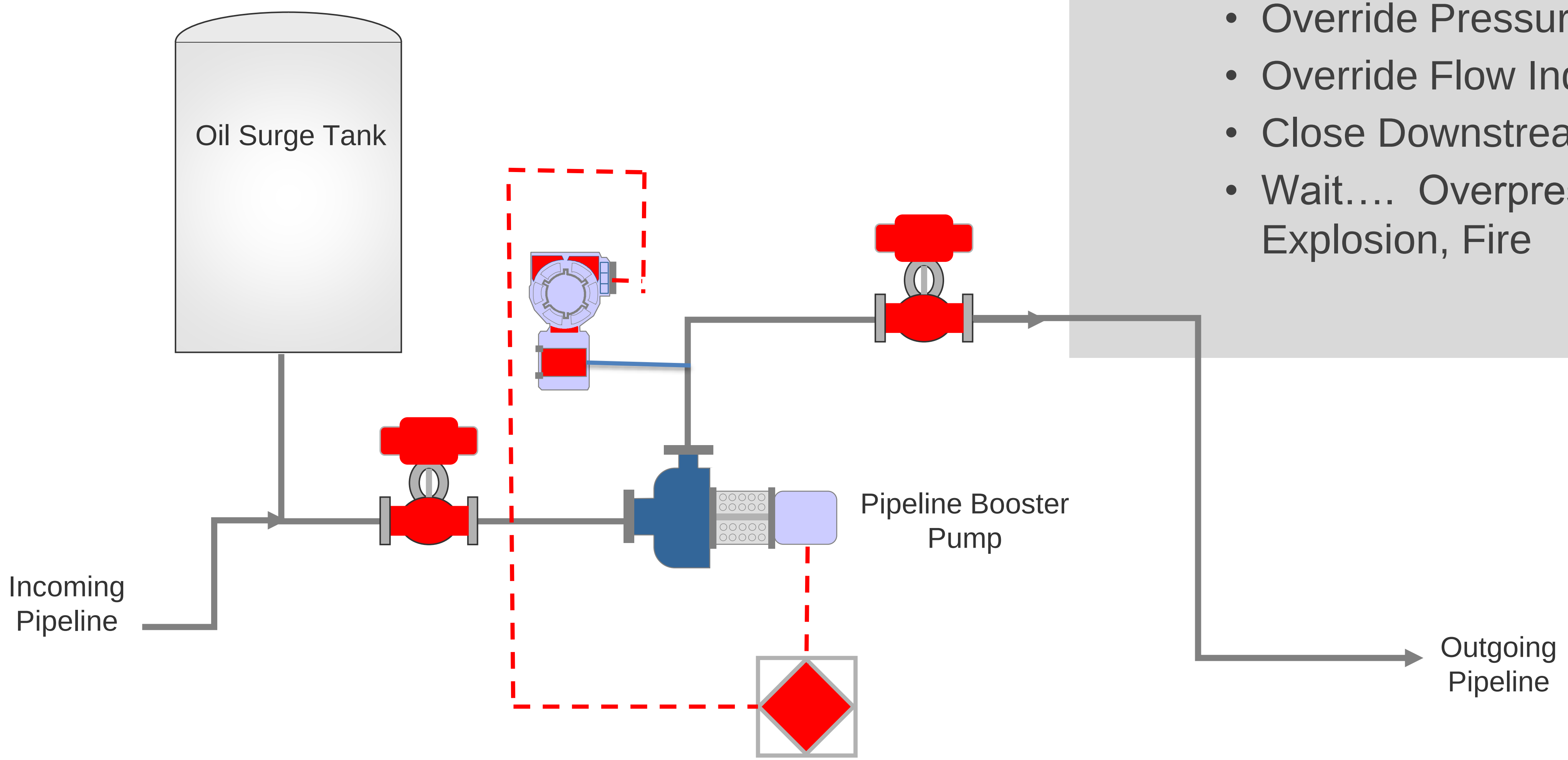
- Cybersecurity design should be based on the risk of the PROCESS
- Most cyber-related risk analysis focuses on ICS equipment
  - Poorly defined accident scenarios
  - Infinite potential outcomes
  - Lack of consideration of Inherent Safety
- Well designed plants do not need cybersecurity to prevent catastrophic loss of containment
- Use of Security PHA Review will identify PROCESS scenarios of cyber concern
  - Assign appropriate cybersafeguarding
  - Propose inherently safe against cyberattack safeguards

