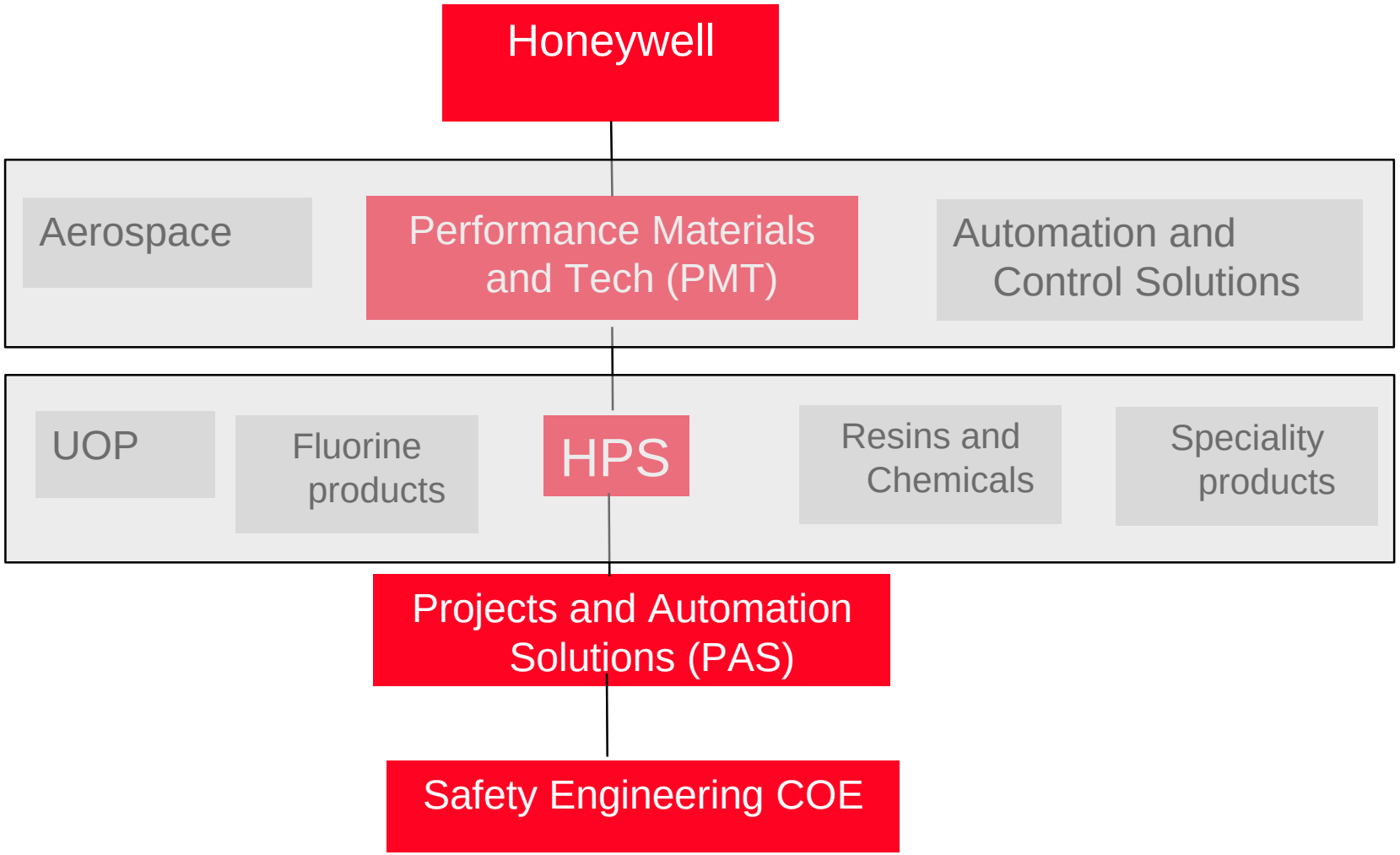
Prasad Goteti

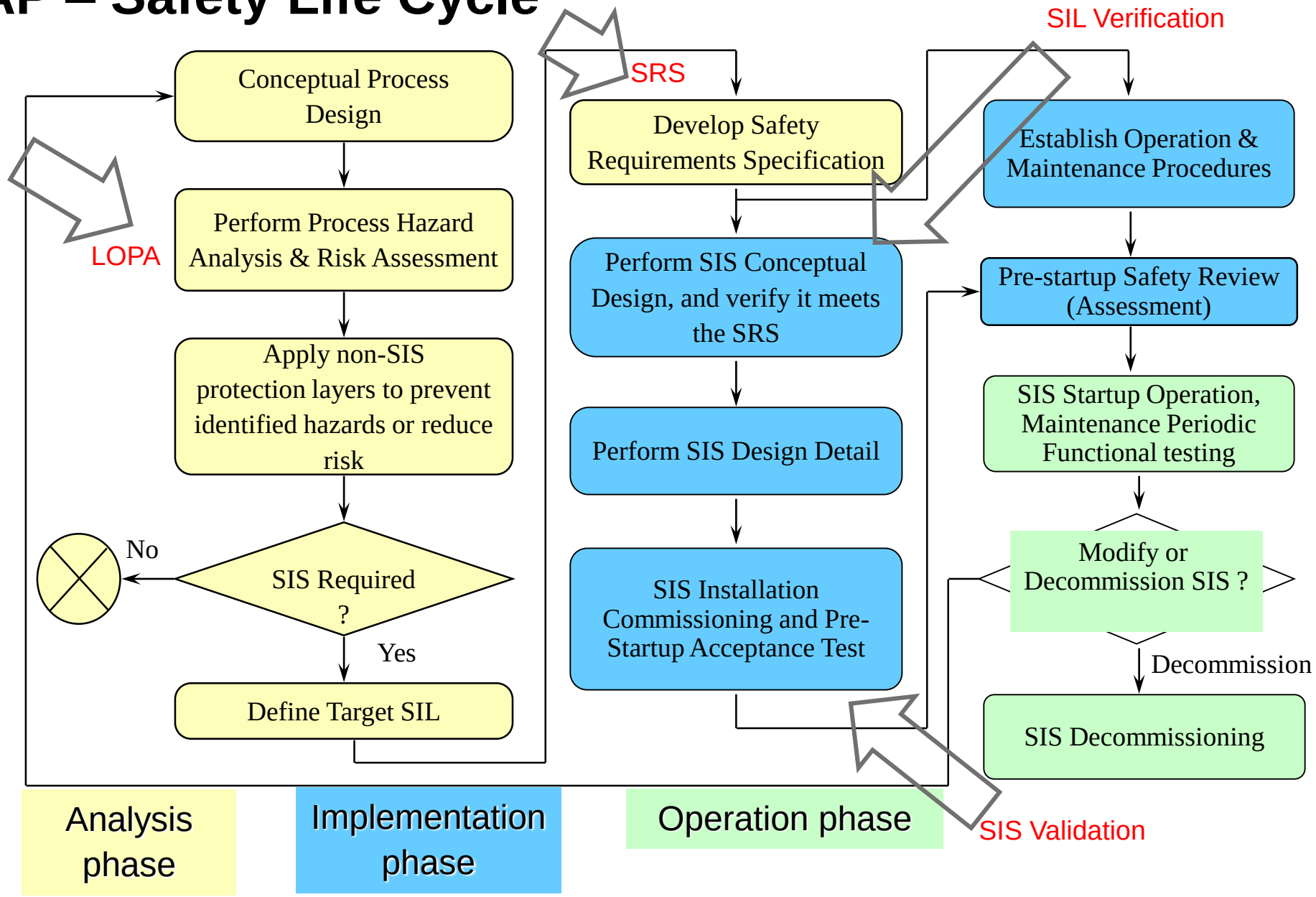
May 10, 2018

PROOF TESTING SAFETY INSTRUMENTED SYSTEMS

Honeywell

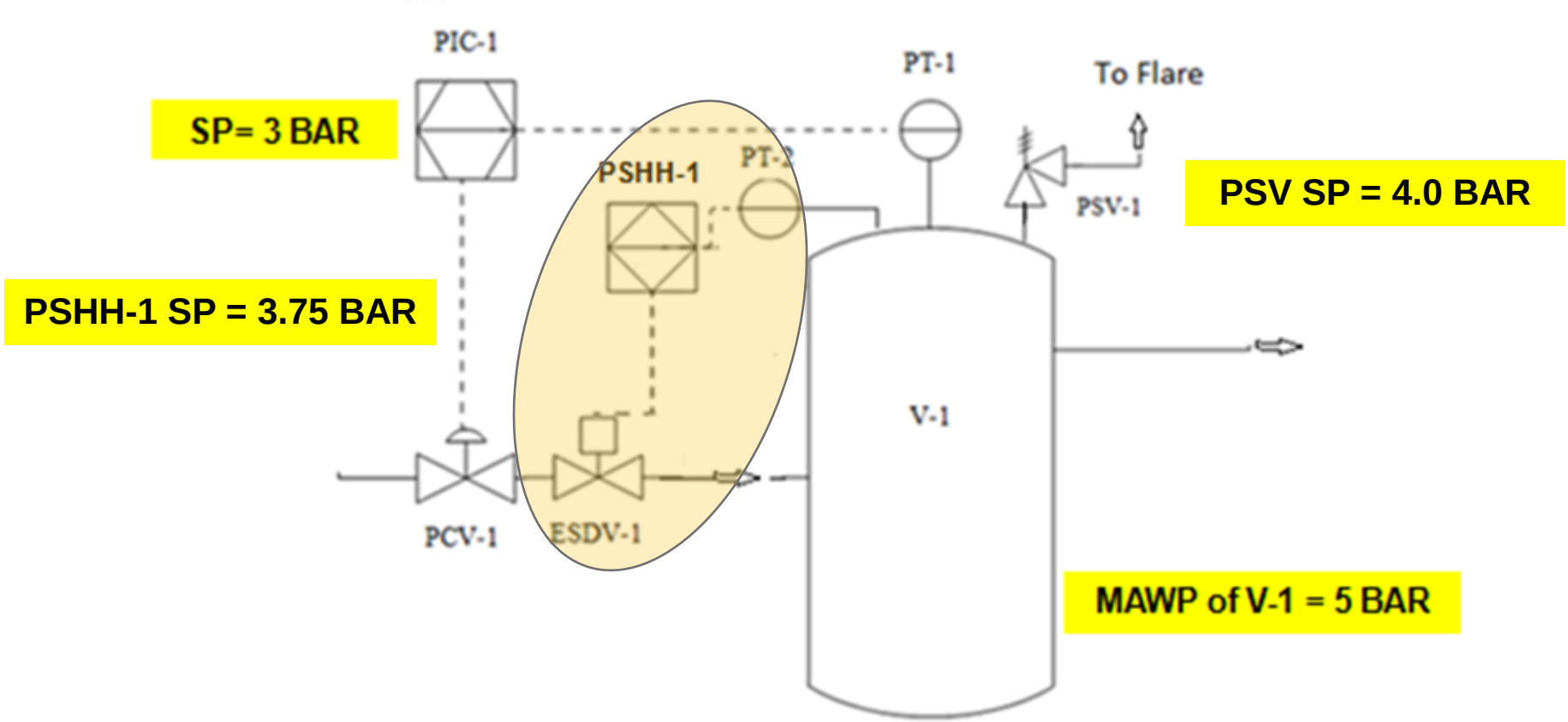


RECAP – Safety Life Cycle



Honeywell
THE POWER OF CONNECTED

RECAP –LOPA determined SIL2 SIF requirement



- High Pressure Trip PSHH-1 added (which is SIL2 rated, ie 99% Reliable as a minimum)
  - Shuts off ESDV-1 when PT-2 detects Pressure in Vessel V-1 > 3.75 BAR
  - ESDV-1 will be a De-energized To Trip (DTT) Fail Close valve, Open when Pressure is less than 3.75 BAR

