Aspects in the compliance to IEC 61511 standard in Refineries and Petrochemical plants

Tracy Lau
Regional Business Development Manager for Safety
Schneider Electric South East Asia

Safety Case Symposium 2018 Singapore

Life Is On

Schneider Electric

Challenges in Refinery Operation

Maximize Productivity

- High Reliability
- Minimising down-time
- Long proof testing periods

Design a Safety Instrumented System that has both high reliability & high integrity

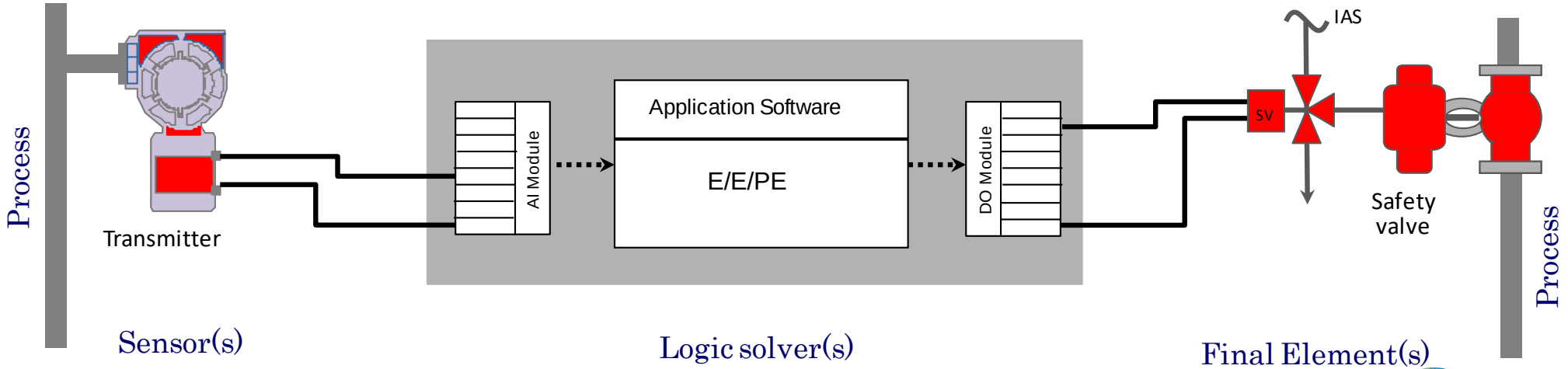
Safe Operation

- Meeting regulator requirement & IEC61511 compliance for SIS
- De-energize to trip function
- Short testing period for high SIL safety function
- Partial valve stroke testing
- Considering process safety time and system response times

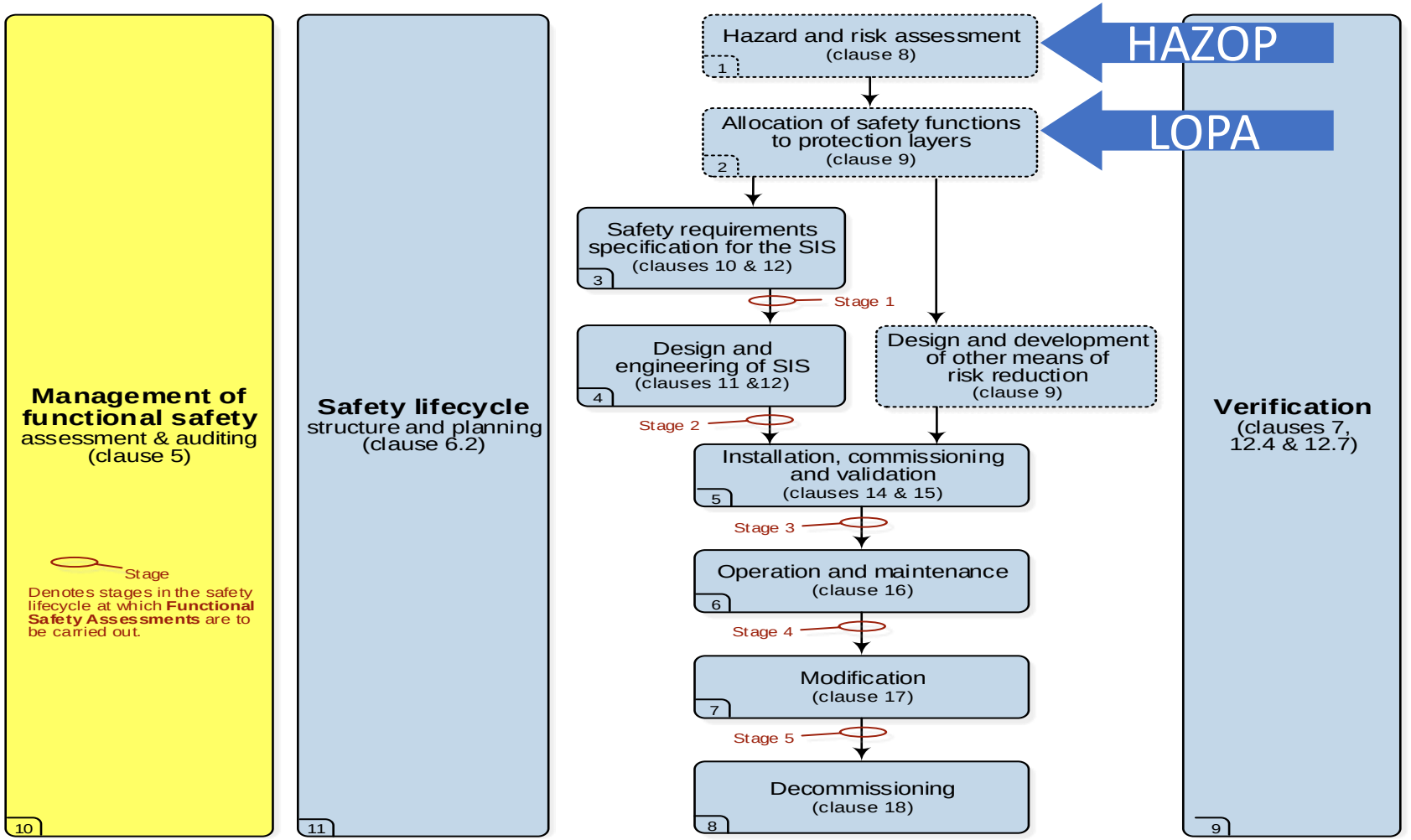
What is Safety Instrumented System (SIS)?

"A system designed to respond to conditions in the plant which may be hazardous in themselves or, if no action was taken, could eventually give rise to a hazard, and to generate the correct outputs to mitigate the hazardous consequences or prevent the hazard."

Source - Health and Safety Executive (HSE), 1987



IEC61511 Safety Lifecycle



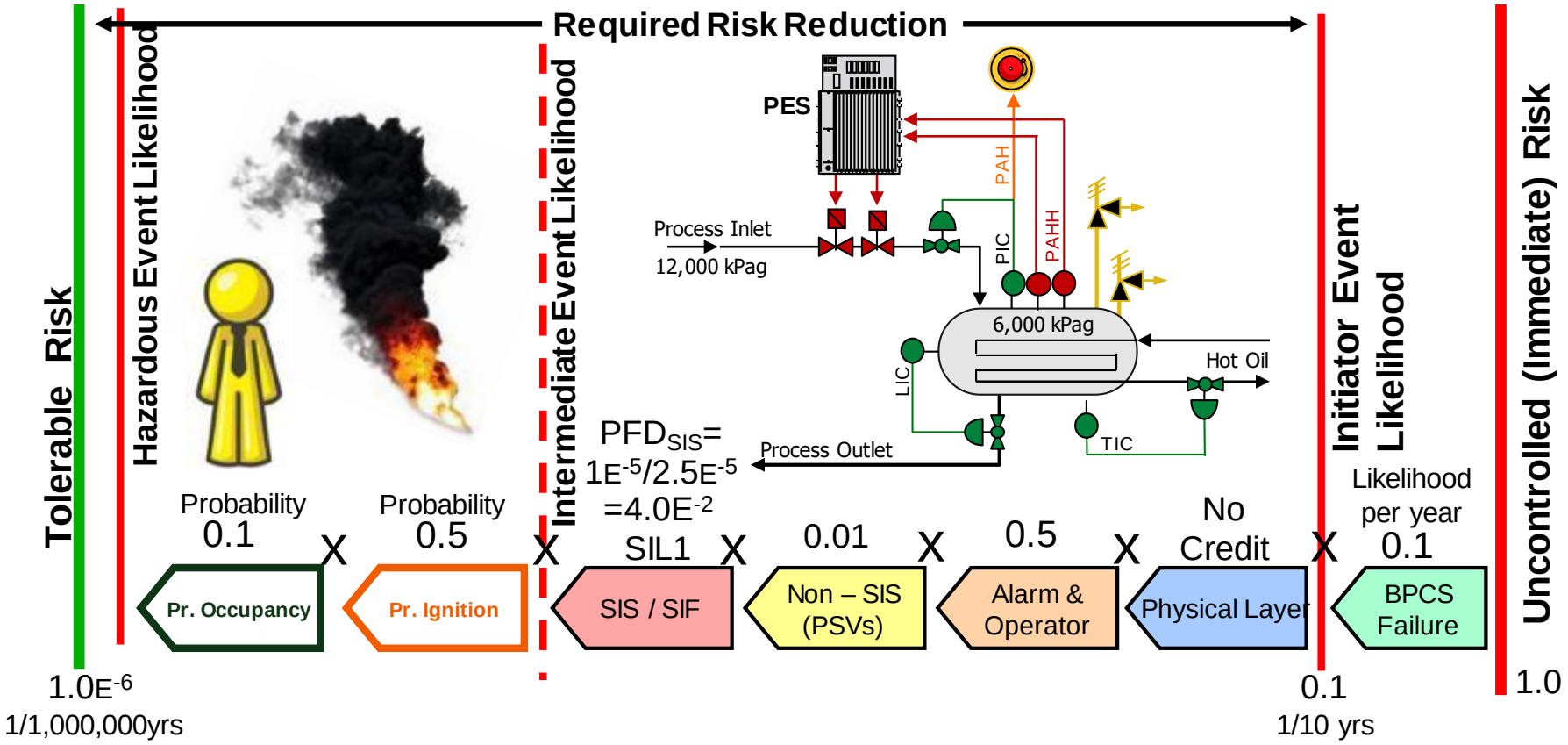
Pitfalls in the application of safety lifecycle