The current state of cybersecurity

Our Example – Oil Pipeline Pump Station

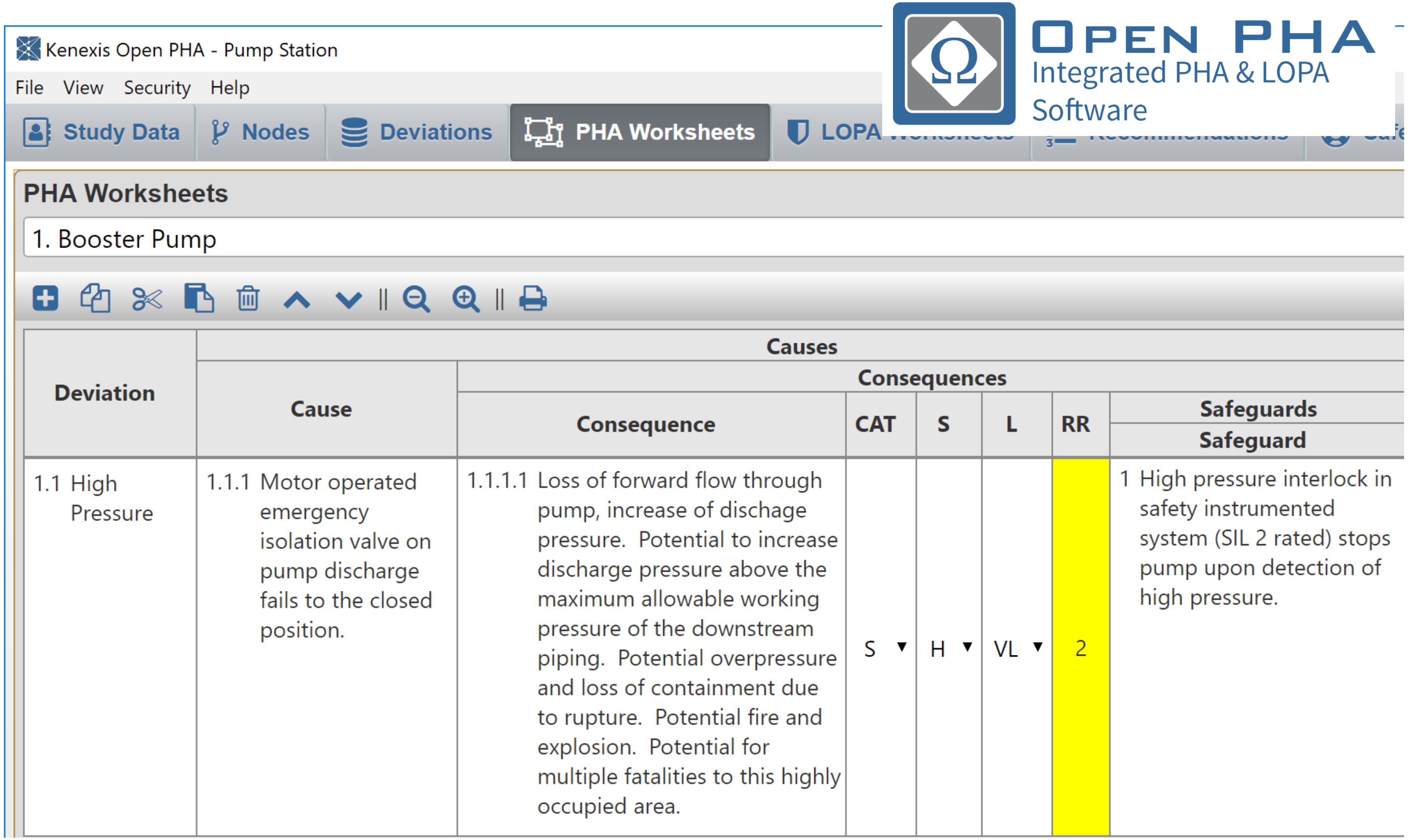


Pump Station Schematic - Original



- Scenario
  - Override High Pressure Shutdown
  - Override Pressure Indication/Alarm
  - Override Flow Indication Alarm
  - Close Downstream Isolation Valve
  - Wait…. Overpressure, Rupture, Explosion, Fire

Process Risk Assessment - HAZOP



OPEN PHA
Integrated PHA & LOPA Software

PHA Worksheets

1. Booster Pump

	Causes						
		Consequences					
							Safeguards
Deviation	Cause	Consequence	CAT	S	L	RR	Safeguard
1.1 High Pressure	1.1.1 Motor operated emergency isolation valve on pump discharge fails to the closed position.	1.1.1.1 Loss of forward flow through pump, increase of dischage pressure. Potential to increase discharge pressure above the maximum allowable working pressure of the downstream piping. Potential overpressure and loss of containment due to rupture. Potential fire and explosion. Potential for multiple fatalities to this highly occupied area.	S ▾	H ▾	VL ▾	2	1 High pressure interlock in safety instrumented system (SIL 2 rated) stops pump upon detection of high pressure.

- Process Hazards Analysis
- ~50 years old
- HAZOP is the most common method
- Facility is broken down into Nodes and every deviation like High Pressure, Low Temperature, Reverse Flow is considered
- If safeguards are inadequate, recommendations are made