Honeywell
THE POWER OF CONNECTED

RECAP - Reliability calculations – SIF design

$$PFD_{avg}(SIF\text{-}1) = PFD_{avg}(SE) + PFD_{avg}(LS) + PFD_{avg}(FE)$$

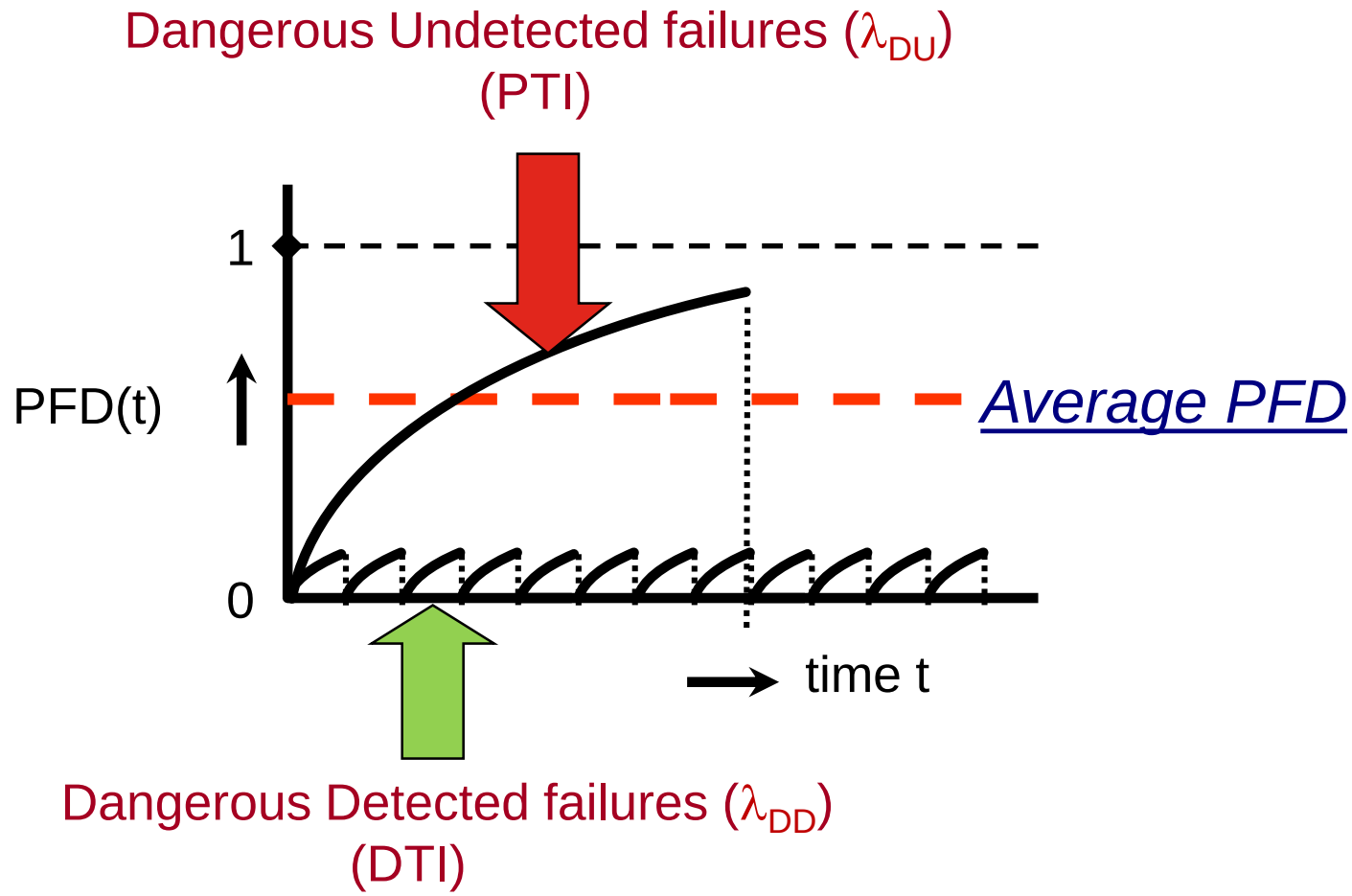
Make sure it is SIL2 (at least 99% Reliable)

RECAP - PFDavg value of a component

- PFDavg (approx.) = $(\lambda_{DU}. PTI) / 2 + (\lambda_{DD}. DTI) / 2$

  - **PFDavg** is the Average Probability of Failure on Demand
  - **DTI** is the Diagnostic Test Interval, normally in seconds for Smart transmitters and Programmable Logic Solvers, within which some Dangerous failures will be detected online depending on the Diagnostic coverage
  - **PTI** is the Proof Test Interval, usually in months, when failures NOT detected by online diagnostics will be detected (assuming a Proof Test Coverage of 100%)

PTI vs DTI, for Dangerous failures



Online Diagnostics

- **Diagnostic Coverage (DC)**
  - Fraction of failures detected by automatic on-line diagnostic tests.
  - $\lambda_{DD} = DC. \lambda_D$

- **Diagnostic Test Interval (DTI)**
  - Interval between on-line tests to detect faults in a safety-related system that has a specified diagnostic coverage

Types of Component failures

There are two types :

- **Random Hardware failures** are “failures, occurring at a random time, which results from a variety of degradation mechanisms in the hardware”.
- **Systematic failures** are “failures related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation or other relevant factors.”

Random Hardware failures

- Random Hardware failures (λ_{total}) :

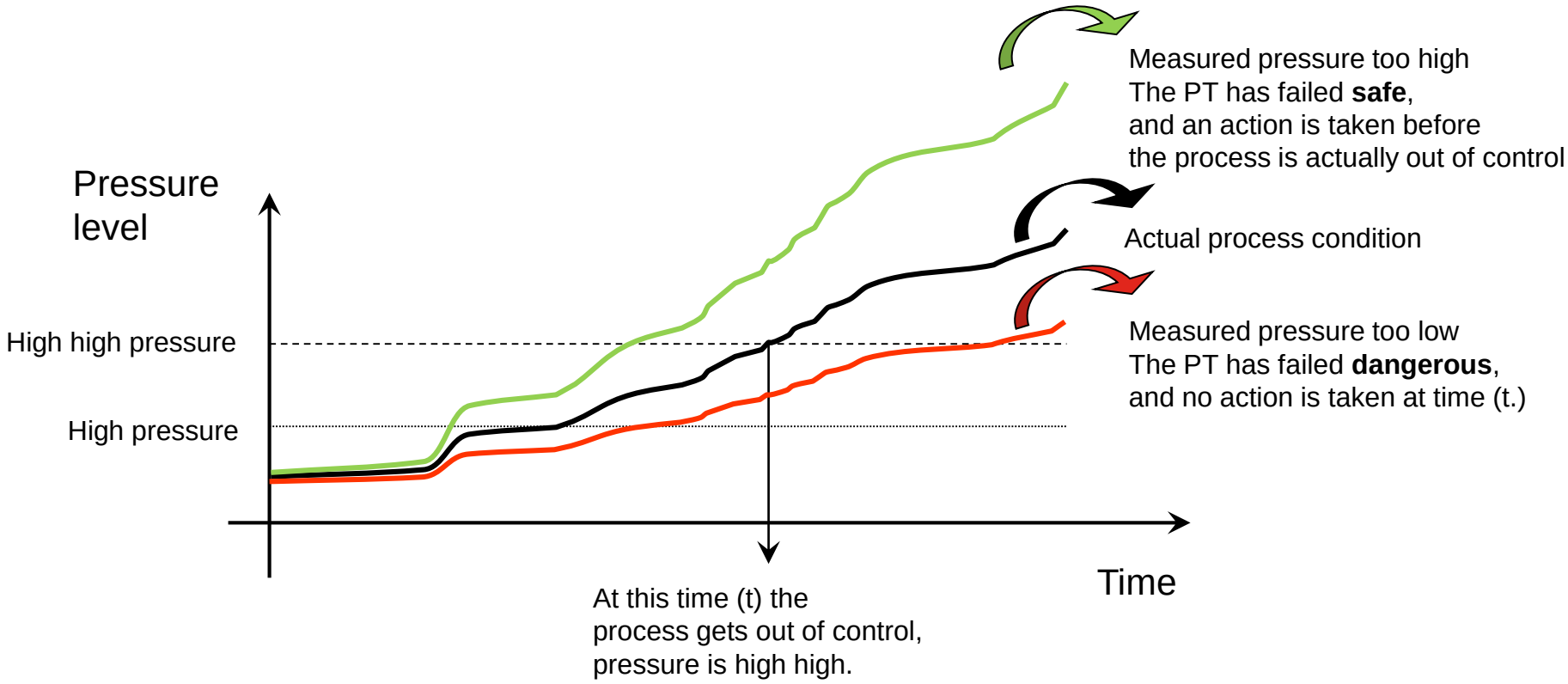
$\lambda_{total} = \lambda_S$ (Safe failures) + λ_D (Dangerous failures)

