CE 400 / CE 500

Process Safety Management

Lecture 31

Layer of Protection Analysis

Part IV - Safety Instrumented Functions

Instructor: David Courtemanche

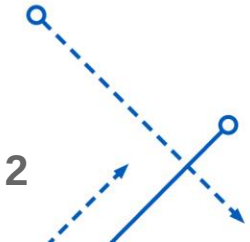
University at Buffalo
Department of Chemical and Biological Engineering
School of Engineering and Applied Sciences

SIF SIL

Safety Instrumented Function (i.e. an Interlock) Safety Integrity Level

- SIL Levels:
  - SIL 1 is an interlock designed to have a PFD of 0.1 or less
  - SIL 2 is an interlock designed to have a PFD of 0.01 or less
  - SIL 3 is an interlock designed to have a PFD of 0.001 or less

- One must analyze the SIF components and design and calculate the PFD in order to determine what SIL it meets



How to Determine SIL of a SIF*

- Devices will often be listed as having a certain SIL rating
  - SIL 2 level probe
- You need to actually calculate the PFD for the actual SIF
- A Safety Instrumented Function typically has 3 elements
  - Sensor – detects the irregular condition
  - Logic Solver – takes the information from the sensor and determines what action to take
    - Some interlocks can be “hard wired” – the signal from the sensor directly opens or shuts electronic circuits
  - Final Element(s)
    - Valves, pumps, etc
- If the logic solver is the BPCS you cannot claim a PFD less than 0.1

* Interlocks and LOPA are a particularly acronym laden discipline

PFD of SIF

- In order for the Safety Instrumented Function to provide protection, it must perform successfully at all three elements
- Therefore the Sensing, Logic Controller, and Final Element steps behave with Series Interaction
- Because the three elements should each have a very low probability of failure the overall PFD can be expressed as:

$$PFD_{SIF} = \sum_{i=1}^{n} PFD_i = PFD_{Sensor} + PFD_{Logic} + PFD_{final\ elements}$$

- Where PFD_i is the PFD for each element i

PFD of SIF

$$PFD_{SIF} = PFD_{Sensor} + PFD_{Logic} + PFD_{final\ elements}$$

- In the case where:

$$PFD_{Sensor} = 0.1$$
$$PFD_{Logic} = 0.001$$
$$PFD_{final\ elements} = 0.01$$

- It would be understandable to state:

$$PFD_{SIF} = 0.1 + 0.001 + 0.01 = 0.111$$

- But that assumes too much precision in the PFD_{Sensor} value, so the better value to use is:

$$PFD_{SIF} = 0.1$$

How to improve PFD of a SIF

- One can specify individual components with lower individual PFD
- Redundancy, Redundancy, Redundancy
  - See what I did there?
- Testing Interval can be used to reduce PFD for the SIF
  - From Lecture 25:

$$U = \frac{\tau_u}{\tau_i} = \frac{1}{2}\mu\tau_i$$

  - U is the proportion of the time that the SIF is unavailable to protect
  - τ_i is the testing interval, μ is the failure rate
  - The individual PFD of the components are reported with a certain testing period prescribed
    - You can reduce the PFD by testing more frequently
    - Testing is a pain, so you don't want to just "test in" reliability if you can avoid it

SIL Data

- Data may also be reported in terms of failure rates
  - Here is a site I found: http://silsafedata.com/
- Some Data from this site:

- Rates in FITs – 1 Failure per billion hours – DU stands for Dangerous Undetected Failure Rate

Category	Type	DU Lower Bound	DU Upper Bound
Level Transmitter	Analog/Smart	60	250
Level Transmitter	Safety Certified	40	150
Actuator	Pneumatic	120	700
Valve	Ball Valve	300	900
Main Processor	BPCS	500	2000
Main Processor	Safety PLC	0	300

Component PFD

- $PFD = 1 - e^{-\mu\tau_i}$
- Example – Analog level transmitter
  - $\tau_i = 1\ yr = 8760\ hr$

$$PFD = 1 - e^{-\mu\tau_i} = 1 - e^{-\frac{200}{10^9 hr} * 8760\ hr} = 0.00175$$

Category	Type	DU from manufacturer	PFD 1 yr test
Level Transmitter	Analog/Smart	200	0.002
Level Transmitter	Safety Certified	50	0.0005
Actuator	Pneumatic	500	0.006
Valve	Ball Valve	500	0.006
Main Processor	BPCS	1000	0.008
Main Processor	Safety PLC	200	0.002