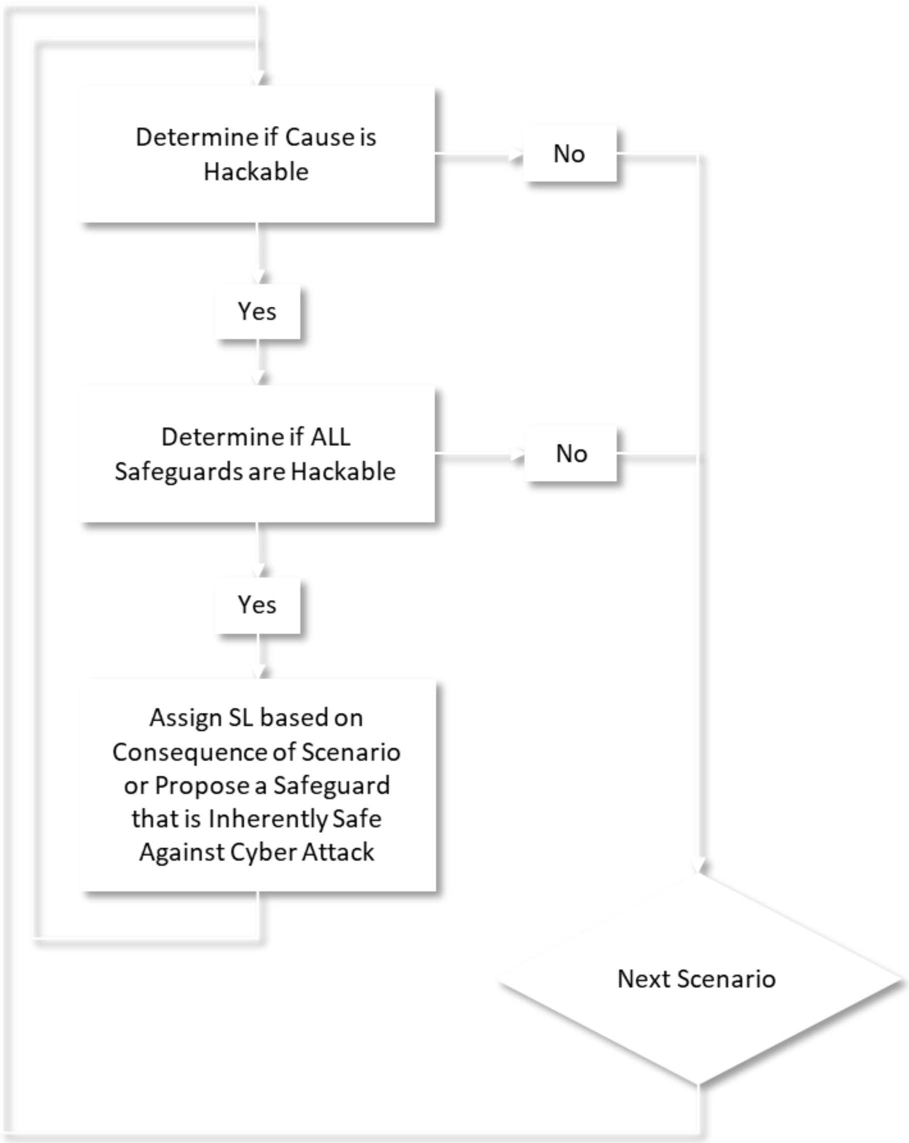
Considers Random Hardware Failures – SPR Modifies for Deliberate

Security PHA Review

- Designed to either generate the cybersecurity performance targets for a zone or specify the recommendations for inherently cyber-secure layers of protection
- Developed by technical safety practitioners with a strong background in industrial controls implementation and cybersecurity
- Designed to fit with existing project life cycles of design, implementation, and operation of process plants while leveraging existing engineering tasks and reports generated for process safety
- Makes SL-T (ISA/IEC62443) selection similar to LOPA for SIL selection targets for SIF

Security PHA Review Flow

- Can be done after a PHA, or as a step during we check each SCENARIO
  - Is the initiating event hackable
  - Microprocessors are hackable
  - Control loops, SIS functions, operator interface actions are all micro-based
  - Human operation manually opening a valve are not hackable yet
  - Mechanical safety devices like pressure relief valves are not hackable
- If all layers are hackable
  - Assign Security Level (SL) or recommend inherently safe device



Determine if Cause is Hackable

No

Yes

Determine if ALL Safeguards are Hackable

No

Yes

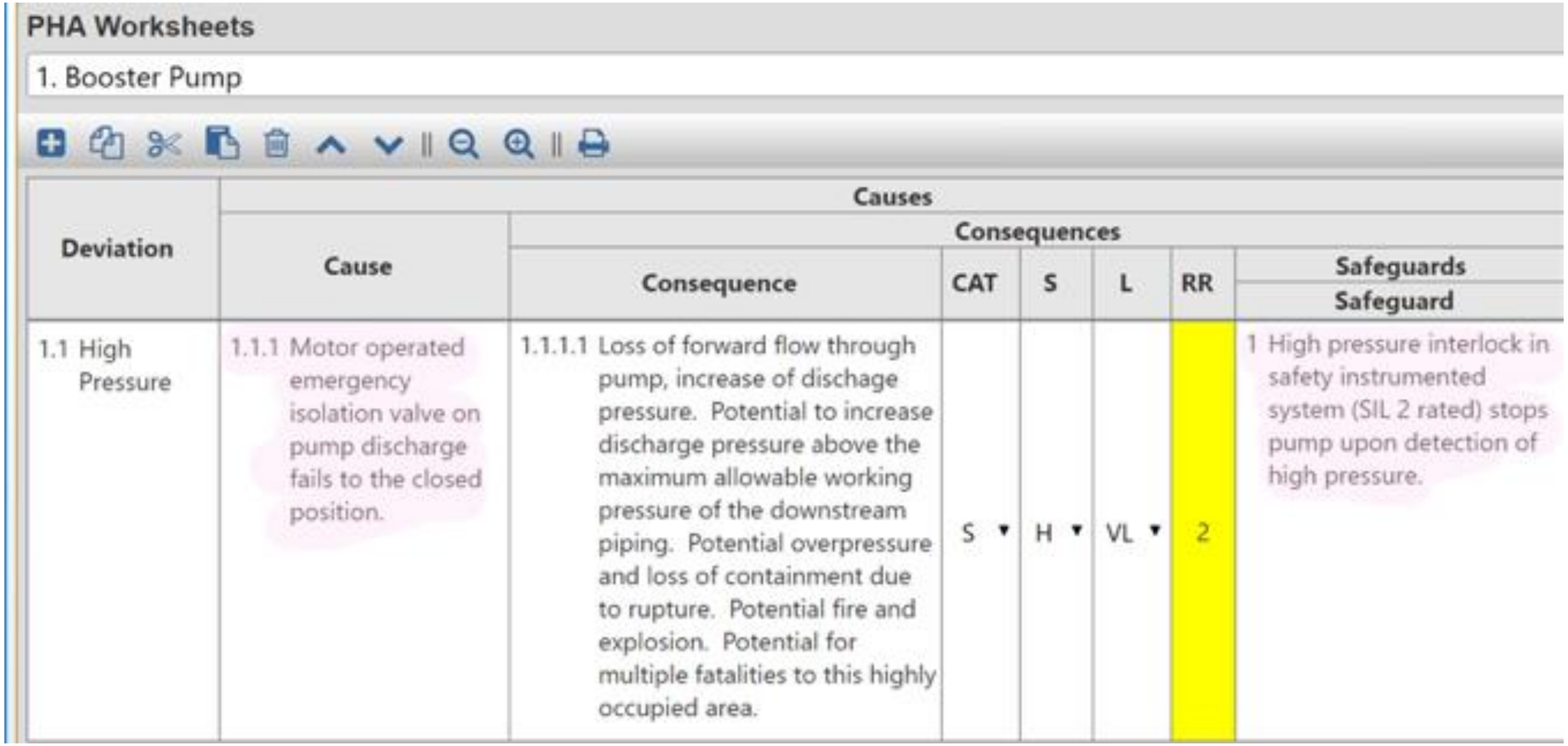
Assign SL based on Consequence of Scenario or Propose a Safeguard that is Inherently Safe Against Cyber Attack