Safe failures do NOT have the potential to put the safety related system in a hazardous or fail to function state

Dangerous failures HAVE the potential to put the safety-related system in a hazardous or fail-to-function state

Safe vs. Dangerous failure of a Sensing Element

- Analogue Pressure Transmitter



Types of Failures in a Pressure Transmitter

- Safety Function example - On High Pressure (> 3.75 BAR), the PT should sense and send a signal to the Logic Solver which takes a specific executive action

SAFE

Senses Pressure as > 3.75 BAR when it is < 3.75 BAR

- **Safe Detected, λ_{SD}** By online Diagnostics
- **Safe Undetected, λ_{SU}**

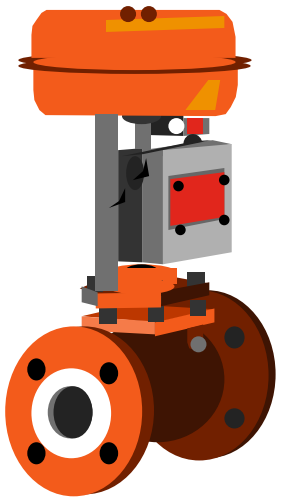
DANGEROUS

Senses Pressure as < 3.75 BAR when it is > 3.75 BAR

- **Dangerous Detected, λ_{DD}** By online Diagnostics
- **Undetected, λ_{DU}** **(PROOF TEST should detect these failures)**

Types of failures in a Valve

- Safety valve, normally open & normally energized
- In case of an out of control process, the valve has to close



SAFE
Closes spontaneously due to loss of energy

- **Safe Undetected**
- **Safe Detected**

DANGEROUS
Stuck at open

- **Dangerous Detected**
  By valve stroke test
- **Dangerous Undetected**
  (PROOF TEST should detect these failures)

Logic Solver failures

SAFE
(Eg - IO module acts when NOT needed)

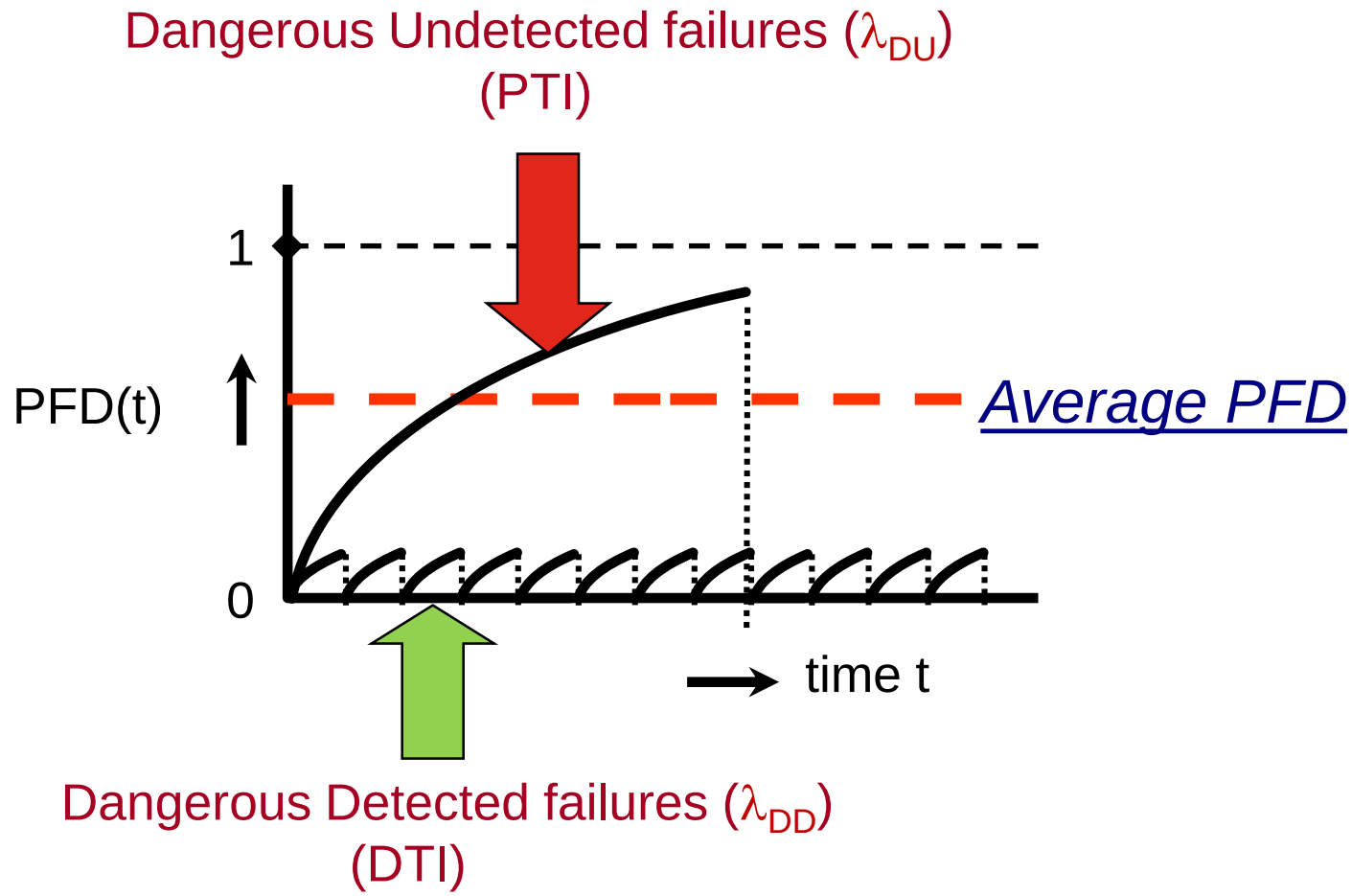
- **Safe Detected**
  99% plus detected by online diagnostics
- **Safe Undetected**
  Less than 1% of failures during PROOF TEST