- No corporate IEC 61511 Safety Management Plan (SMP) is in place. It is left to EPC to decide procedures.
- An SMP is in place but there is insufficient guidelines and awareness for implementation.
- An SMP and guidelines are in place but they are not fully implemented to reduce cost.
- SMP lifecycle activities are implemented but there is insufficient verification, assessment and auditing activities.
- SMP lifecycle activities are terminated once the EPC leaves the site.

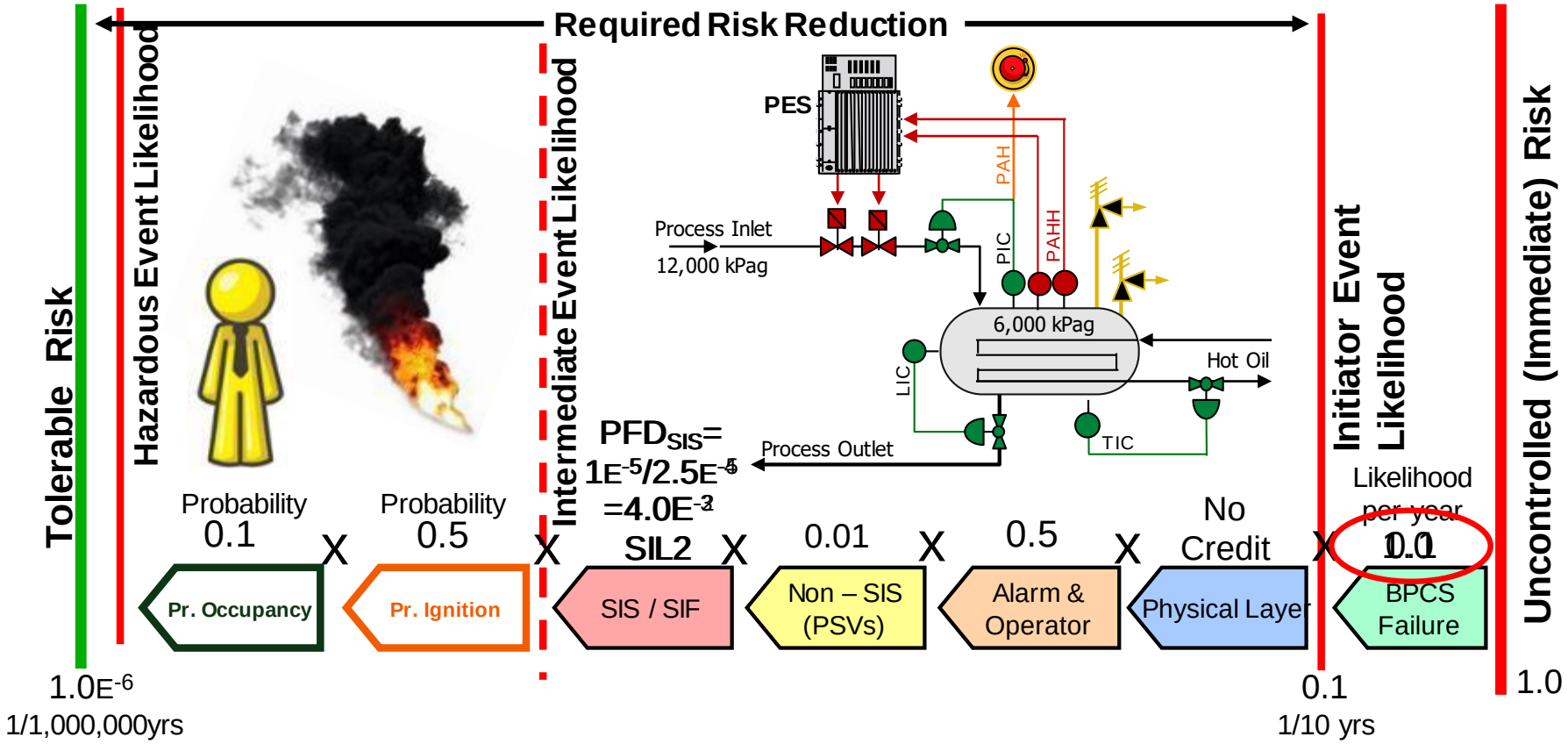
Pitfalls in the application of HAZOP

- A Hazard & Operability (HAZOP) study is a core aspect in the IEC 61511 safety lifecycle.
- If gaps exist in the HAZOP, these gaps could be propagated throughout the rest of the lifecycle activities. This may lead to deficiencies in the design and implementation of the SIS.
- Gaps in a HAZOP study could be caused by:
  - The HAZOP leader is not experienced or familiar with the process
  - Insufficient preparation prior to the HAZOP workshop
  - The HAZOP leader is not familiar with functional safety and not aware on the input information required from the HAZOP to make decisions on the other lifecycle activities
  - Lack of communication within the HAZOP team
  - Insufficient documentation & time for HAZOP
  - The HAZOP does not reference tag numbers of process units, controls loops and safety functions
  - The HAZOP is considered just as a 'tick' activity

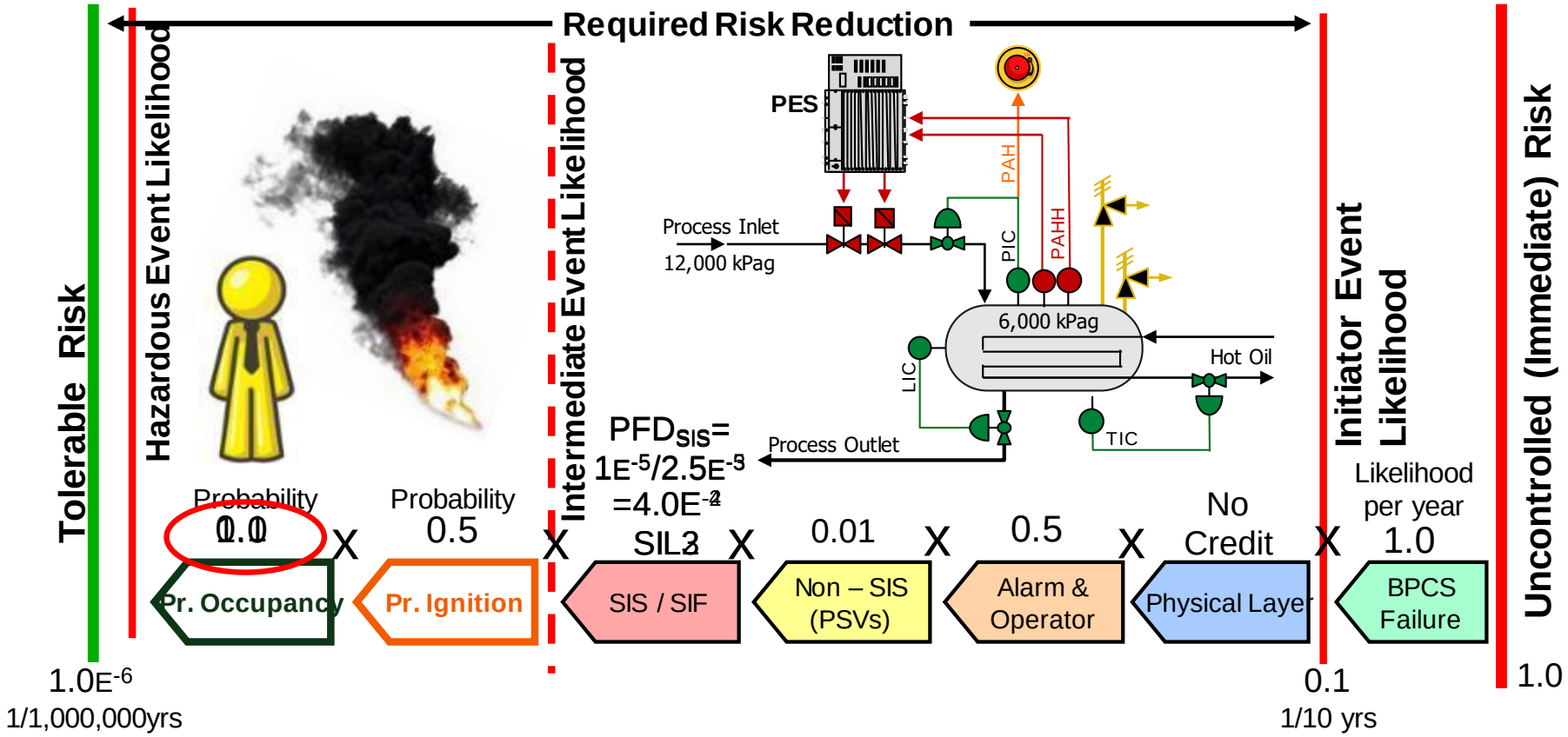
SIL Determination – Layer of Protection Analysis