Next Scenario

SPR of Overpressure Scenario

OPEN PHA
Integrated PHA & LOPA Software

- Scenario is Determined to be Hackable
  - Cause is Hackable
  - All Safeguards are Hackable



PHA Worksheets

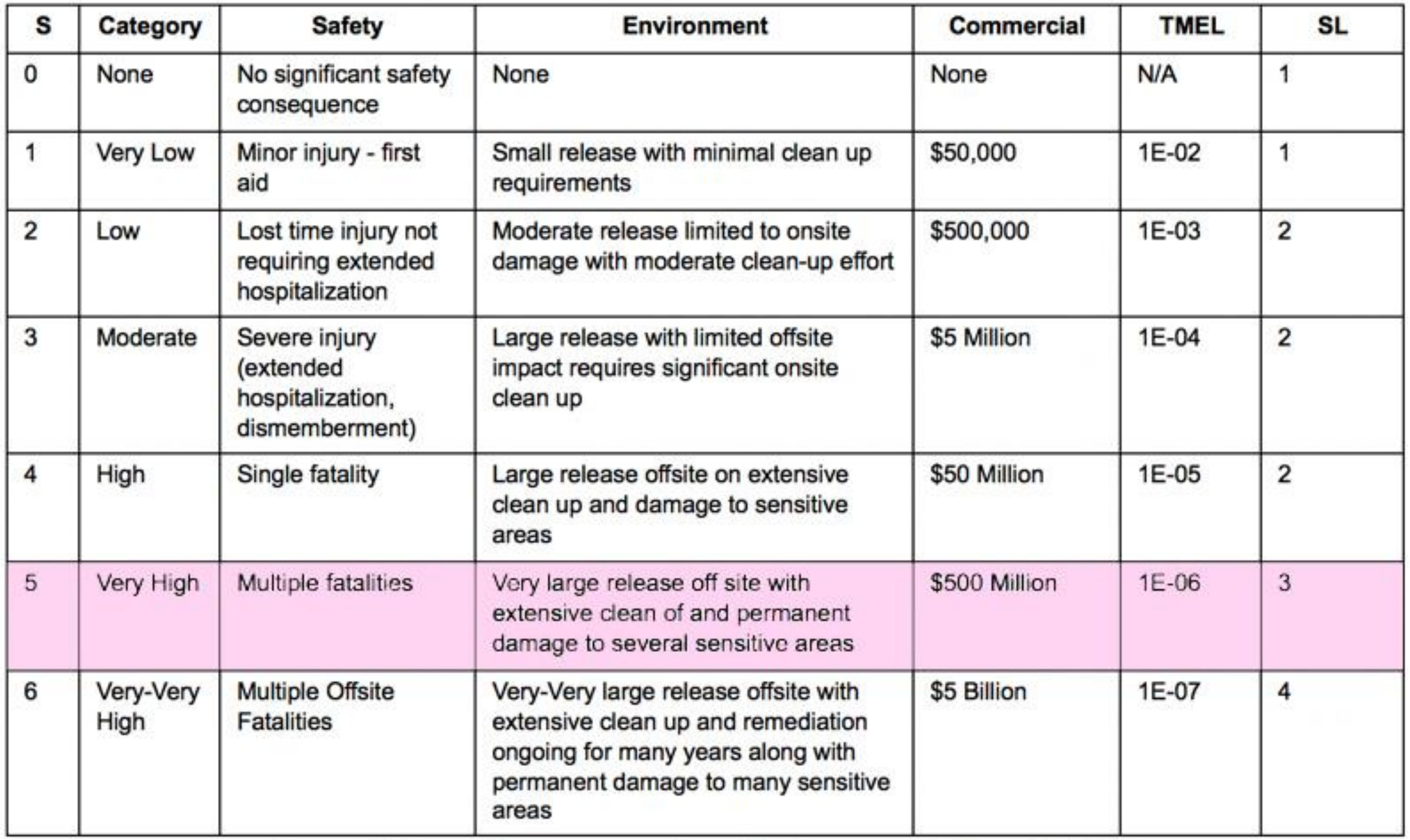
1. Booster Pump

Deviation	Causes						
		Consequences					
	Cause	Consequence	CAT	S	L	RR	Safeguards
							Safeguard
1.1 High Pressure	1.1.1 Motor operated emergency isolation valve on pump discharge fails to the closed position.	1.1.1.1 Loss of forward flow through pump, increase of dischage pressure. Potential to increase discharge pressure above the maximum allowable working pressure of the downstream