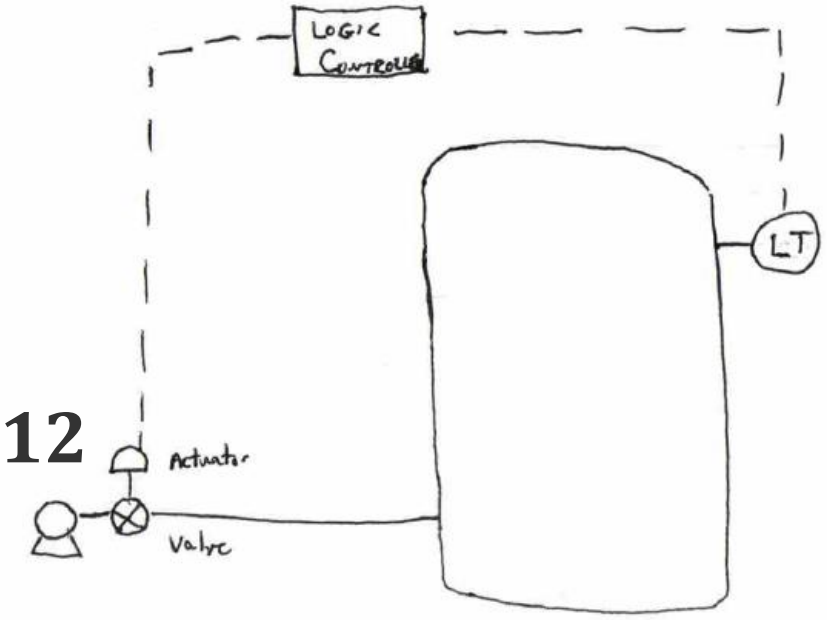
SIL Simplified Example

We are leaving out some intermediate components

Primary control – differential pressure level measurement shuts off the pump via BPCS

$$PFD_{SIF} = PFD_{Sensor} + PFD_{Logic} + PFD_{final\ elements}$$

- Analog Level Transmitter: $PFD_{Sensor} = 0.002$
- BPCS: $PFD_{Logic} = 0.008$
- Actuated Valve
  - Actuator and Valve act in Series
  - $PFD_{final\ elements} = 0.006 + 0.006 = 0.012$



- $PFD_{SIF} = 0.002 + 0.008 + 0.012 = 0.022$
- **SIL 1** – Note that really you **CANNOT** claim a "Safety Interlock" that uses the BPCS

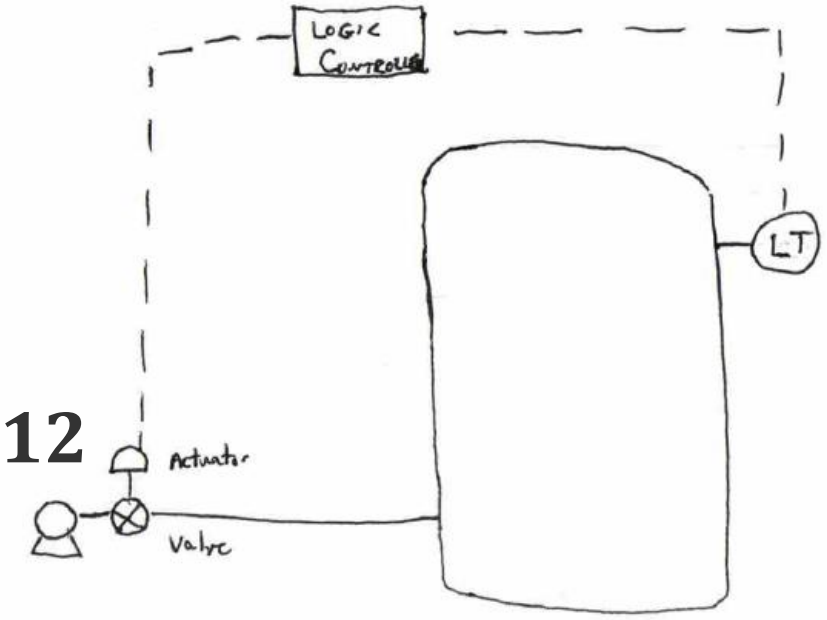
SIL Simplified Example

We are leaving out some intermediate components

Primary control – differential pressure level measurement shuts off the pump via BPCS

$$PFD_{SIF} = PFD_{Sensor} + PFD_{Logic} + PFD_{final\ elements}$$

- Safety Level Transmitter: $PFD_{Sensor} = 0.0005$
- SIS: $PFD_{Logic} = 0.002$
- Actuated Valve
  - Actuator and Valve act in Series
  - $PFD_{final\ elements} = 0.006 + 0.006 = 0.012$