DANGEROUS
(Eg - IO module Does NOT respond when needed)

- **Dangerous Detected**
  99% plus detected by online diagnostics
- **Dangerous Undetected**
  Less than 1% of failures detected during PROOF TEST

Honeywell
THE POWER OF CONNECTED

PTI vs DTI, for Dangerous failures



Systematic failures

- Presently there is NO mathematical way to quantify Systematic failure rate
- Ways to reduce Systematic failures :
  - A “Proven in use” process while designing and manufacturing components with good Quality checks will help reduce Hardware and Software Systematic failures
  - Well tested application software written in a low level language (like ladder logic or FLDs) to reduce the possibility of introducing Systematic errors

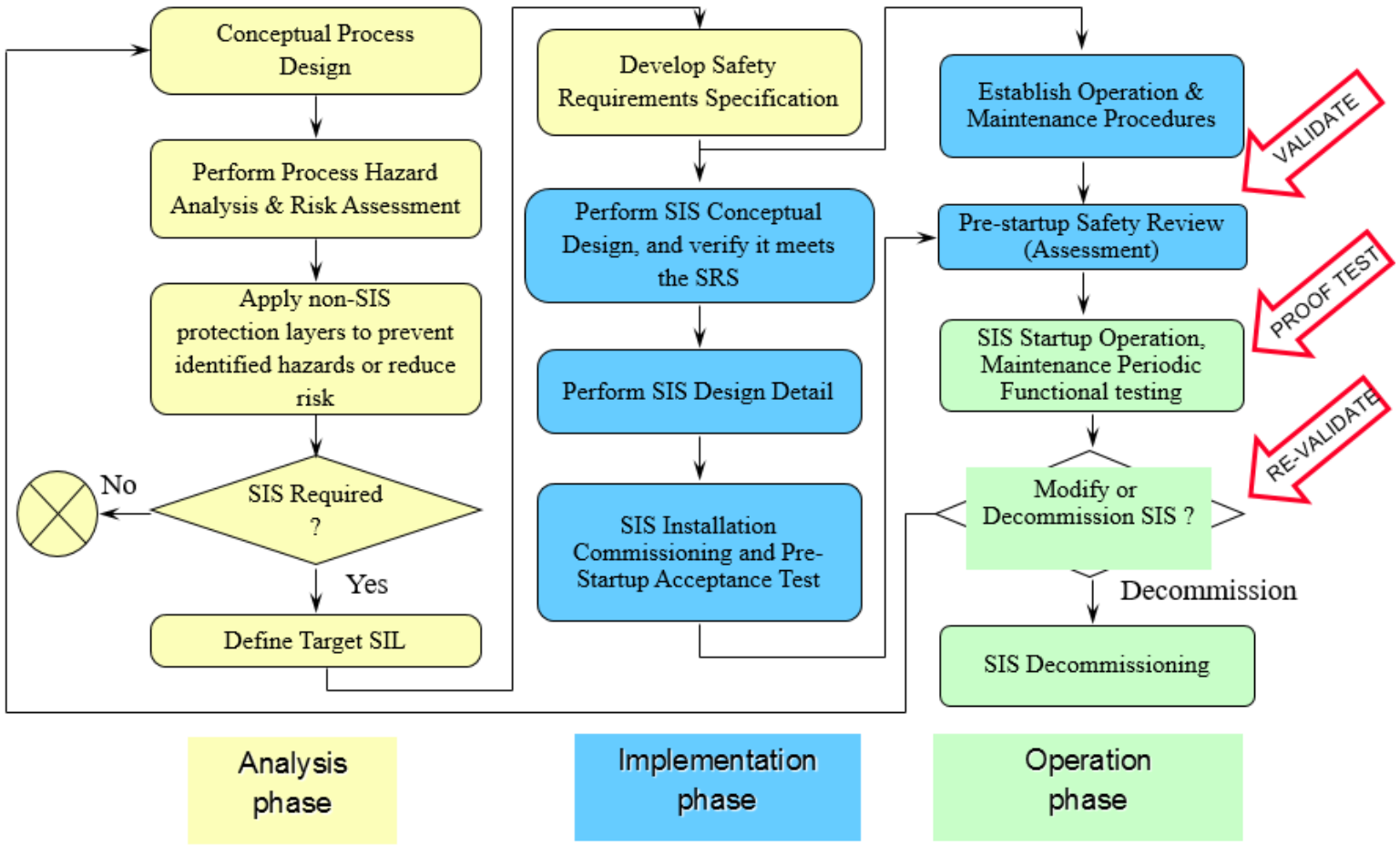
Validation, Proof Test and Revalidation

- **Validation** – per IEC 61511 - Activity of demonstrating that the safety instrumented function(s) and safety instrumented system(s) under consideration after installation meets in all respects the safety requirements specification