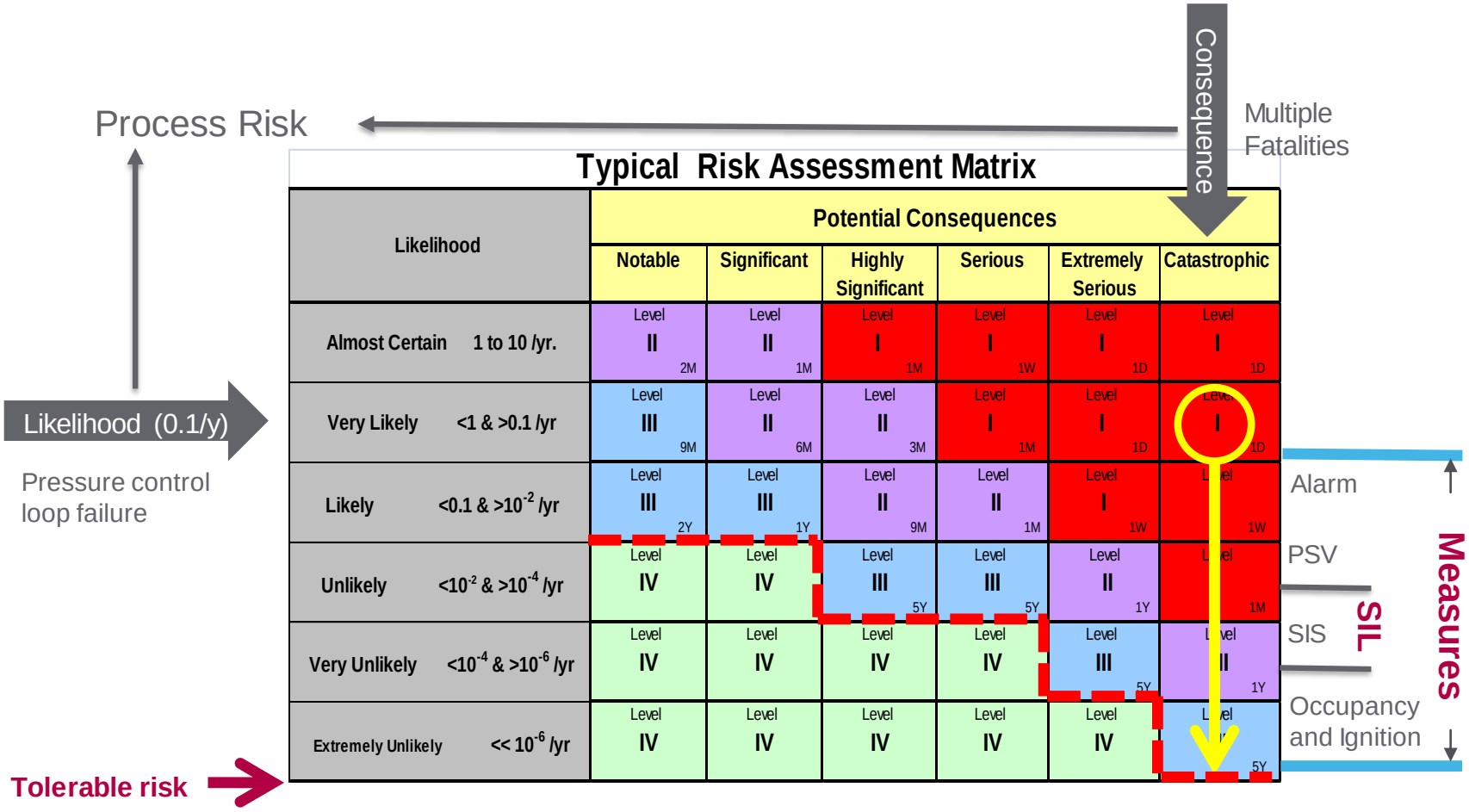
SIL Determination – Higher Demand, Higher SIL



SIL Determination – Higher Occupancy, Higher SIL



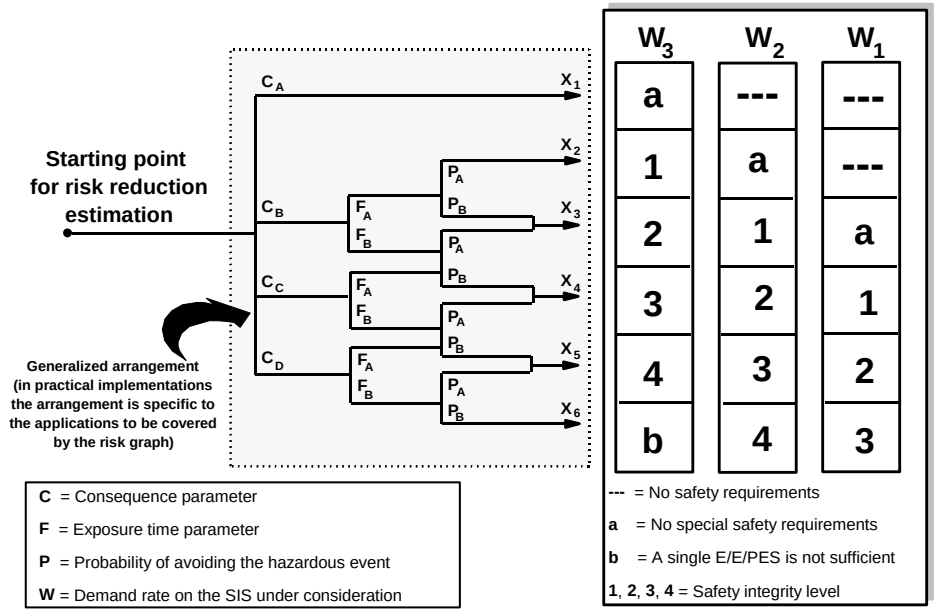
SIL Determination – Reducing Risk



Corporate Risk Matrix

- To classify the risk reduction required from a safety function (SIL) the corporate must have risk matrix with identified risk tolerance.

Do not use sample of risk matrices shown the standards!
These risk matrices do not represent corporate risk tolerance!



SIL Determination

- **A demand on a safety function** is caused by failure of control system or other equipment in the plant. More reliability of these devices leads to a lower required SIL.
- **Use a proven failure rate** for the frequency of demand (site data is best).
- **Greater independence of protection layers** available results in lower common cause failures and lower required SIL.
- **Decreased occupancy** (people within the hazardous area) the lower the required SIL.
- **Perform a review** on the above every five years and revise the SIL assigned.

Why do we want to avoid a high SIL?

Pitfalls in SIL Determination

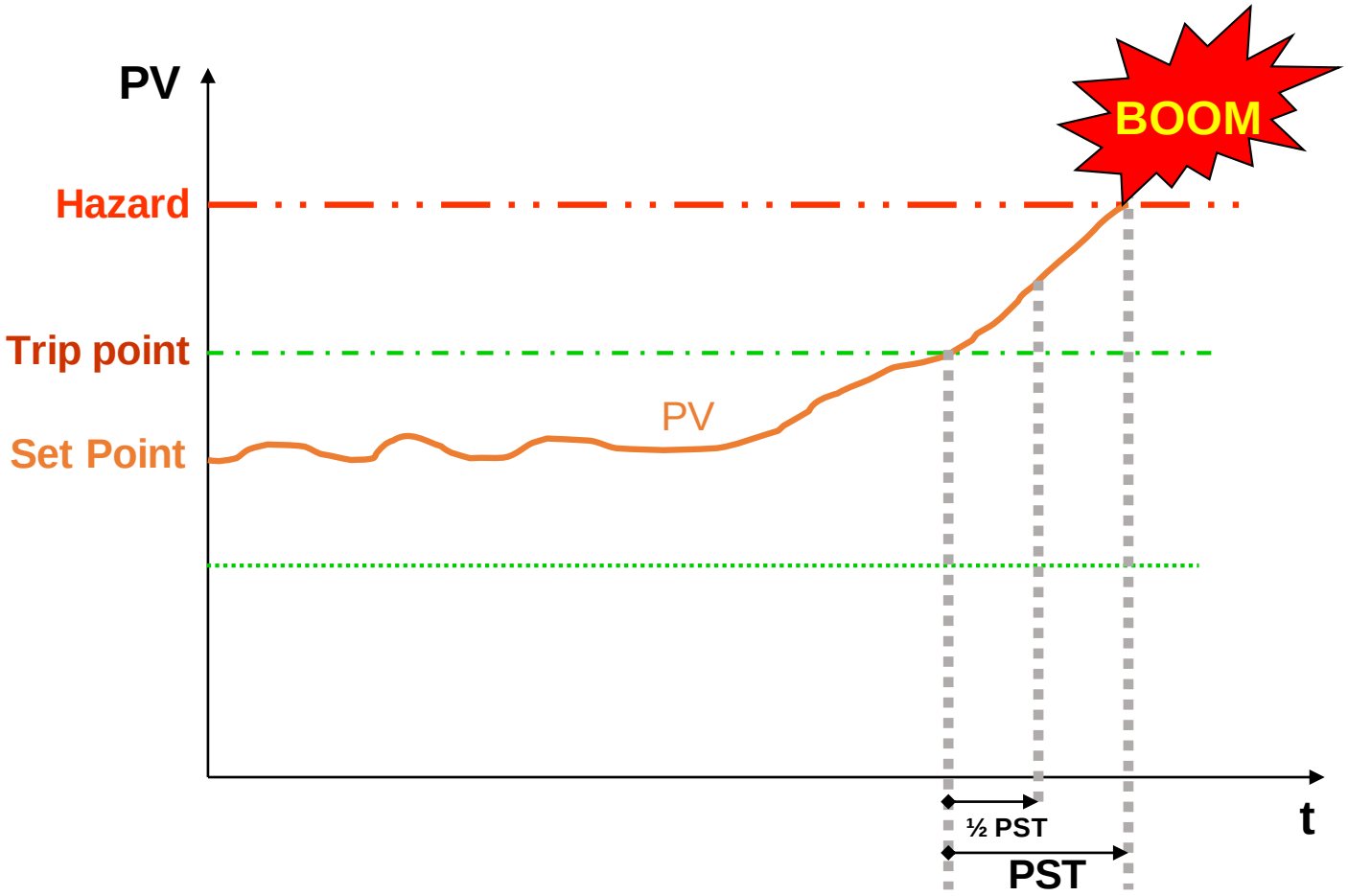
- Use a proven methodology for SIL assignment – typically Layer of Protection Analysis (LOPA) is ideal. Avoid SIL determination methods that provide quick results (reduce workshop time) but result in higher assigned SILs. The corporation may pay a higher price for the rest of plant life.
- Use an experienced functional safety expert. Less experienced engineers tend to be conservative and end up with higher SIL. Alternatively, they may assign too much credit leading to a low SIL.