- $PFD_{SIF} = 0.0005 + 0.002 + 0.012 = 0.015$
- **SIL 1 and can be considered a "Safety Interlock"**

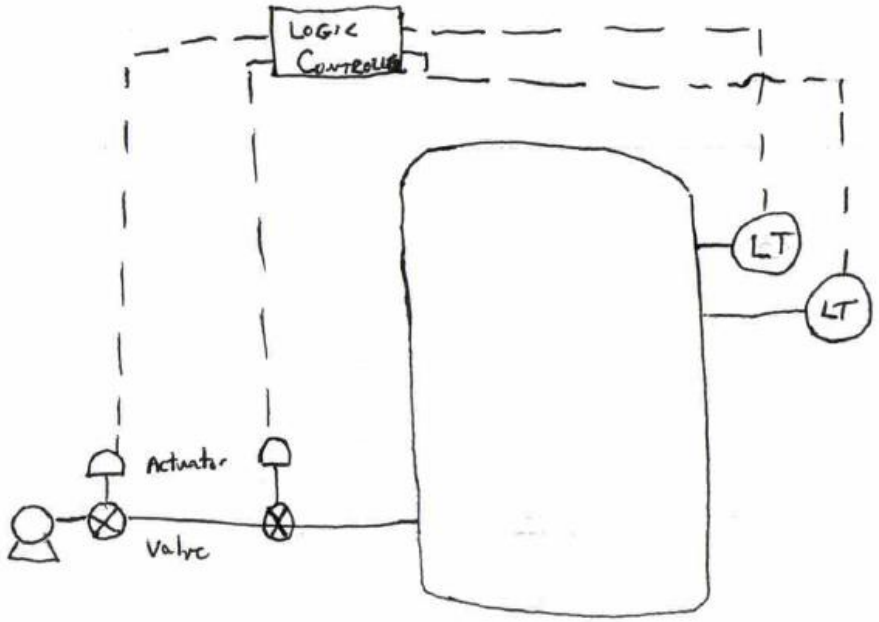
SIL Simplified Example

We are leaving out some intermediate components

Primary control – differential pressure level measurement shuts off the pump via BPCS

$$PFD_{SIF} = PFD_{Sensor} + PFD_{Logic} + PFD_{final\ elements}$$

- 2 Safety Level Transmitters in Parallel : $PFD_{Sensor} = 0.0005 * 0.0005 = 0.00000025$
- SIS: $PFD_{Logic} = 0.002$
- Actuated Valve
  - Actuator and Valve act in Series, both sets work in parallel
  - $PFD_{one\ set} = 0.006 + 0.006 = 0.012$
  - $PFD_{final\ elements} = 0.012 * 0.012 = 0.00014$



- $PFD_{SIF} = 0.00000025 + 0.002 + 0.00014 = 0.002$
- **SIL 2 – Safety Interlock**
  - Question – Did we need the redundant level transmitters to reach SIL 2?
  - Question – Could we have used redundant analog level transmitters?

