Functional Safety in Industrial Application

Modifications in the Latest Revision of the IEC 65108 and the Consequences for Final Elements like Valves/Actuator Combinations

mokveld

Elango Pushpalingam - TUV Functional Safety Engineer ID 2212/10
Regional Sales Manager – South & Southeast Asia.

Functional Safety in Industrial Application

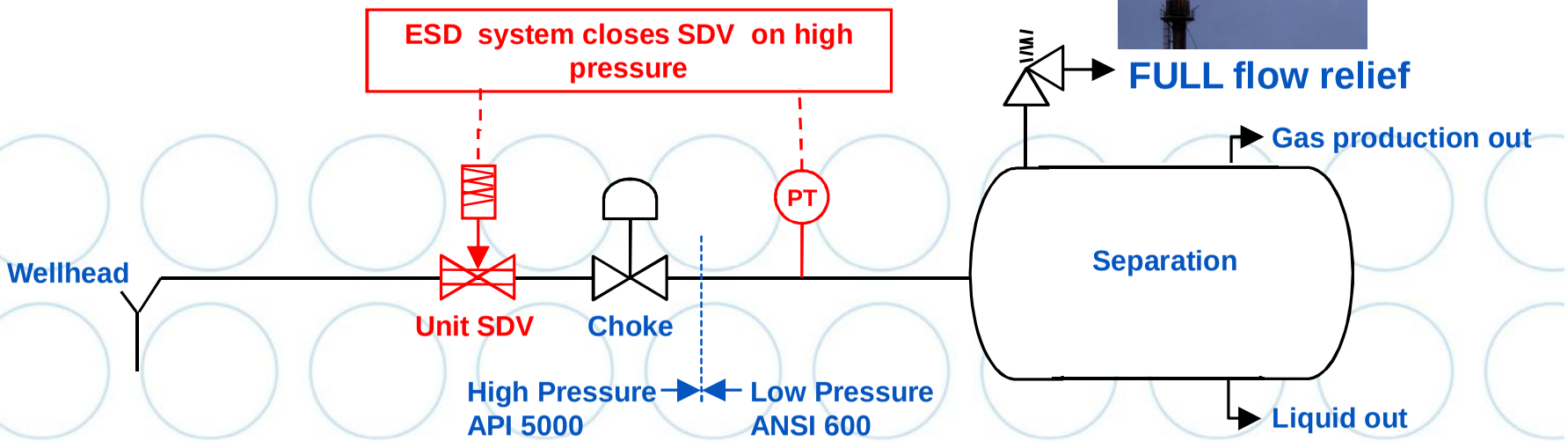
- This presentation will focus on the modifications in the IEC 61508 related to the final elements

- It does not cover all modifications / additions or revisions in the standard.

mokveld

1950: Over-pressure protection on gas wells

- Prescriptive API RP 14C



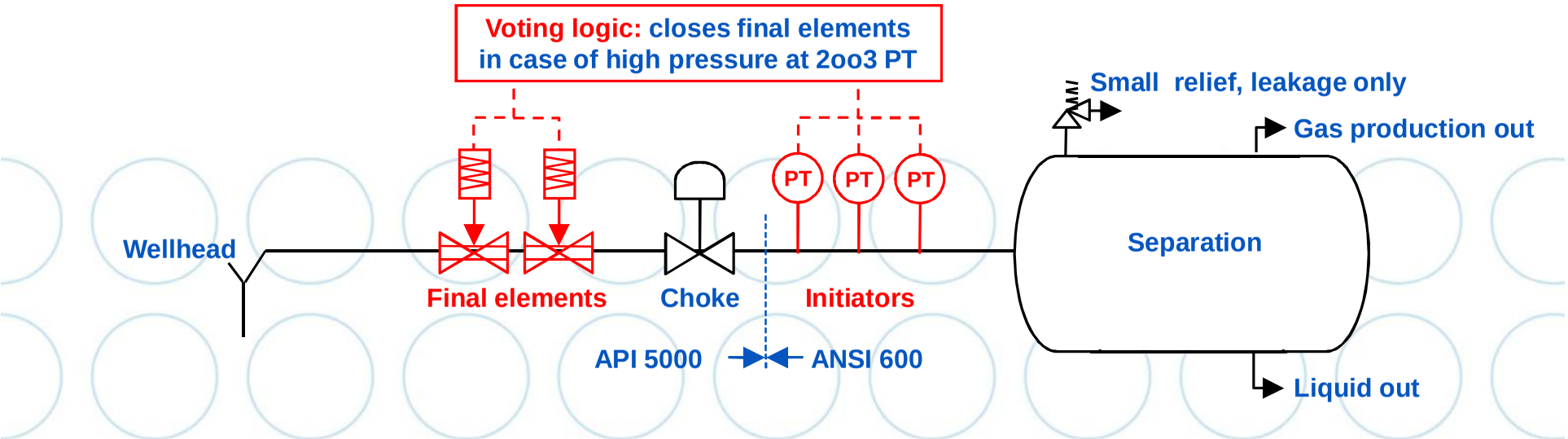
In case the outlet of the separator blocks:

- The Unit SDV closes,
- The relief is opened to flare, flare is sized for full flow

mokveld

1995: Over-pressure protection on gas wells

(No IEC 61508 and 11 yet)

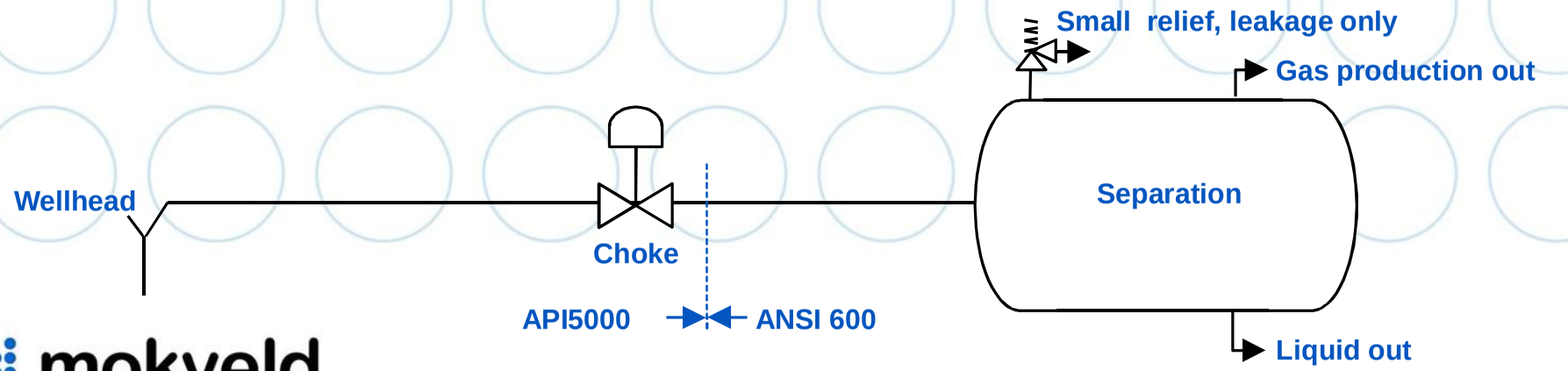


The full flow relief and flare system are replaced by
2 Safety Shut-down valves

mokveld

Using IEC 61508 on this example

- First a HAZOP and RISK analysis to define the required SIL level
- Assume overpressure is in 2 seconds
- Assume in case of over-pressure people will get injured or worse
- Resulting in SIL3 protection is required on the separator



mokveld

SIS Architecture

IEC 61508 HFT for type A equipment, like Final element

Safe failure fraction	Hardware fault tolerance		
	0 (1oo1)	1 (1oo2)	2 (1oo3)
< 60 %	SIL1	SIL2	SIL3
60 % - < 90 %	SIL2	SIL3	SIL4
90 % - < 99 %	SIL3	SIL4	SIL4
≥ 99 %	SIL3	SIL4	SIL4
NOTE A hardware fault tolerance of N means that N+1 faults could cause a loss of the safety function.			