piping. Potential overpressure and loss of containment due to rupture. Potential fire and explosion. Potential for multiple fatalities to this highly occupied area.	S	H	VL	2	1 High pressure interlock in safety instrumented system (SIL 2 rated) stops pump upon detection of high pressure.

KENEXIS
All Rights Reserved 2017

Address Hackability with Security Level

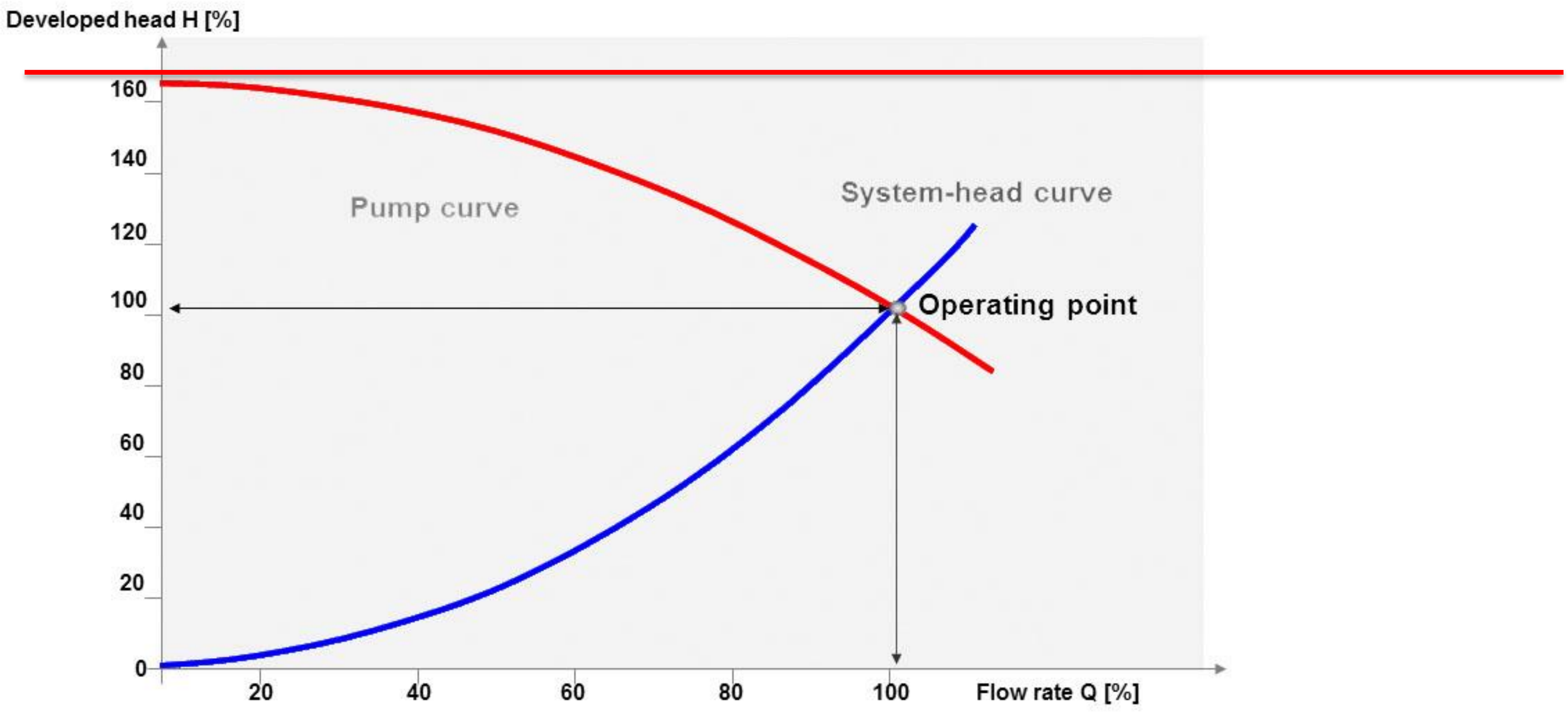
- When a scenario is hackable, risk could be addressed by appropriate level of cyber-safeguarding
  - Function of consequence
  - Consequence category determines SL
  - Organizational risk criteria must be define
- In this example, SL 3 could be selected