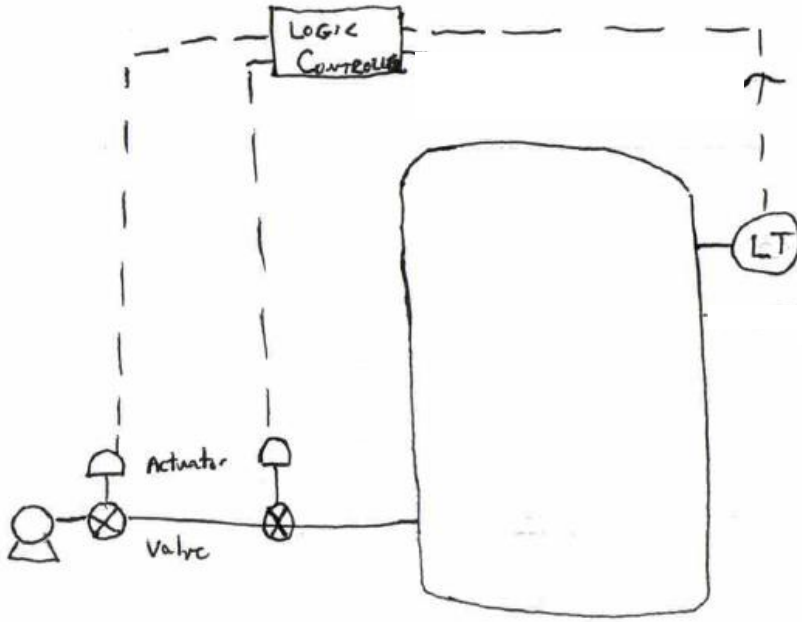
SIL Simplified Example

Primary control – differential pressure level measurement shuts off the pump via BPCS

We are leaving out some intermediate components

$$PFD_{SIF} = PFD_{Sensor} + PFD_{Logic} + PFD_{final\ elements}$$

- 1 Safety Level Transmitter : $PFD_{Sensor} = 0.0005$
- SIS: $PFD_{Logic} = 0.002$
- Actuated Valve
  - Actuator and Valve act in Series, both sets work in parallel
  - $PFD_{one\ set} = 0.006 + 0.006 = 0.012$
  - $PFD_{final\ elements} = 0.012 * 0.012 = 0.00014$



- $PFD_{SIF} = 0.0005 + 0.002 + 0.00014 = 0.003$
- **SIL 2 – Safety Interlock**

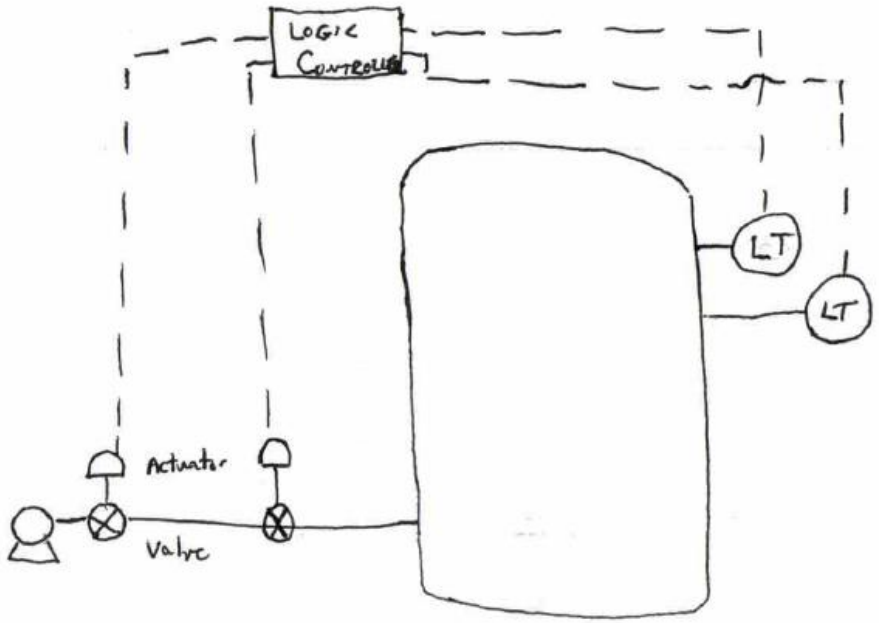
SIL Simplified Example

We are leaving out some intermediate components

Primary control – differential pressure level measurement shuts off the pump via BPCS

$$PFD_{SIF} = PFD_{Sensor} + PFD_{Logic} + PFD_{final\ elements}$$

- 2 Analog Level Transmitters in Parallel: $PFD_{Sensor} = 0.002 * 0.002 = 0.000004$
- SIS: $PFD_{Logic} = 0.002$
- Actuated Valve
  - Actuator and Valve act in Series, both sets work in parallel
  - $PFD_{one\ set} = 0.006 + 0.006 = 0.012$
  - $PFD_{final\ elements} = 0.012 * 0.012 = 0.00014$



- $PFD_{SIF} = 0.000004 + 0.002 + 0.00014 = 0.002$
- **SIL 2 – Safety Interlock**