Do not allow EPC to run the show

Pitfalls in Detail Design

- No Safety Requirement Specification (SRS) is prepared for SIS detail design.
- Many SRS items are left to EPC to decide which may impact on the plant's on-going reliability and availability such as:
  - Acceptable SIS nuisance trip rate
  - SIS response to detected failures
  - Mean time to restoration
- Failure to ensure the SIS design meets the required Process Safety Time.

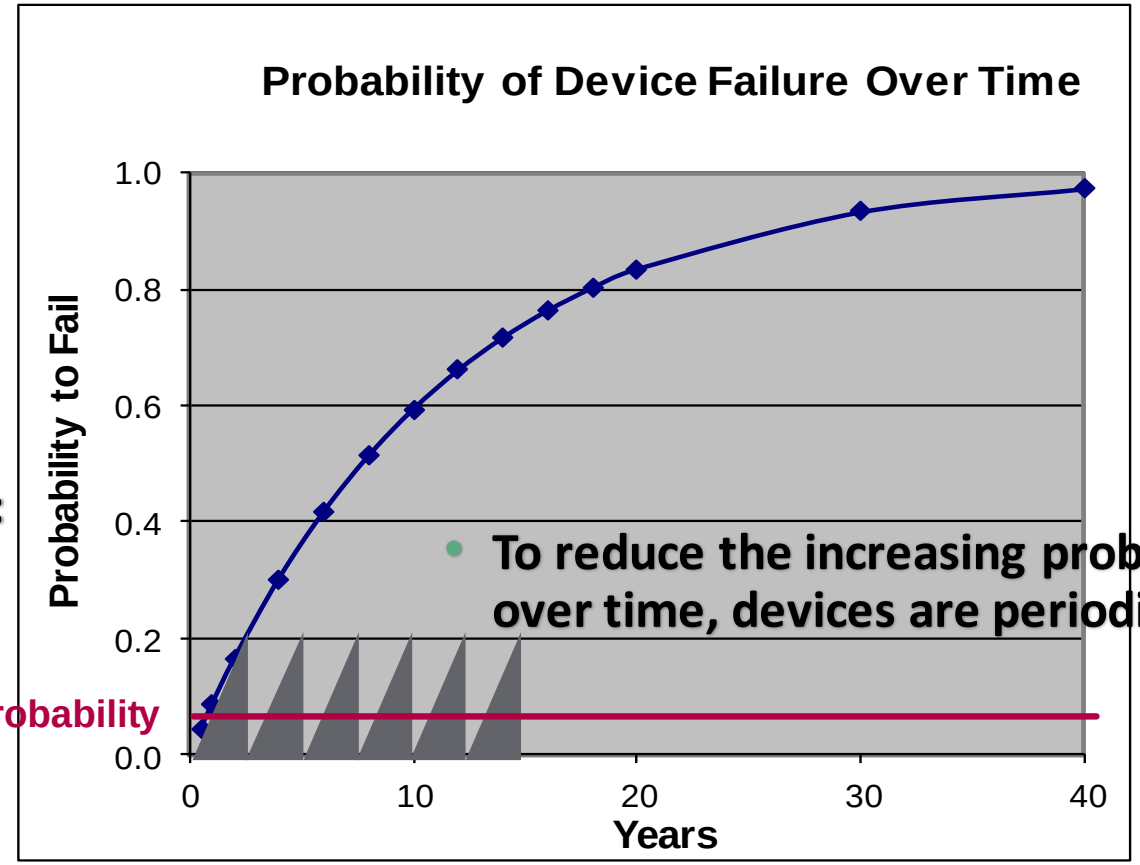
Process Safety Time (PST)



- PST is a function of the process chemistry and/or process dynamics. It must be estimated by calculation or dynamic simulation.
- The safety function response time should be at least half the PST.

SIL Verification

- All devices fail - it is not a matter of if, but when.



- **If a device is tested at interval TI, then the average PFD would be:**

PFDavg = λdu TI / 2

- **To reduce the increasing probability a device failure over time, devices are periodically proof tested.**

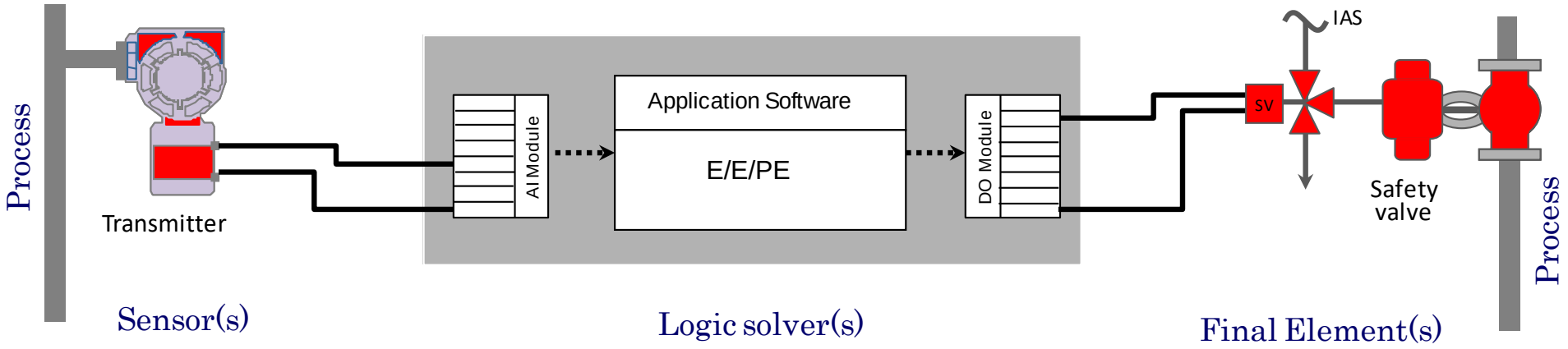
- **The probability of a device to fail follows the exponential function:**

PFD = (1-e-λt)

where t = time

λ = device failure rate

Probability Failure on Demand

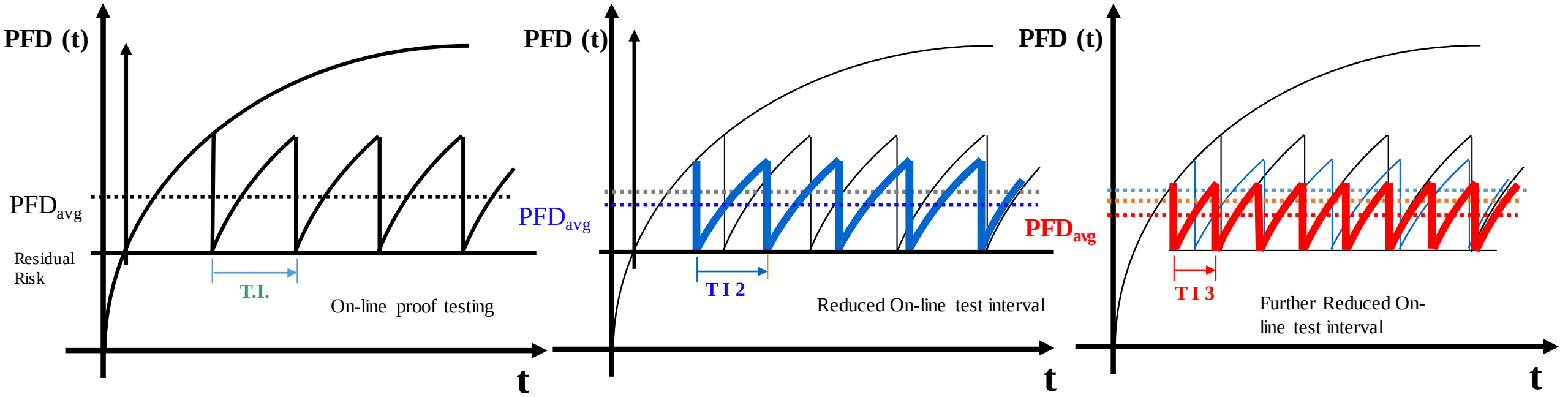


$$\mathrm{PFD}_{\mathrm{SIF}} = \sum \mathrm{PFD}_{\mathrm{Sensor,\,i}} + \sum \mathrm{PFD}_{\mathrm{Logic\,Solver}} + \sum PFD_{FinalElement,i}$$