S	Category	Safety	Environment	Commercial	TMEL	SL
0	None	No significant safety consequence	None	None	N/A	1
1	Very Low	Minor injury - first aid	Small release with minimal clean up requirements	$50,000	1E-02	1
2	Low	Lost time injury not requiring extended hospitalization	Moderate release limited to onsite damage with moderate clean-up effort	$500,000	1E-03	2
3	Moderate	Severe injury (extended hospitalization, dismemberment)	Large release with limited offsite impact requires significant onsite clean up	$5 Million	1E-04	2
4	High	Single fatality	Large release offsite on extensive clean up and damage to sensitive areas	$50 Million	1E-05	2
5	Very High	Multiple fatalities	Very large release off site with extensive clean of and permanent damage to several sensitive areas	$500 Million	1E-06	3
6	Very-Very High	Multiple Offsite Fatalities	Very-Very large release offsite with extensive clean up and remediation ongoing for many years along with permanent damage to many sensitive areas	$5 Billion	1E-07	4

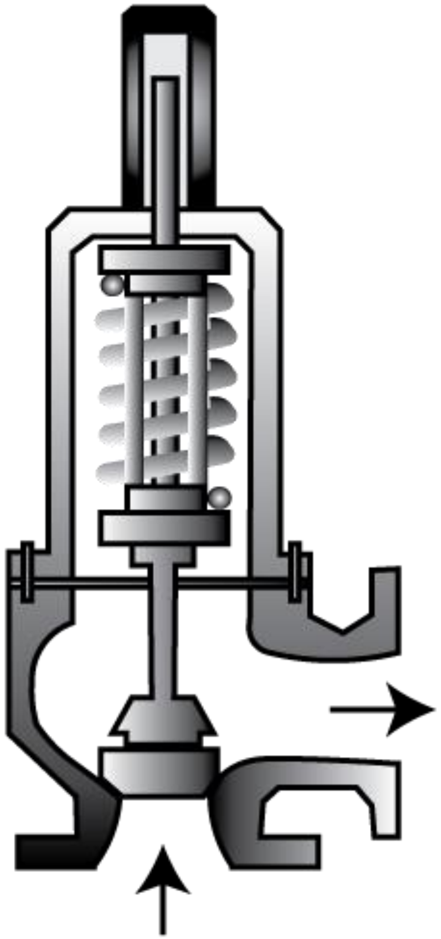
Propose Non-Hackable Safeguards – Inherent Safety

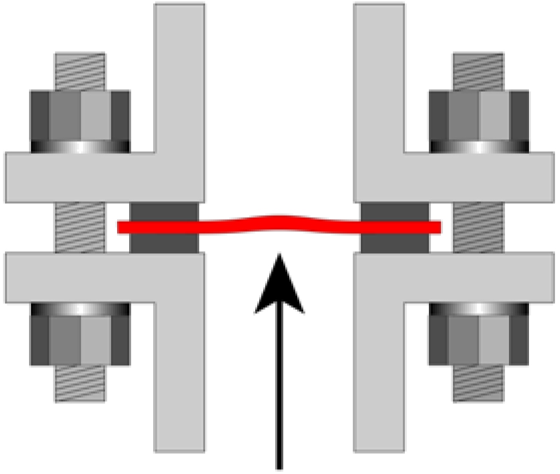
- Install piping that is rated to withstand a higher pressure than the pump is capable of developing

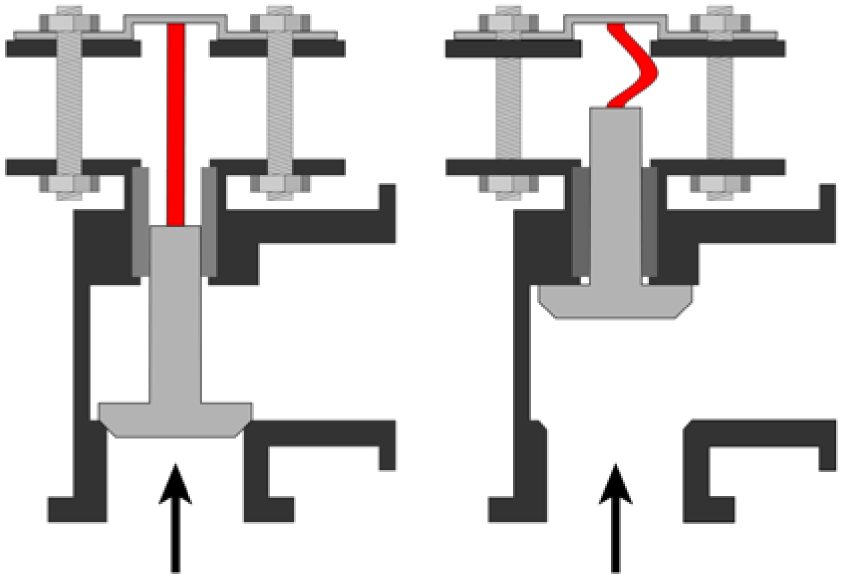


Non-Hackable Safeguards – Pressure Relief/Spillback

- Relieves excess pressure by creating pathway back to inlet or other safe vent location