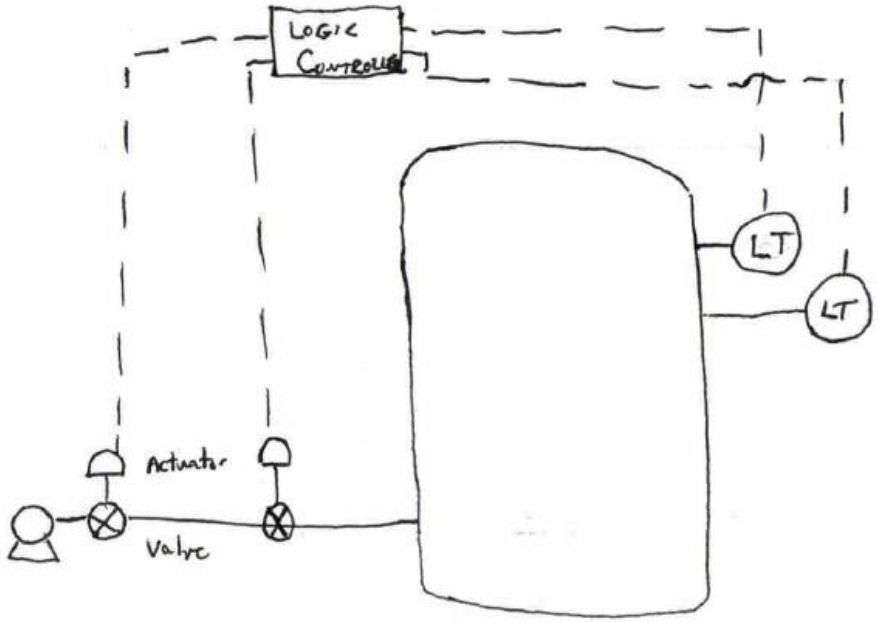
SIL Simplified Example

We are leaving out some intermediate components

Primary control – differential pressure level measurement shuts off the pump via BPCS

$$PFD_{SIF} = PFD_{Sensor} + PFD_{Logic} + PFD_{final\ elements}$$

- 1 Analog Level Transmitter: $PFD_{Sensor} = 0.002$
- SIS: $PFD_{Logic} = 0.002$
- Actuated Valve
  - Actuator and Valve act in Series, both sets work in parallel
  - $PFD_{one\ set} = 0.006 + 0.006 = 0.012$
  - $PFD_{final\ elements} = 0.012 * 0.012 = 0.00014$

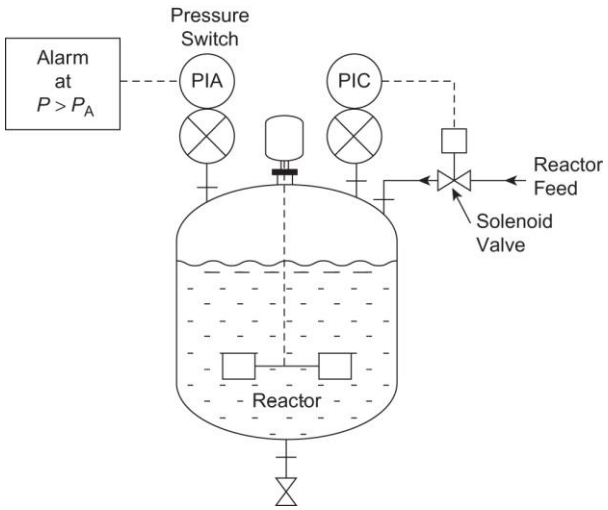


- $PFD_{SIF} = 0.002 + 0.002 + 0.00014 = 0.004$
- **SIL 2 – Safety Interlock**

SIL Example Observations

- In order to be a Safety Interlock we cannot use the BPCS or any of the elements used in the primary control
- Redundancy is most impactful when applied to the weakest link (i.e. highest PFD) in the chain
- There is more to it than just the SIL, as you can see we had several designs that met SIL 2, but they had PFDs ranging from 0.002 to 0.004
- You can also look for components with lower DU (Dangerous Uprotected Failure Rates)
- In extreme cases you can run 2 SIS to achieve two independent parallel SIF