Proof Testing

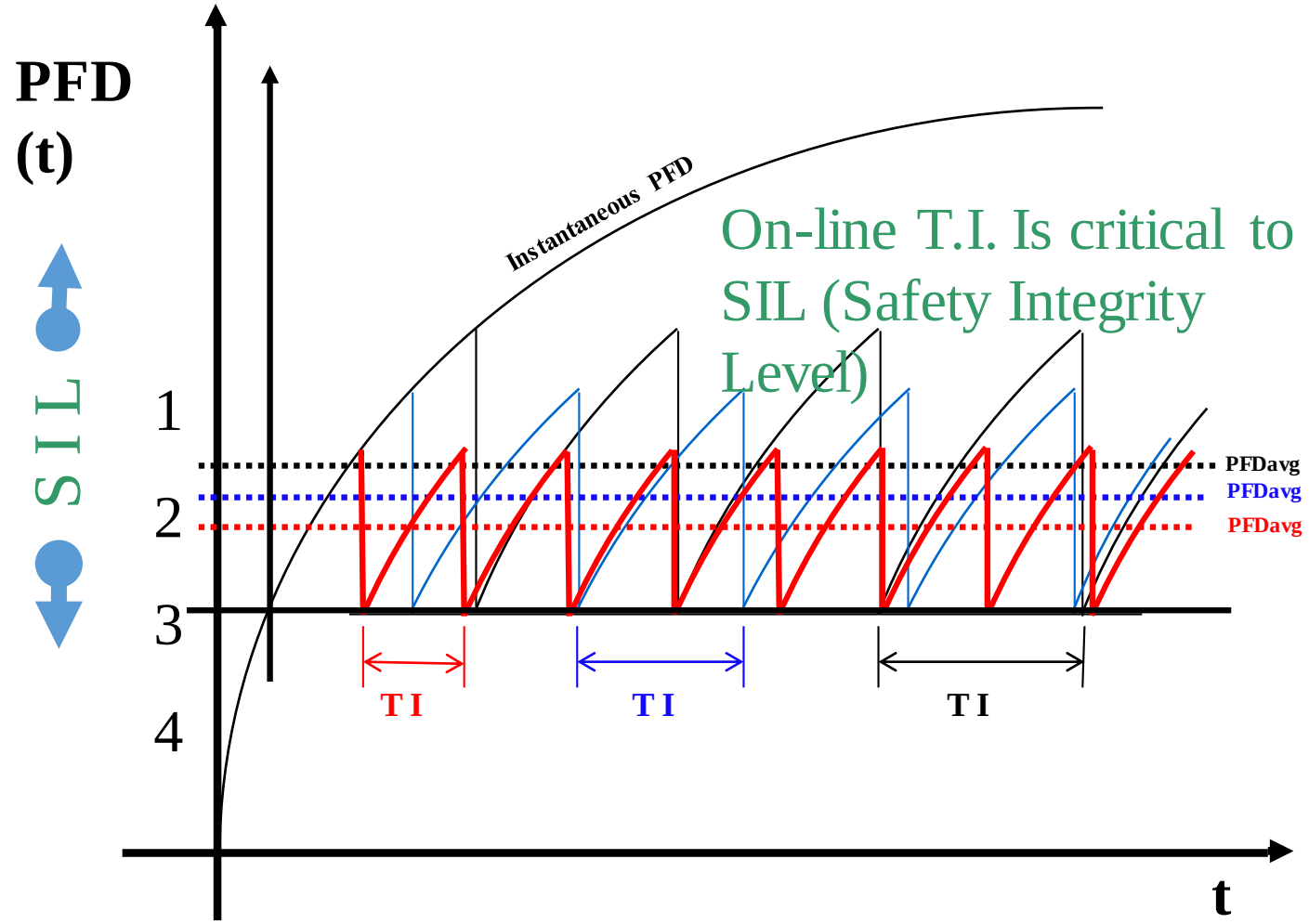
- All SIS devices must be proof tested periodically.
- The proof testing interval depends on the integrity required for the device. Higher integrity (SIL) requires more testing (shorter testing period).
- The testing must follow certain procedures to ensure that the devices do not have any hidden failures.
- The test must be conducted by trained instrument technicians.
- Higher frequency of offline testing of ESD valves means increased plant shutdown and reduced productivity.
- To achieve a lower proof testing frequency the design may utilize more instrumentation (1oo2 and 2oo3 configuration).
- To maintain high integrity (SIL2 & SIL3) and achieve increased proof testing intervals (i.e. extended turnaround time) may require online testing or PVST.

Reduced Test Interval



$$PFD_{avg} = \lambda_{du} TI / 2$$

Reduced Test Interval



Pitfalls in the calculation of PFD_{avg} (SIL Verification)

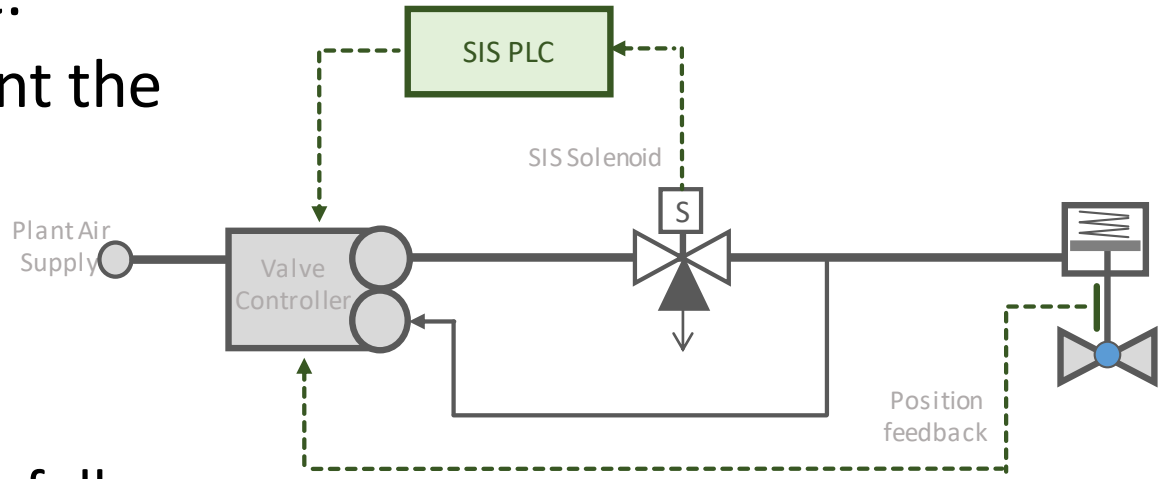
- SIL Verification is often seen as a matter of calculating the PFD for all items in the cause and effect.
- SIL Verification requires full understanding to the process and the definition of critical final elements required to place the process into a safe state.
- Incorrectly assumed that product specific failure data is the best data for PFD calculation. This is totally incorrect:
  - It does not reflect environmental conditions, particularly for valves
  - For pressure based transmitters, impulse line blockage is not considered in specific data. Impulse line failure (blockage) can be 3-5 times higher than the dangerous failure of the transmitter.
- Common cause failures not considered. For redundant elements, CCF may contribute over 80% of the total failure.

ESD Valves

- Traditionally, ESD valves have been tested at unit turnaround every 2-3 years, using offline full-stroke testing.
- However, due to improved mechanical reliability and preventative maintenance programs, many operating refineries tend to extend unit turnaround intervals to 5+ years.
- Extended turnaround intervals yield great economic returns through increased production. However, it can also mean that block valves are expected to go longer between functional tests, yet still achieve the same performance level. This is simply not possible.