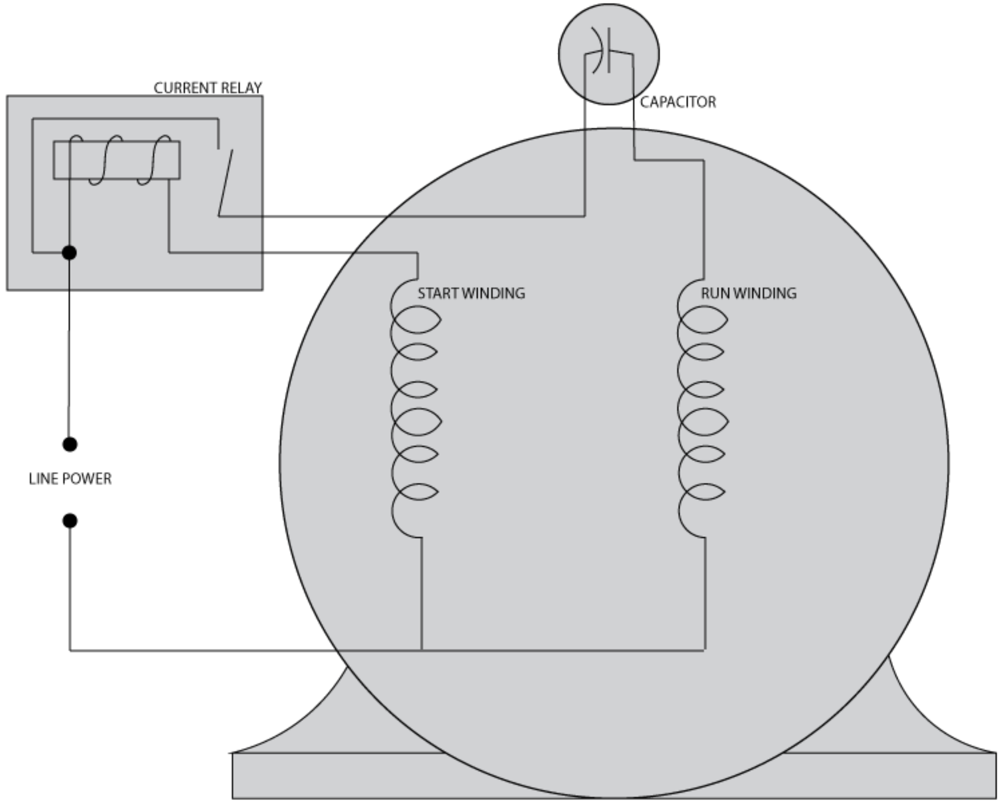






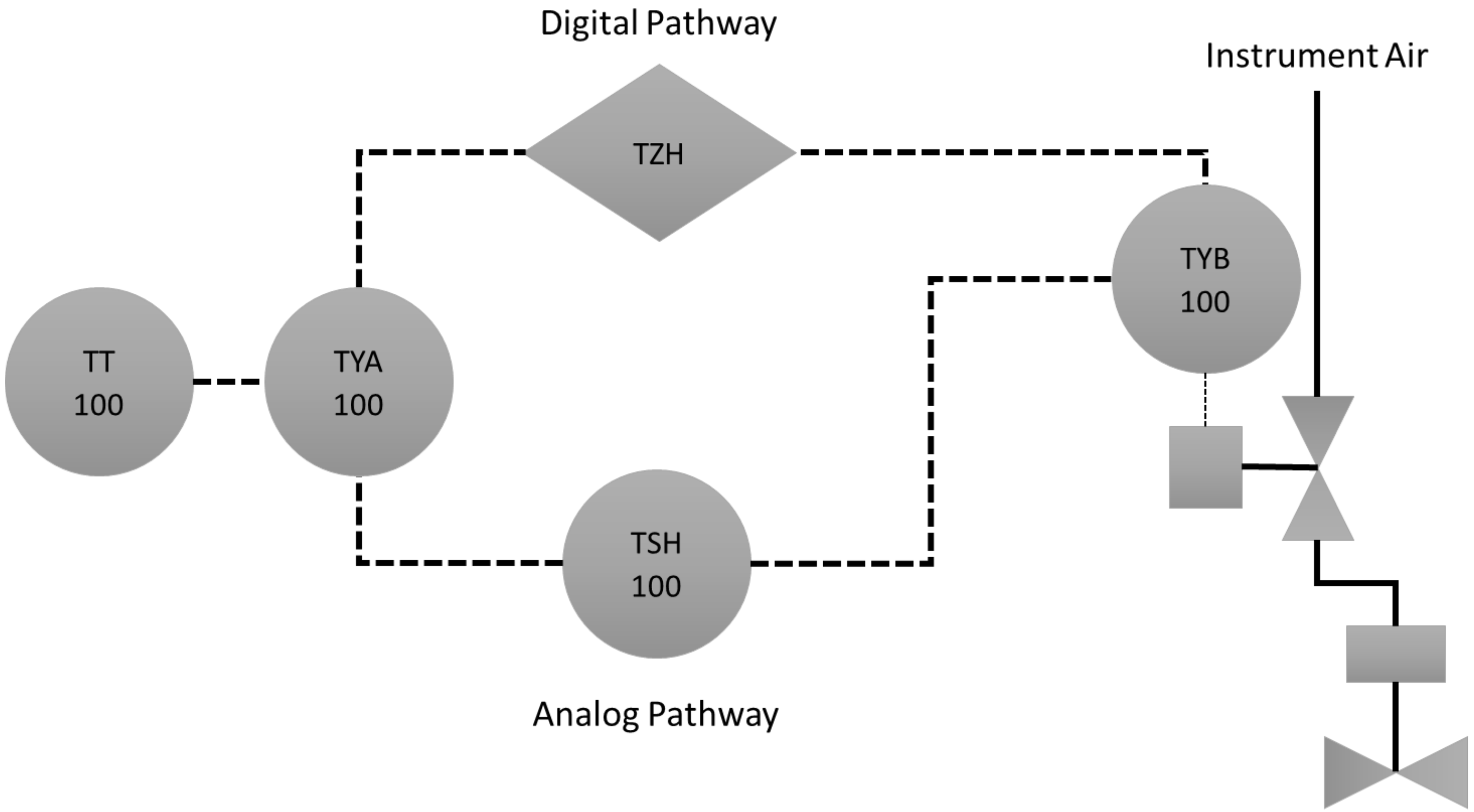
Non-Hackable Safeguards – Motor Overload Relay