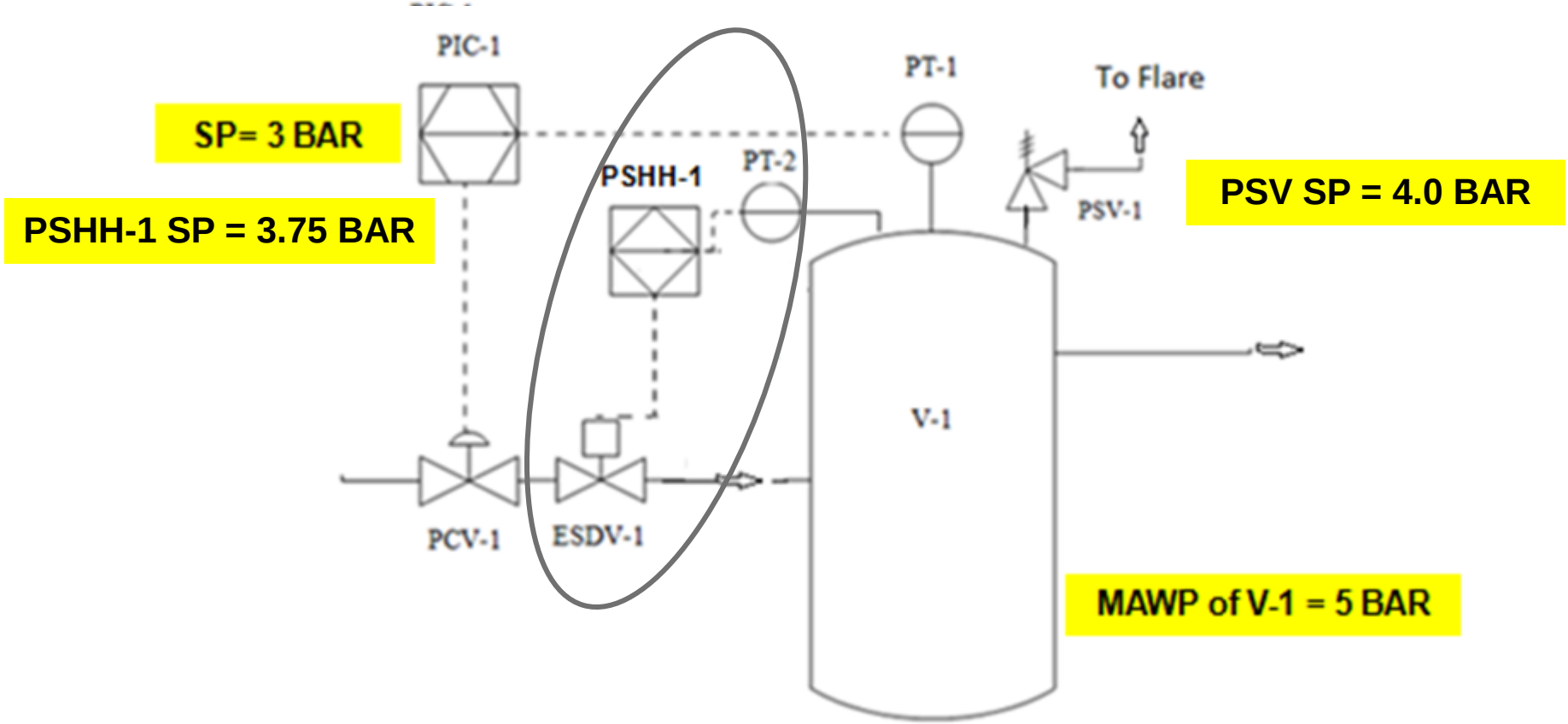
- **Proof Test** – per IEC 61511 - Test performed to reveal undetected faults (both Random and Systematic) in a safety instrumented system so that, if necessary, the system can be restored to its designed functionality

- **Re-validation** – Activity of demonstrating that a modified safety instrumented function(s) and safety instrumented system(s) under consideration after modification meets in all respects the modified safety requirements specification