Table 2 Architectural constraints on type A safety-related subsystems

Safe Failure Fraction: $(\Sigma\lambda_S + \Sigma\lambda_{Dd})/(\Sigma\lambda_S + \Sigma\lambda_{Dd} + \Sigma\lambda_{Du})$

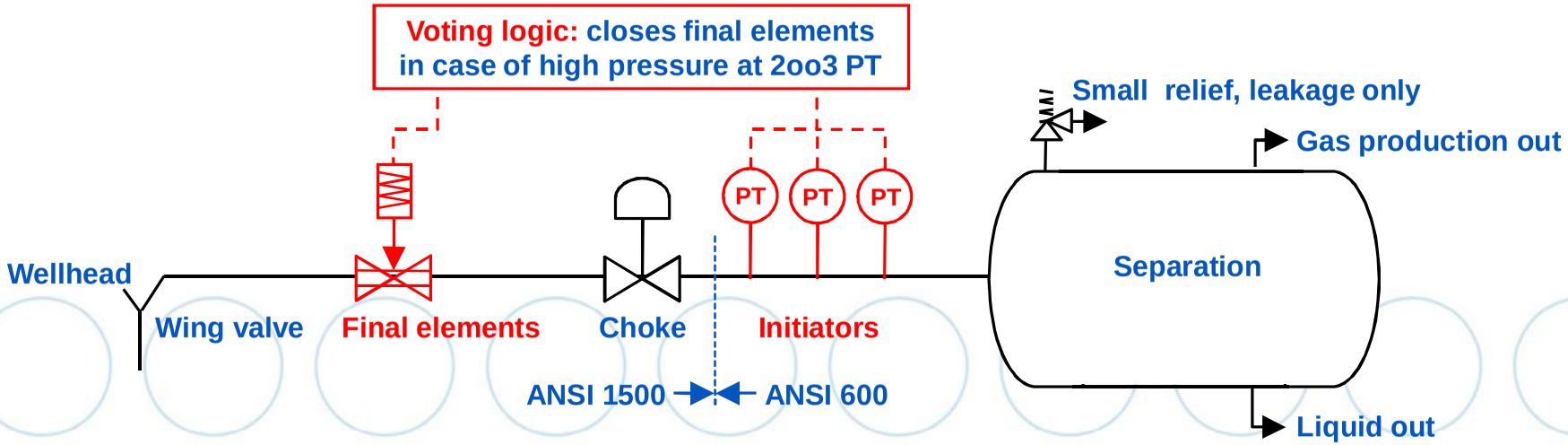
Where:

λ_S	=	Safe failure rate
λ_{Dd}	=	Dangerous detected **by diagnostics**
λ_{Du}	=	Dangerous undetected **by diagnostics**

mokveld

1998: IEC61508

In case SFF > 90% then IEC 61508 allows 1oo1 in SIL3



- "Old" prescriptive standards require redundancy (SSV + Full Flare)
- Partial Stroke Test devices and optimistic Safe Failure assessment generate high SFF's
- Pushing IEC to limit: No redundancy 1oo1 Final element

mokveld

2003: IEC 61511

Required redundancy final elements

Safety Integrity Level	Architecture for final elements and sensors		Architecture when "proven in use"	
SIL	**HWFT**	**Redundancy**	**HWFT**	**Redundancy**
1	0	1oo1	0	1oo1
2	1	1oo2	0	1oo1
3	2	1oo3	1	1oo2
4	Special requirements, refer to IEC 61508			

However the design / installation will be based on IEC61508.

mokveld

2010: IEC 61508

No HFT reduction by diagnostics

7.4.4.1.1 With respect to the hardware fault tolerance requirements

a) a hardware fault tolerance of N means that N+1 is the minimum number of faults that could cause a loss of the safety function (for further clarification see Note 1 and Table 2 and Table 3). In determining the hardware fault tolerance no account shall be taken of other measures that may control the effects of faults such as diagnostics;

- HFT should not be reduced based on diagnostics devices.

mokveld

2010: IEC 61508

Further definition of Diagnostics test interval

7.4.4.1.5 When estimating the safe failure fraction of an element which,

– has a hardware fault tolerance greater than 0, and which is implementing a safety function, or part of a safety function, operating in high demand mode or continuous mode of operation; or,

– is implementing a safety function, or part of a safety function, operating in low demand mode of operation, credit shall only be taken for the diagnostics if the sum of the diagnostic test interval and the time to perform the repair of a detected failure is less than the MTTR used in the calculation to determine the achieved safety integrity for that safety function.