- Detects excessive/insufficient current in pump motor coil windings and disconnects power to motor



Non-Hackable Safeguards – Analog SIF Mimic

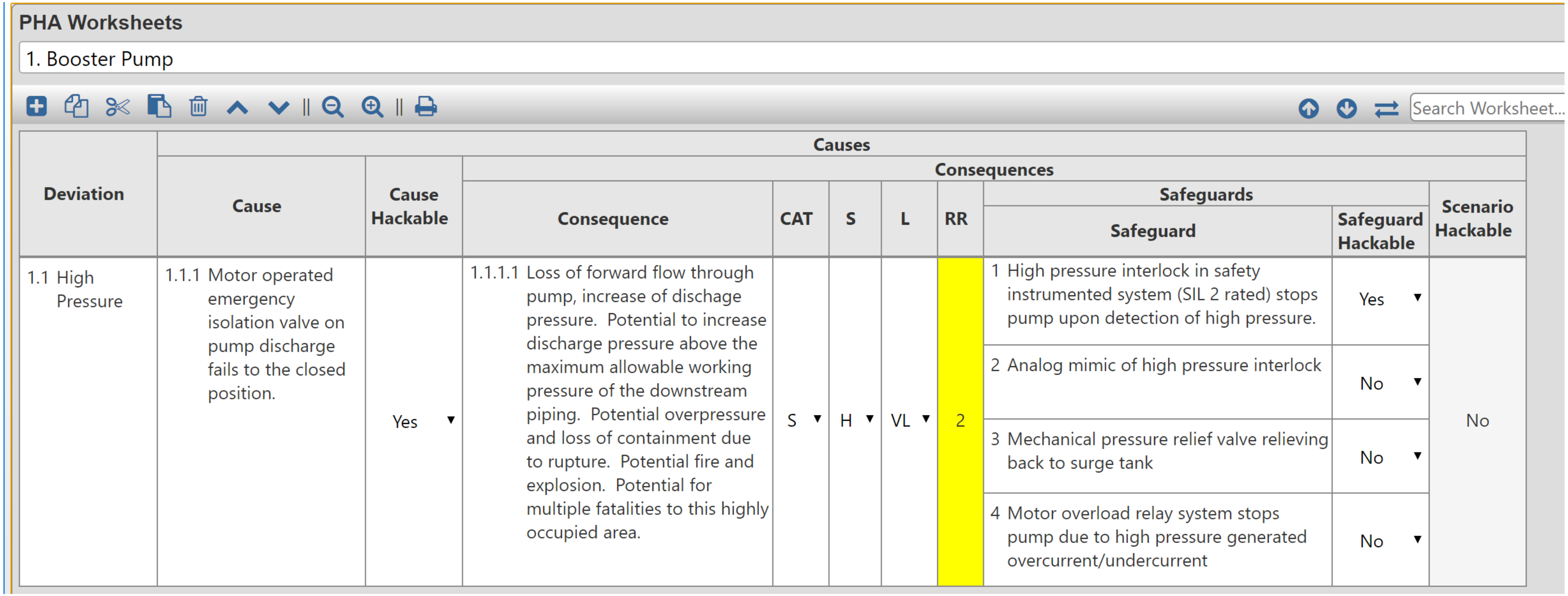
- Perform the same action as the computer based (hackable) SIF with analog electronics – analog transmitter, current monitor relay, solenoid valve



SPR of Revised Overpressure Scenario

OPEN PHA
Integrated PHA & LOPA Software

- Scenario is Determined to be Non-Hackable



PHA Worksheets

1. Booster Pump

Deviation	Causes									
			Consequences							
								Safeguards		
	Cause	Cause Hackable	Consequence	CAT	S	L	RR	Safeguard	Safeguard Hackable	Scenario Hackable
1.1 High Pressure	1.1.1 Motor operated emergency isolation valve on pump discharge fails to the closed position.	Yes ▾	1.1.1.1 Loss of forward flow through pump, increase of dischage pressure. Potential to increase discharge pressure above the maximum allowable working pressure of the downstream piping. Potential overpressure and loss of containment due to rupture. Potential fire and explosion. Potential for multiple fatalities to this highly occupied area.	S ▾	H ▾	VL ▾	2	1 High pressure interlock in safety instrumented system (SIL 2 rated) stops pump upon detection of high pressure.	Yes ▾	No
								2 Analog mimic of high pressure interlock	No ▾	
								3 Mechanical pressure relief valve relieving back to surge tank	No ▾	
								4 Motor overload relay system stops pump due to high pressure generated overcurrent/undercurrent	No ▾	

KENEXIS

Security PHA Review Benefits

- Lower risk to tolerable level based on lowering consequence of event
- Better understanding of attack vectors
- Make the right choices for the design you have
- Increased efficiency by extending existing studies
- Standards compliance by building on recognized and generally accepted good engineering practices

- ISA Book and Training – “Security PHA Review” Coming Soon!!!