Partial Valve Stroke Testing (PVST)

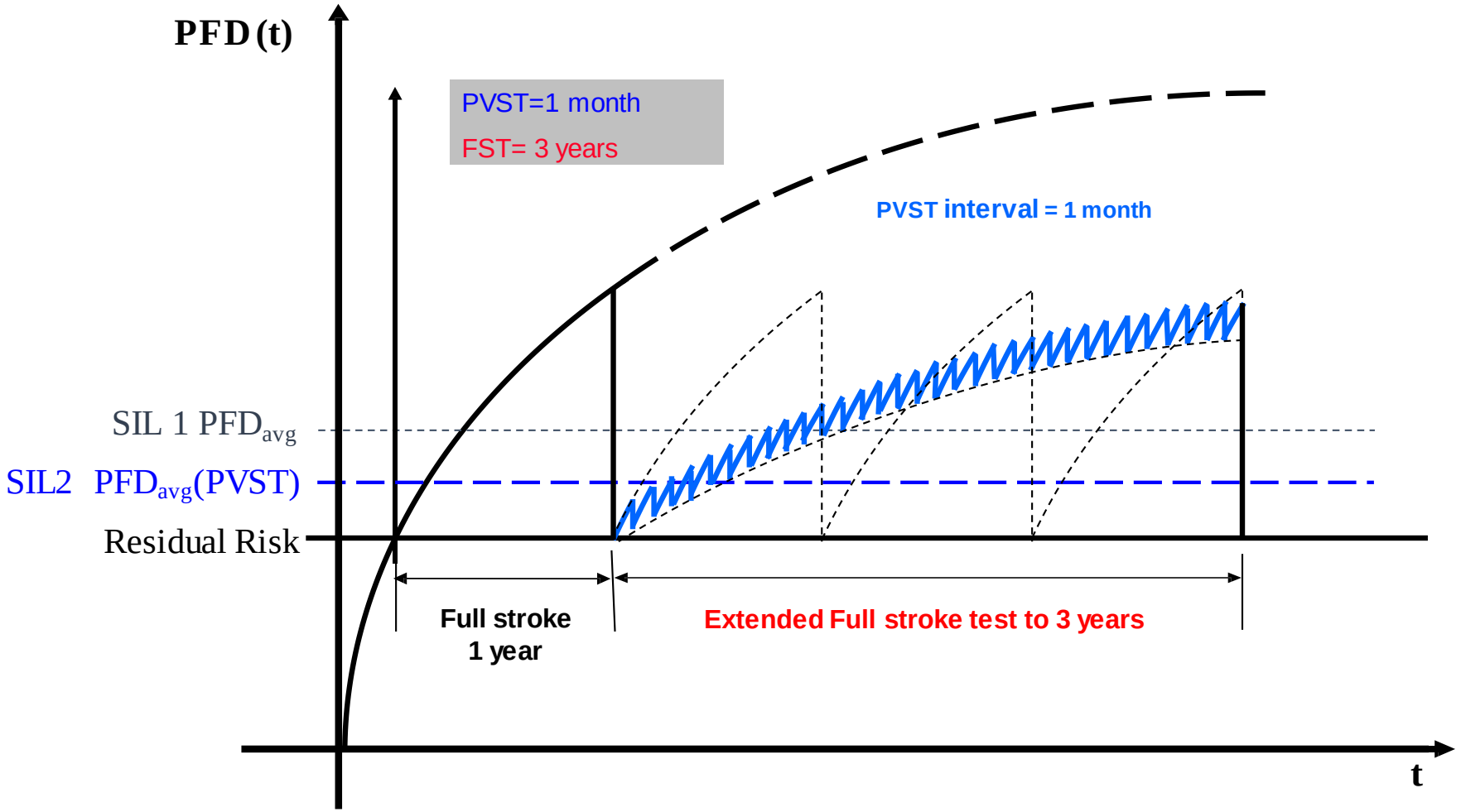
- When SIL 2 or SIL 3 performance is required, five-yearly functional tests are inadequate.
- Consequently, it is necessary to supplement the offline full stroke test.
- This involves implementation of valve diagnostics, such as:
  - Partial valve stroke testing (PVST), or
  - Alternate testing strategies, such as online full stroke testing.
- PVST is a method whereby a portion of the valve assembly is tested at a more frequent interval than the full test rate.



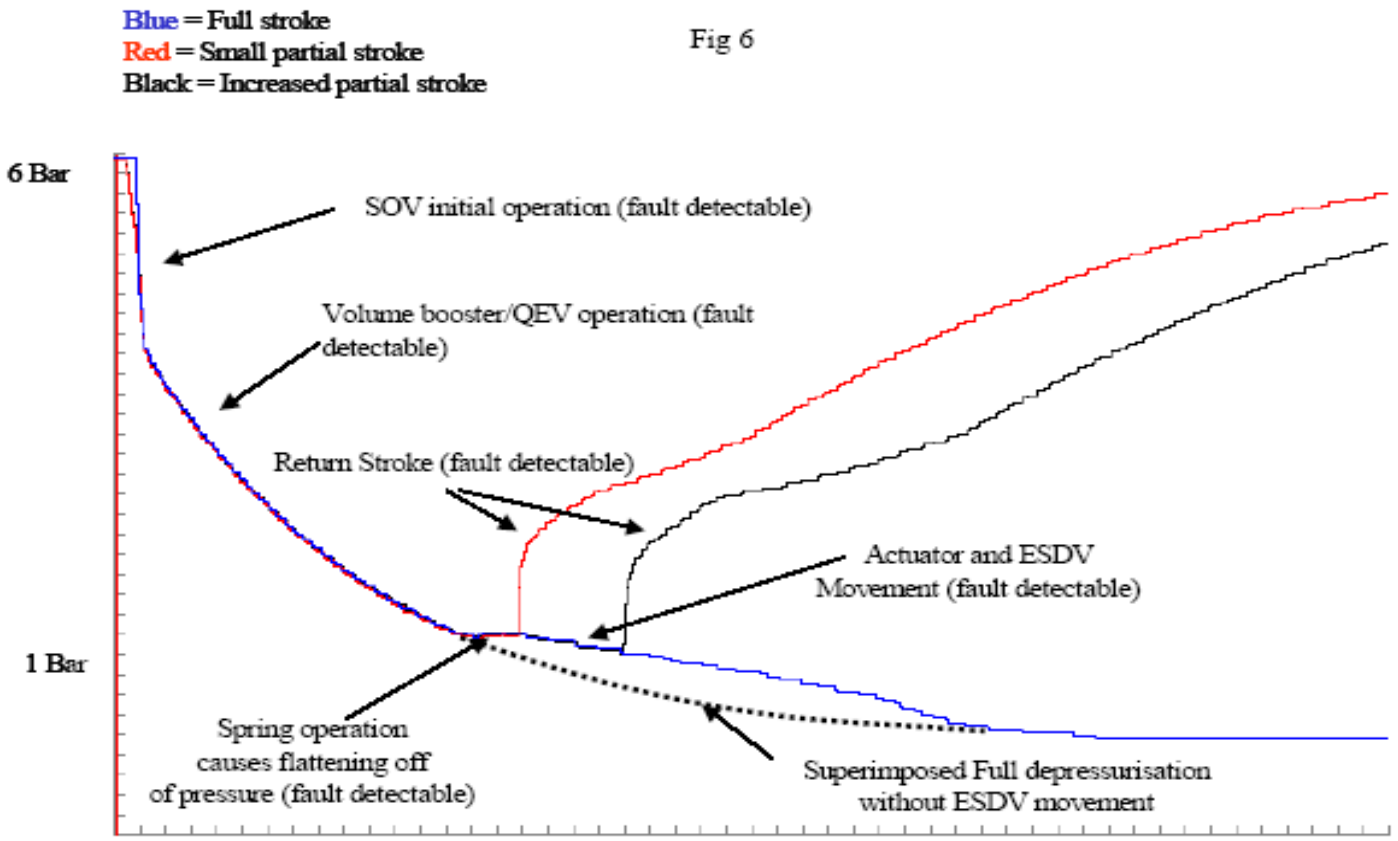
✓ **An accelerated (partial) proc**

≠ **<u>Not</u> an automatic diagnostic**

Extending Full Stroke Test Interval



Valve Signature



- Valve signatures show their response over time.
- This is achieved by capturing the valve position in time with respect to the incoming pressure.
- The signature of the ‘as new’ valve when it was commissioned can be compared with the signature taken during subsequent testing to predict if and how fast the valve is degrading.

Partial Valve Stroke Test (PVST)

Perceived Advantages:

- Provides an improvement to the SIL of the SIF, particularly for SIL 2 SIFs where it is not possible to meet the SIL 2 PFD requirement with a single valve.
- Provides predictive maintenance data. The valve signature during PVST could be used to identify slow movement in the valve that could escalate to valve sticking in the future.
- Allow extension of the full stroke test interval.
- By setting lower positioner pressures, quick valve response could be achieved to meet Process Safety Time requirements.
- Reduce the need for valve bypasses.

Partial Valve Stroke Test (PVST)

Disadvantages:

- By adding a positioner (or other PVST devices) the total valve assembly becomes less reliable and could introduce increased nuisance valve tripping.
- The main drawback of PVST systems is the increased probability of accidental activation of the safety system causing a shutdown.
  - This is generally the primary concern of operators with regard to PVST and for this reason many PVST systems remain dormant after installation.
  - Therefore it must be ensured that partial valve movement does not have a significant impact on the process which could cause a process shutdown
- Several refineries have decommissioned their PVST due to nuisance failures without investigating the reasons for nuisance trips or providing alternatives to the PVST solution.
- Frequent testing of these valves promotes wear and tear and increases potential leakage and failure.

It is important to select the correct PVST configuration and devices.