“When” in a Safety Life Cycle

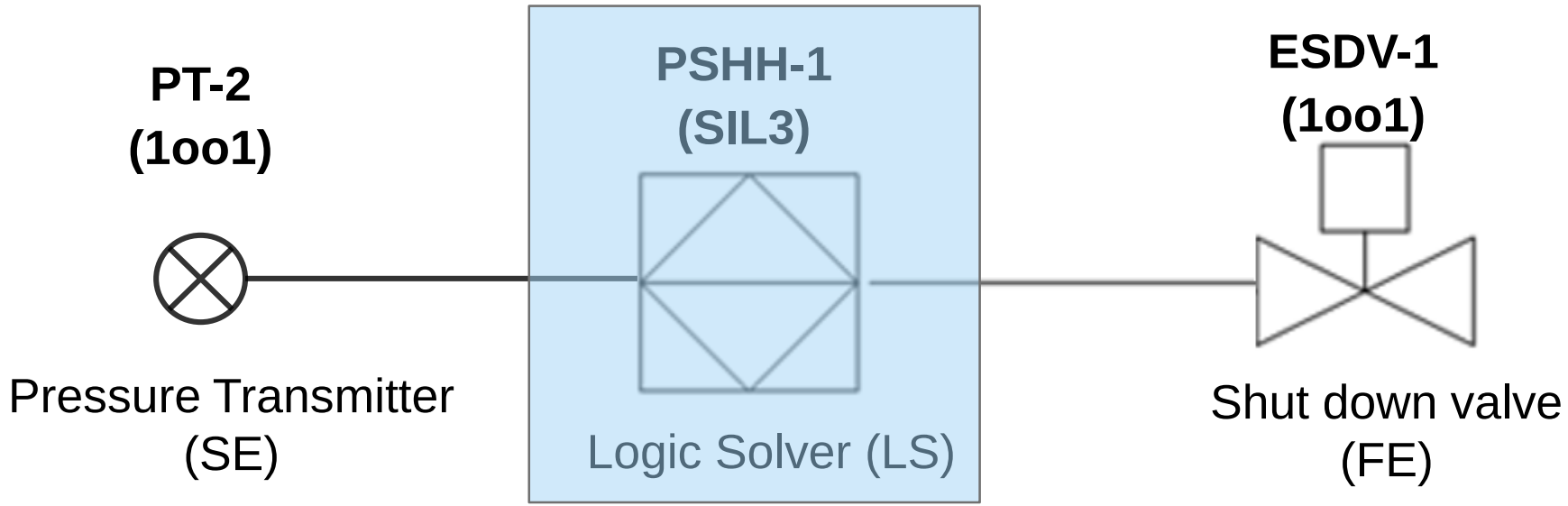


SIF, PSHH-1



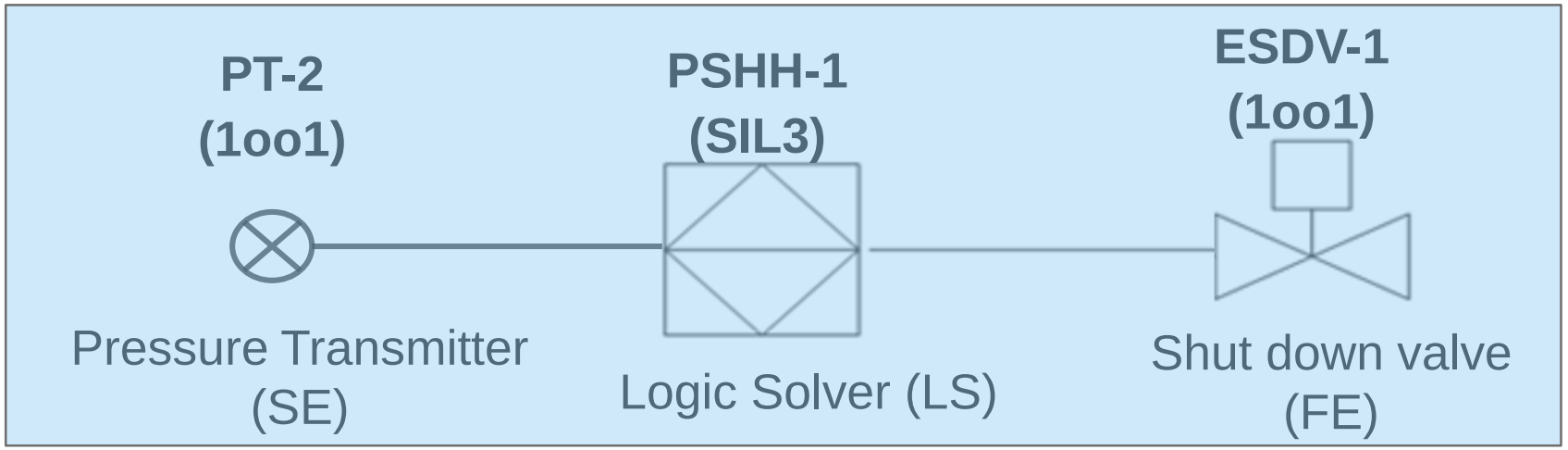
Validation / Re-validation refers to the **WHOLE SIF**, not just some components of a SIF which are installed / modified

How do I validate my SIS Logic Solver ?



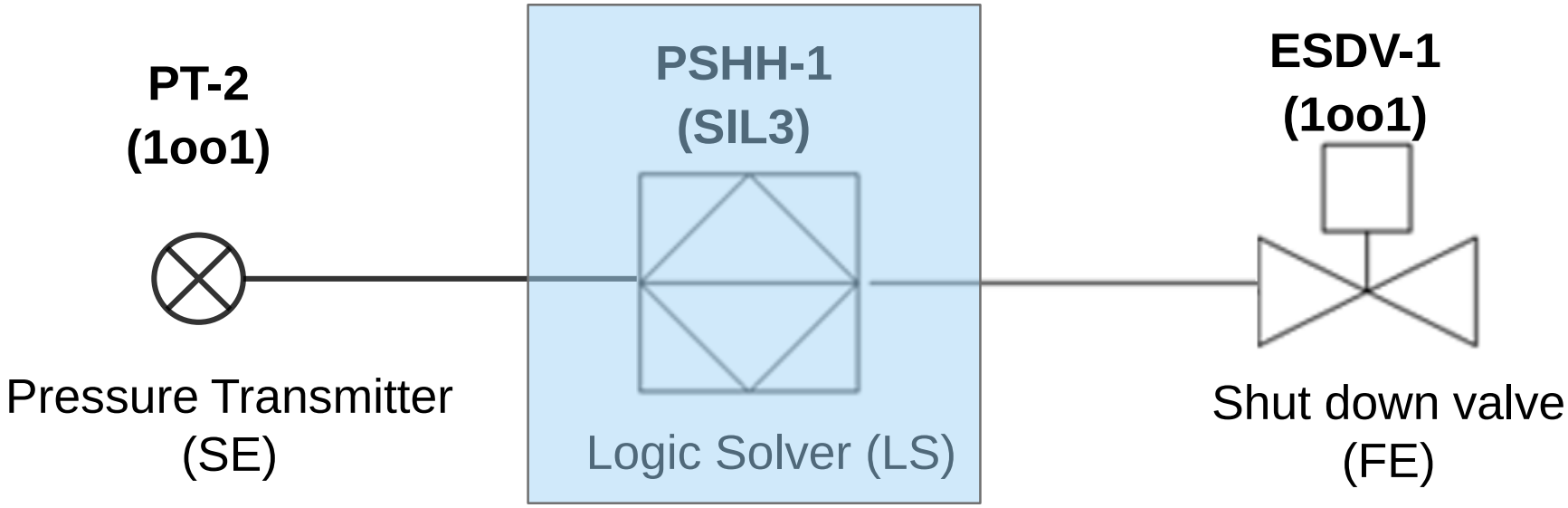
- Validation of the SIS logic solver could be done independently at a Factory Acceptance Test (FAT) and / or when installed, wired up with field instruments and powered up at site.
- Usually a FAT is conducted so that before the complete SIS validation at site, there is enough time to fix both random and systematic errors, if found.

How do I validate my SIS ?



- After site installation, Functional testing of every SIF per the SRS requirements would include the following (and more) :
  - Input Trip condition
  - Reset after trip
  - Input Bypassed
  - Input Bad signal
  - etc

When do I Proof test my SIS Logic Solver ?



- Most SIS Logic Solver suppliers will provide a recommended maintenance checklist and a suggested time period for maintenance.
- If the supplier suggested time period is less than the PTI used to calculate PFDavg of the SIS logic solver, then the end user should follow the time period suggested by the SIS logic solver supplier for Proof Testing the SIS logic solver

SIS Logic Solver Proof Test

- PFDavg SIL3 Logic Solver = $(\lambda_{DU}. PTI) / 2 + (\lambda_{DD}. DTI) / 2$

  - Usually the DC for SIL3 rated Logic Solvers is very High (> 99%), so

    $\lambda_{DU} >> \lambda_{DD}$

  - Therefore $(\lambda_{DU}. PTI) / 2 >> (\lambda_{DD}. DTI) / 2$

  - DD failures are detected by **online diagnostics**
  - DU failures are detected during **Proof test** and are very small in quantity

How do I Proof test my SIS Logic Solver ?