- Note : This is the longest interval specified.
- On these short intervals **no diagnostics possible on final elements**. Partial stroke every 8 hours not feasible.

mokveld

2010: IEC 61508

Safe Failures more stringent defined

safe failure

failure of an element and/or subsystem and/or system that plays a part in implementing the safety function that:

a) results in the spurious operation of the safety function to put the equipment under control (or part thereof) into a safe state or maintain a safe state; or

b) increases the probability of the spurious operation of the safety function to put the equipment under control (or part thereof) into a safe state or maintain a safe state

mokveld

2010: IEC 61508

Safe Failures more stringent defined

no part failure

failure of a component that plays no part in implementing the safety function

NOTE: The **no part failure is not used for SFF calculations**

no effect failure

failure of an element that plays a part in implementing the safety function but has no direct effect on the safety function

NOTE 1: The no effect failure has by definition no effect on the safety function so it cannot contribute to the failure rate of the safety function.

NOTE 2 The **no effect failure is not used for SFF calculations**.

mokveld

2010: IEC 61508

Safe Failures more stringent defined

- This means for a final element one of the few safe failures is a leaking seal in the actuator.

- Valves only probably do not have safe failures

- This has a big effect on the safe failure fraction (SFF) calculation.

mokveld

2010: Safe failure Fraction of a final element?

- $(\Sigma\lambda_S + \Sigma\lambda_{DD})/(\Sigma\lambda_S + \Sigma\lambda_{DD} + \Sigma\lambda_{DU})$
- λ_S significant reduction
- λ_{DD} Now zero while no diagnostics?
- λ_{Du} remains unchanged

- Safe Failure Fraction of Final elements shall reduce significantly due to new revision

IEC 61508 HFT for type A equipment, like Final element

Safe failure fraction	Hardware fault tolerance		
	0 (1oo1)	1 (1oo2)	2 (1oo3)
< 60 %	SIL1	SIL2	SIL3
60 % - < 90 %	SIL2	SIL3	SIL4
90 % - < 99 %	SIL3	SIL4	SIL4
≥ 99 %	SIL3	SIL4	SIL4

NOTE A hardware fault tolerance of N means that N+1 faults could cause a loss of the safety function.

Table 2 Architectural constraints on type A safety-related subsystems

mokveld

2010: Partial Proof Tests are not preferred.