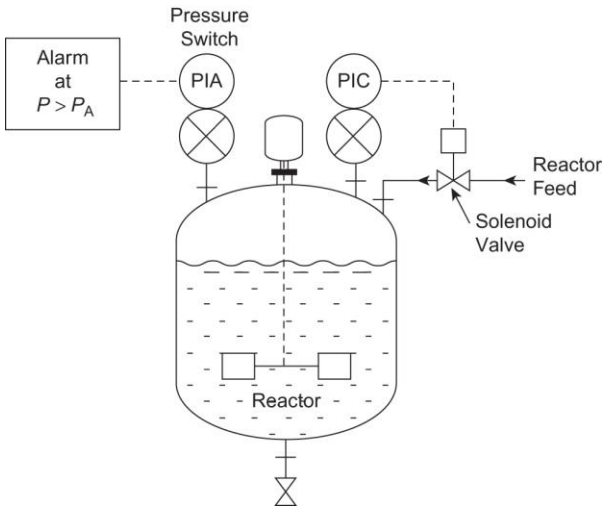
LOPA / PFD / SIL Example



- Reactor Example from Lecture 17
- Initiating Event: Operator accidently makes up reactor feed batch with double initiator concentration
  - Batches last 8 hours, therefore 3 batches per day or 1095 batches per year
  - Probability of error per operation
    - Range from literature - 10^{-1} to 10^{-3} per opportunity
    - Team estimates a value of 10^{-2}
  - Initiating Event Frequency is therefore 11 double batches per year

LOPA / PFD / SIL Example

- PHA team has determined that the overpressure situation will lead to a fatality
- Company guidelines determine that the acceptable frequency of a fatality is 1 per 10,000 years
- Campaign Risk – products that are at risk for run-away reaction account for 20% of the production time
- Conditional Modifier – Reactor is in a room with a blowout panel that can direct pressure away from control room. Personnel are only in the room 10% of the time during the at-risk campaigns



Existing Safety System

- Alarms
  - The pressure switch and alarm light must both work in series
  - Operator Response is also in series, assume R = 0.75
  - The reliability of the alarm is given by $\boldsymbol{R = \prod_{i=1}^{n} R_i = 0.87 * 0.96 * 0.75 = 0.626}$
  - The failure probability is $\boldsymbol{P_1 = 1 - R = 1 - 0.626 = 0.374}$.
- BPCS Emergency Shutoff System
  - The pressure switch and solenoid valve must both work in series
  - The reliability of this control system is given by $\boldsymbol{R = \prod_{i=1}^{n} R_i = 0.87 * 0.66 = 0.574}$
  - The failure probability is $\boldsymbol{P_2 = 1 - R = 1 - 0.574 = 0.426}$.

The LOPA

- Enter in the Values from the previous pages

LOPA #	Impact Event Description	Severity Level	Initiating Cause	Initiating Frequency	General Process Design	BPCS	Alarms, etc	Campaign Risk	Conditional Modifier	Existing SIF PFD	Event Likelihood	Target Likelihood	Required SIF SIL
1	Double Batch leads to Runaway causing overpressure leading to fatality	C4	Double Strength Feed Batch	11	1	0.426	0.374	0.2	0.1	1	0.0350513	1.00E-04	2.85E-03

- We see that we need to add a SIF with a PFD level of 0.003 or lower
- This will be a **SIL of 2**
- From previous slides if we had a new SIF with a dedicated pressure switch that had similar performance as the safety level transmitter and used a SIS controller to shut off 2 additional actuated valves in series we would meet the desired risk level

LOPA Documentation

- LOPA Documentation is a database of the following:
  - Description of the scenario
    - Initiating event and it's frequency
    - Loss Event
    - Impact of Loss Event
  - Risk Target
  - Factors in Risk Equation
    - Enabling Factors, Conditional Modifiers
  - Calculation of Risk
    - As shown on previous slide
  - Determination of whether Risk Tolerance met
  - Documentation of Action Required
    - e.g. "Install SIL 2 Safety Interlock with a PFD of 0.0025 or lower"
    - Do NOT specify the SIF

SIF Documentation

- LOPA Documentation is a database of the following:
  - Description of the SIF and how it works
  - List of components and their PFDs or DU
  - Calculation of SIF PFD
  - SIL rating
  - Testing Frequency Required and Testing Procedure
  - Documentation of test results and any corrective actions required
    - “As Found” and “As Left”