Partial Valve Stroke Test (PVST)

PVST is not practical in all applications:

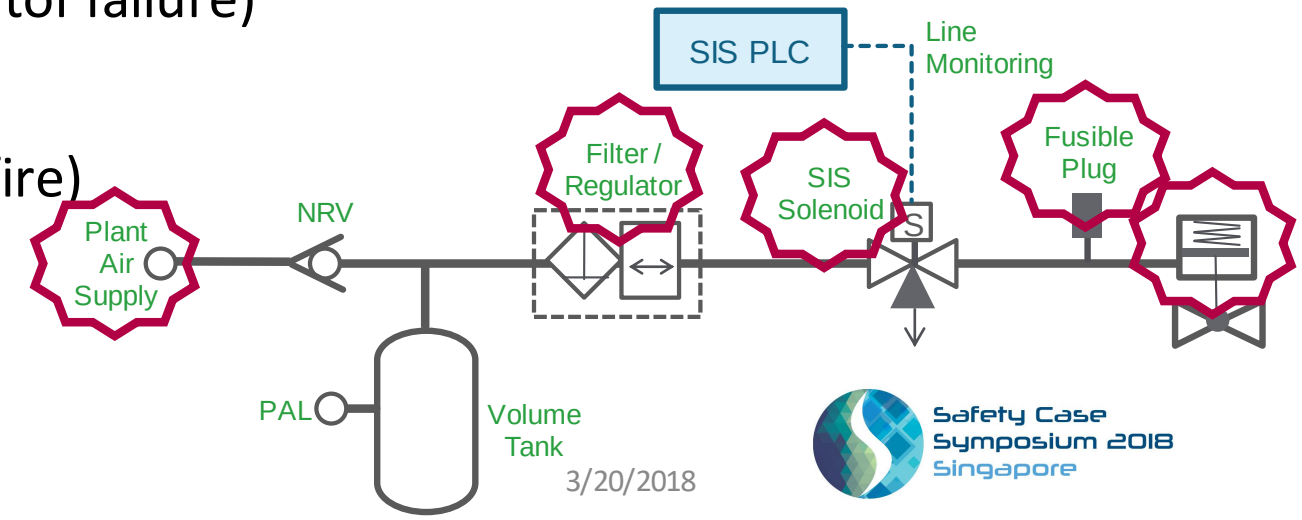
- Normally closed valves (partial opening of the valve may introduce hazardous or unwanted scenario).
- Use of PVST where regular full stroke testing is possible (e.g. online testing is possible without interrupting the process). Since PVST does not provide complete test coverage, additional cost of instrumentation and may introduce additional nuisance tripping, why implement where benefits are minimal?

Energize to Trip Systems

- Traditionally most safety functions are designed to be de-energize to trip (i.e. fail safe).
- This is a safe configuration but less reliable since any loss of power (e.g. electrical/pneumatic) will result in a trip.
- Safe failure of valves in some applications could result in significant hazards, in these cases energize to trip may be suitable. Examples include:
  - Boiler feedwater supply (fail open, close on high level)
  - Boiler steam header outlet / let down valves
  - Purge valves (e.g. nitrogen purge)
  - Deluge and emergency cooling valves

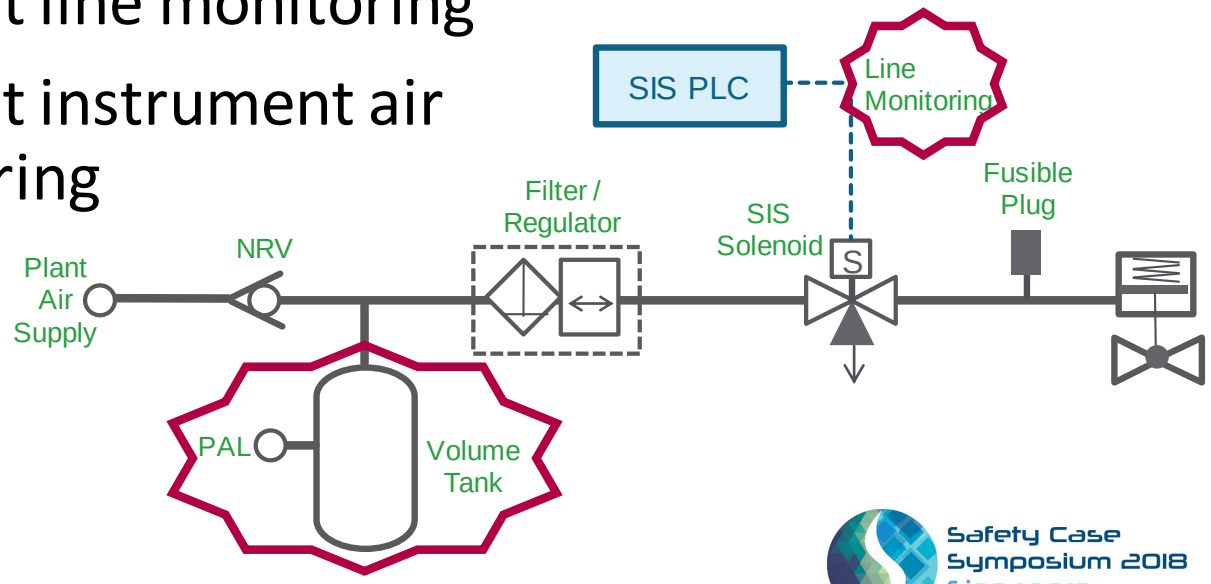
Energize to Trip Systems

- Since energize to trip functions are not fail safe design, extra care must be taken to mitigate the increased sources of dangerous failure.
- A Failure Modes and Effects Analysis (FMEA) should be performed to carefully evaluate the sources of dangerous failures and ensure they are suitably mitigated.
- Additional sources of dangerous failure for pneumatic valves include:
  - Insufficient plant instrument air (compressor failure, excessive demand in plant)
  - Restricted air flow (filter blockage, regulator failure)
  - Solenoid coil burnt-out
  - Thermal fuse venting (due to leakage or fire)
  - Valve diaphragm failure



Pitfalls in designing energize to trip systems

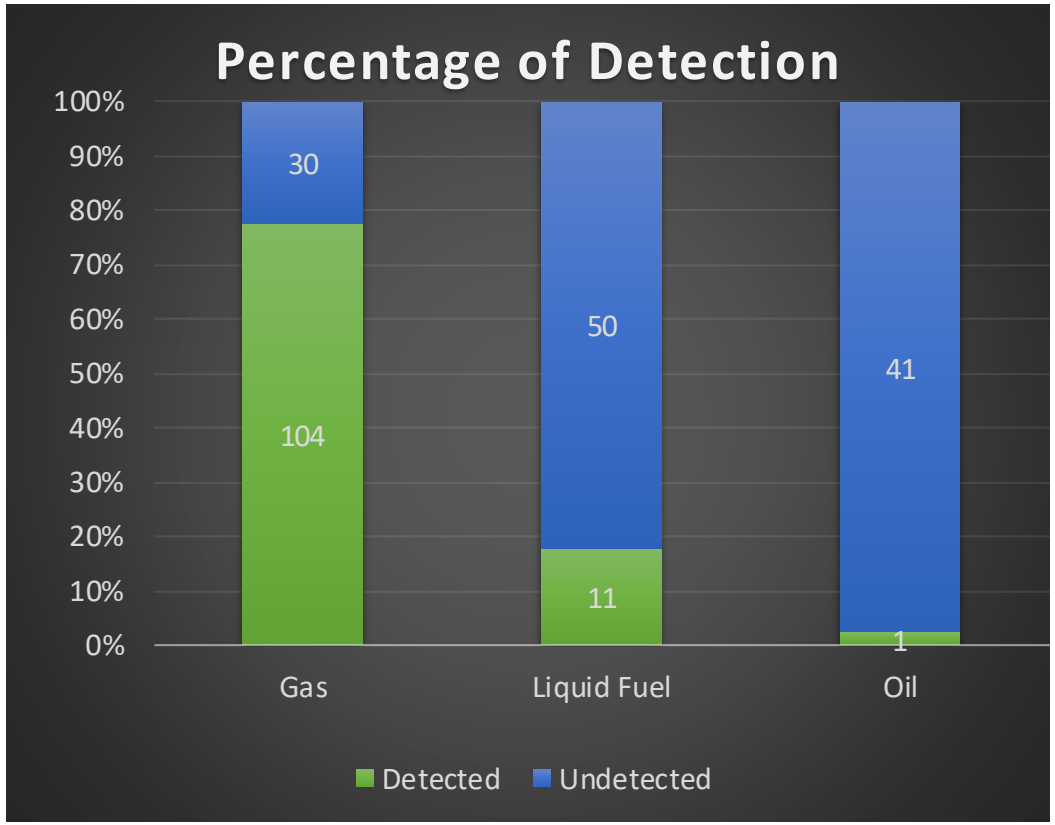
- Only use energize to trip for correct applications, not just to improve reliability.
- IEC 61511-1 Ed.2 clause 11.6.2 – “Energize to trip circuits shall apply means to ensure circuit and power supply integrity.”
  - Do not use energize to trip without line monitoring
  - Do not use energize to trip without instrument air accumulator and pressure monitoring