- Will be suggested by Logic Solver manufacturer
- Typical Proof testing activities for Logic Solver **Hardware** are checking and replacing / fixing the following :

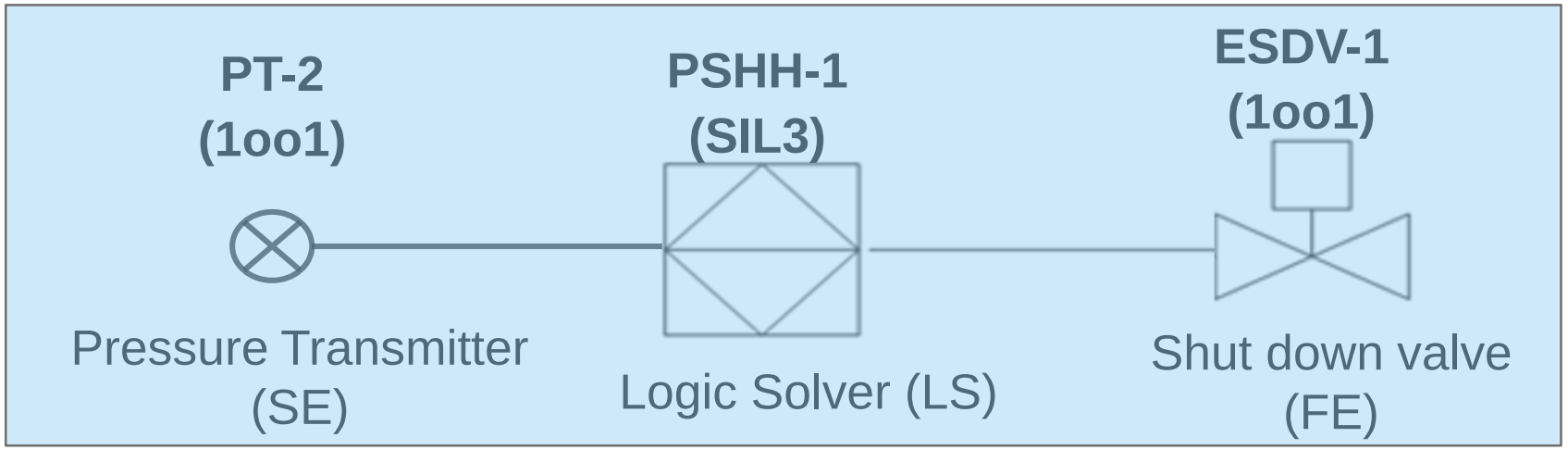
  - Cable damage between SIS Logic Solver modules
  - Voltages to the Control Processor if within the tolerable limits
  - Temperature in the Control Processor if within the tolerable limits
  - Airflow obstruction to various modules
  - Presence of any earth faults
  - Availability of spare parts and usage per requirement

How do I Proof test my SIS Logic Solver ?

- Typical Proof testing activities for Logic Solver **Software** to primarily reduce systematic errors are:

  - Making sure the latest running application software has been backed up.
  - If there has been a change in the firmware of the Logic Solver, it is recommended to upload the new firmware at this time.
  - If the new firmware was already uploaded online earlier or now, or if there were some modifications done to a SIF or SIFs, it is recommended to do a complete functional test of all the SIFs as done during validation. The reason is to make sure that a firmware change or modification to a validated application software has not in any way affected the functioning of all SIFs

How do I Proof test my SIS ?



- Check Transmitter mechanical and electrical installation, calibration etc
- Check valve assembly for mechanical faults if any, if TSO is important, check valve “passing” on closure etc
- Functionally check all SIFs in the SIS

When do I Re-validate my SIS ?

- Revalidation of a SIS is done during the Operation and Maintenance phase of the Safety Life cycle usually when:

  - Additional SIFs may get added, or existing SIFs may get modified or deleted, during the next cycle of a Process Hazard Analysis (usually every 5 years in the USA as per OSHA regulation – 29 CFR 1910.119) or during a system audit or assessment.
  - Modification of an existing SIF based on Operational feedback, for example – too many spurious trips, too many demands etc
  - Change of SIS logic Solver or other SIF components due to excessive Random and / or Systematic failures

Modification to a SIS

A modification plan usually follows end user's Management Of Change (MOC) process which generally details the following:

- Personnel in the company who will authorize the modification
- Reason for the modification to the SIS
- Impact analysis to make sure that this modification :
  - does not lead to any new potential hazardous events , either during implementation or after the modification.
  - does not effect other SIFs in the same SIS
- Implementation of the modification
- Revalidation before "startup" of the modified SIS
- Update of all documentation to reflect the changes done during the modification

Extent of Revalidation of SIS Logic Solver

- Based on IEC61508, Part 3, Table A.8, meant for Programmable Logic Solvers
- Recommended to be used for all types of Logic Solvers

(R = Recommended, HR = Highly Recommended)

Technique/Measure *		Ref.	SIL 1	SIL 2	SIL 3	SIL 4
1	Impact analysis	C.5.23	HR	HR	HR	HR
2	Reverify changed software module	C.5.23	HR	HR	HR	HR
3	Reverify affected software modules	C.5.23	R	HR	HR	HR
4a	Revalidate complete system	Table A.7	---	R	HR	HR

How do I Re-validate my SIS Logic Solver ?

- What to test will depend on the table on the previous slide
- Process is similar to Validation of the SIS Logic Solver to test for Random hardware and Systematic failures

Conclusion

Activity	When ?	Why ?	How ?
SIS Logic Solver Validation	Just before taking SIS logic solver online for the first time	Hardware test to detect Random failures and software to reduce Systematic failures	Test logic solver Hardware and Application Software
SIS Logic Solver Proof test	During the regular maintenance of the SIS Logic Solver dictated by SIL calculations or SIS vendor	Hardware test to detect Random failures by looking for potential errors not detected by online diagnostics and software to reduce Systematic failures	Test logic solver Hardware and Application Software if change in firmware or any modifications have been done
SIS Logic Solver ReValidation	When modifications have been made to a validated SIS logic solver and before taking it online	Hardware test to detect Random failures and software to reduce Systematic failures	Test logic solver Hardware and Application Software. Extent of test will be based on Table 2, which is based on SIL ratings of SIFs in the SIS

References

- ANSI/ISA 84.00.01- 2004 (IEC-61511). “Functional safety – Safety instrumented systems for the process industry sector”.
- IEC-61508, “Functional safety of electrical/ electronic/ programmable electronic safety related systems”.
- “SIS Design Basis Revalidation”, white paper by Kenexis