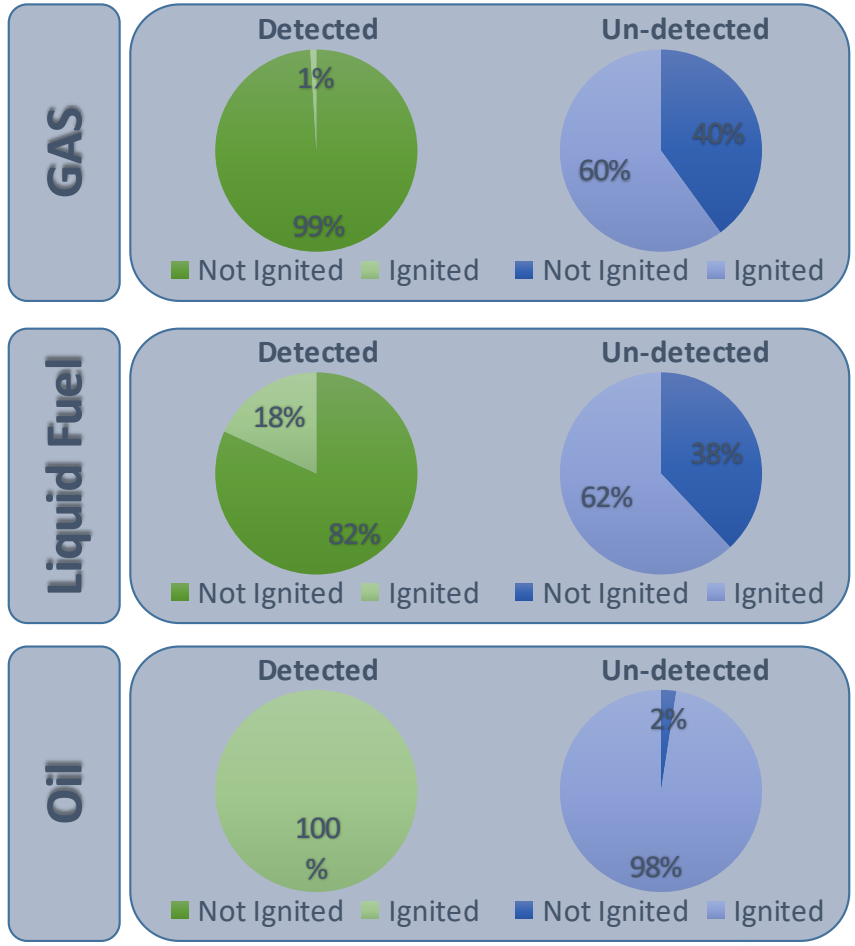


Fire and Gas Systems (FGS)

- IEC 61508 and IEC 61511 do not mention anything about FGS.
- FGS provide risk mitigation whereas SIS provide risk prevention.
- Independence is required between the prevention layer (SIS) and mitigation layer (FGS).
- Guidelines are provided in both standards for assigning SIL for prevention layers (SIS) but not for mitigation layers (FGS).
- There is no clear indication that the FGS is a safety function.
- FGs is designed to be energized to trip and not de-energized to trip, this is unlike most safety instrumented systems. This means FGS is designed with a focus on high reliability and less integrity.

HSE Report of Gas Detector Performance





Pitfalls in designing Fire and Gas Systems

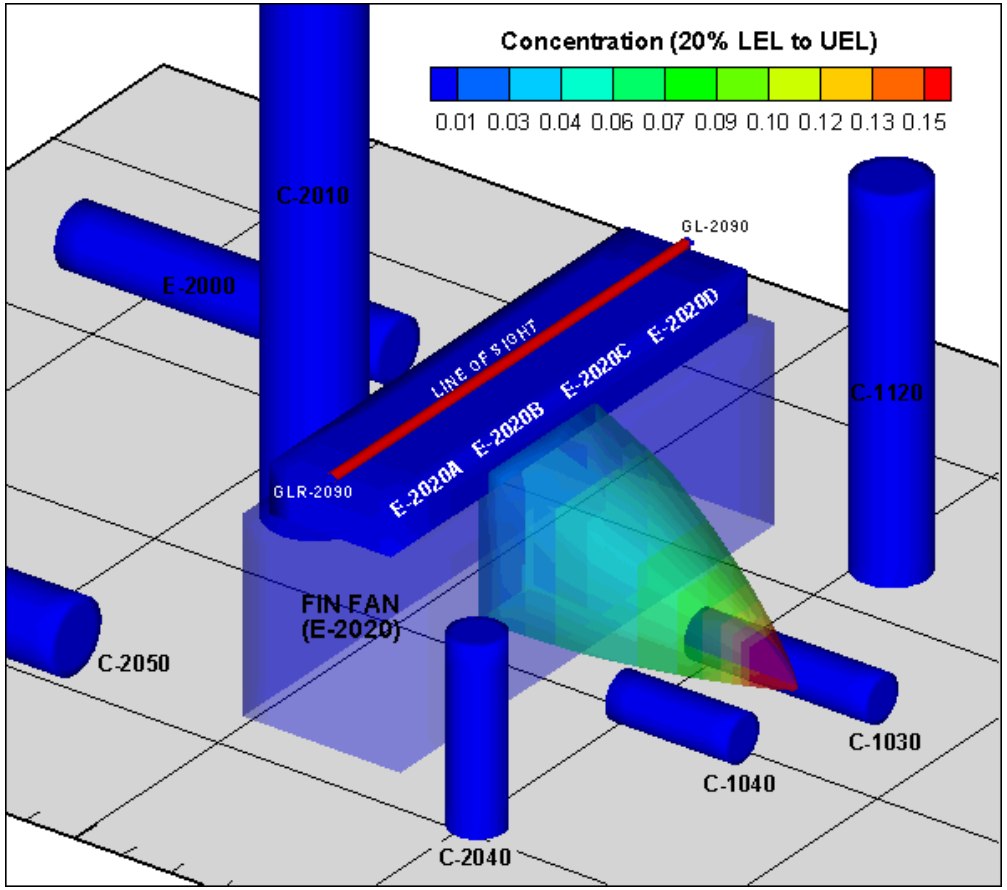
- In gas detection system sensors and final element may function properly, but they may not mitigate the hazards because:
  - Gas sensors fails to detect gas release because incorrect position of the sensors.
  - Wind may dilute the gas before it can be detected.
  - No sufficient detectors (coverage).
- As a result it would be inaccurate to consider PFDavg for a gas detection system as purely the hardware integrity of the different components.

Therefore, calculation of PFDavg based on device failure rates will not cover the total effectiveness of the system.

Detector Converge Mapping / Gas Dispersion Modelling

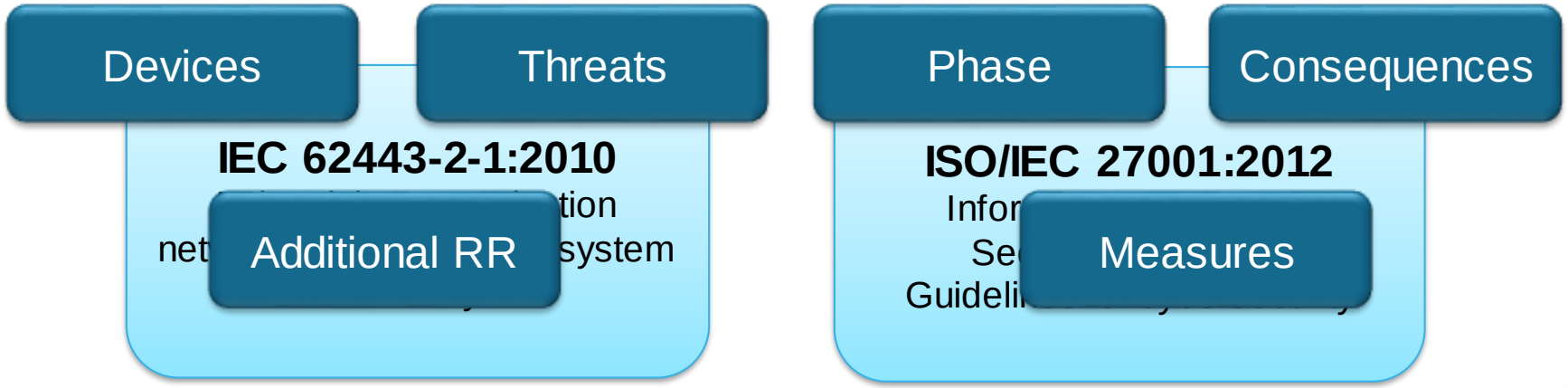
- 20% LEL alarm setting
- 25 mm hole diameter
- 20% LEL cloud boundary
- Still gas undetected and no trip

The 20% LEL pressurized release vapor envelope is expected to stop at the mesh wall of the fin fan structure, which is approximately 12 meters from M2 nozzle. The vapor will continue to travel, disperse and mix with air underneath the fin fan, where the lower concentration vapor will be blown vertically upwards by the fin fans and will intersect the line gas detectors GLR-2090. However, the existing line of sight gas detector may not be able to detect the vapour, as the vapour concentration may have been reduced to less than 20% LEL.



Requirement in Cyber Security

- A new sub-clause has been introduced in the process and risk assessment section of IEC61511 edition 2.
- A Security Risk Assessment shall be carried out on the SIS and its associated devices.
- And the assessment should cover:



A problem has been detected and Windows has been shut down to prevent damage to your computer.

DRIVER_IRQL_NOT_LESS_OR_EQUAL

If this is the first time you've seen this Stop error screen, restart your computer, If this screen appears again, follow these steps:

Check to make sure any new hardware or software is properly installed. If this is a new installation, ask your hardware or software manufacturer for any Windows updates you might need.

If problems continue, disable or remove any newly installed hardware or software. Disable BIOS memory options such as caching or shadowing. If you need to use Safe Mode to remove or disable components, restart your computer, press F8 to select Advanced Startup Options, and then select Safe Mode.

Technical information:

*** STOP: 0x000000D1 (0x0000000C,0x00000002,0x00000000,0xF86B5A89)

*** gv3.sys - Address F86B5A89 base at F86B5000, DateStamp 3dd991eb

Beginning dump of physical memory
Physical memory dump complete.
Contact your system administrator or technical support group for further assistance.

Thank You

Tracy Lau

Regional Business Development Manager for Safety

Schneider Electric South East Asia

Safety Case Symposium 2018 Singapore

www.SafetyCaseSymposium.com

Life Is On | Schneider Electric