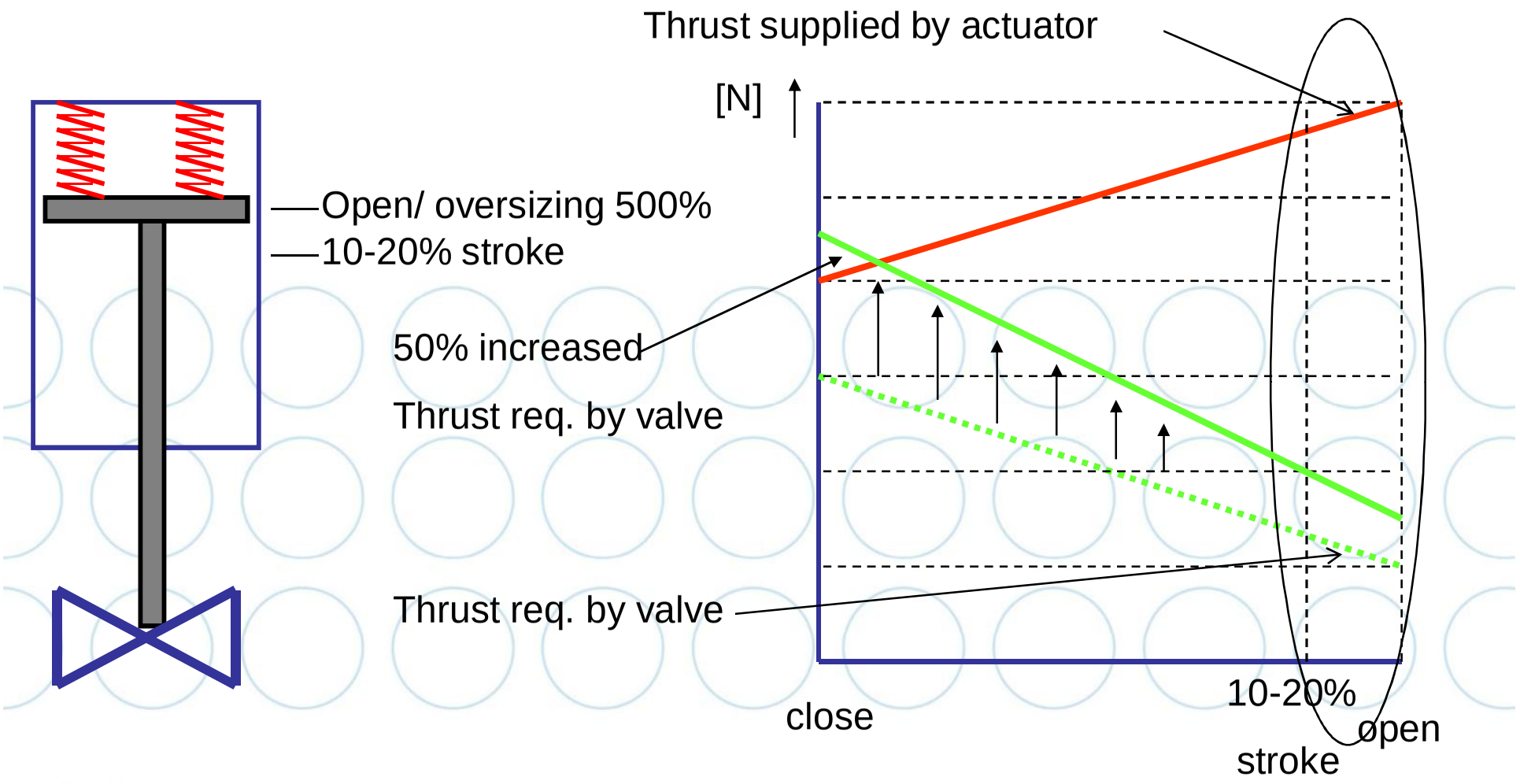
3.8.5 proof test

periodic test performed to detect dangerous hidden failures in a safety-related system so that, if necessary, a repair can restore the system to an “as new” condition or as close as practical to this condition

NOTE 2 The effectiveness of the proof test will be dependent both on failure coverage and repair effectiveness. In practice detecting 100% of the hidden dangerous failures is not easily achieved for other than low-complexity E/E/PE safety-related systems. This should be the target.

- Detecting 100 % of the hidden dangerous failures should be the target.
- This implicates that a specific device to perform partial proof tests is not preferred

mokveld


Thrust supplied by actuator
[N]
Open/ oversizing 500%
10-20% stroke
50% increased
Thrust req. by valve
Thrust req. by valve
close
10-20%
open
stroke

mokveld

HW Compliance two “schools”

Probability (Fr+Jpn) vs Architecture (D+UK)

SFF has no mathematical meaning vs Failure data is too weak

- *7.4.4 ...the highest SIL that can be claimed for a Safety Function is limited by the hardware safety integrity constraints through either one of the two possible routes*
- *1H Based on HFT and SFF concepts (ie. IEC61508 1998)*

or

- *2H Based on component reliability data from feedback from end users, increased confidence levels and HFT.*

When selecting 2H the reliability uncertainties of the failure data shall be taken into account when calculating PFDav. (ie. IEC61511 2003)

mokveld

2010: HFT increased for FE in route 1H IEC61508?

- Diagnostics not possible / not applicable
- Safe Failure Fraction not for mechanical equipment
- Safe Failure Fraction seriously lowered by new revision.

Safe failure fraction	Hardware fault tolerance		
	0 (1oo1)	1 (1oo2)	2 (1oo3)
< 60 %	SIL1	SIL2	SIL3
60 % - < 90 %	SIL2	SIL3	SIL4
90 % - < 99 %	SIL3	SIL4	SIL4
≥ 99 %	SIL3	SIL4	SIL4

NOTE A hardware fault tolerance of N means that N+1 faults could cause a loss of the safety function.

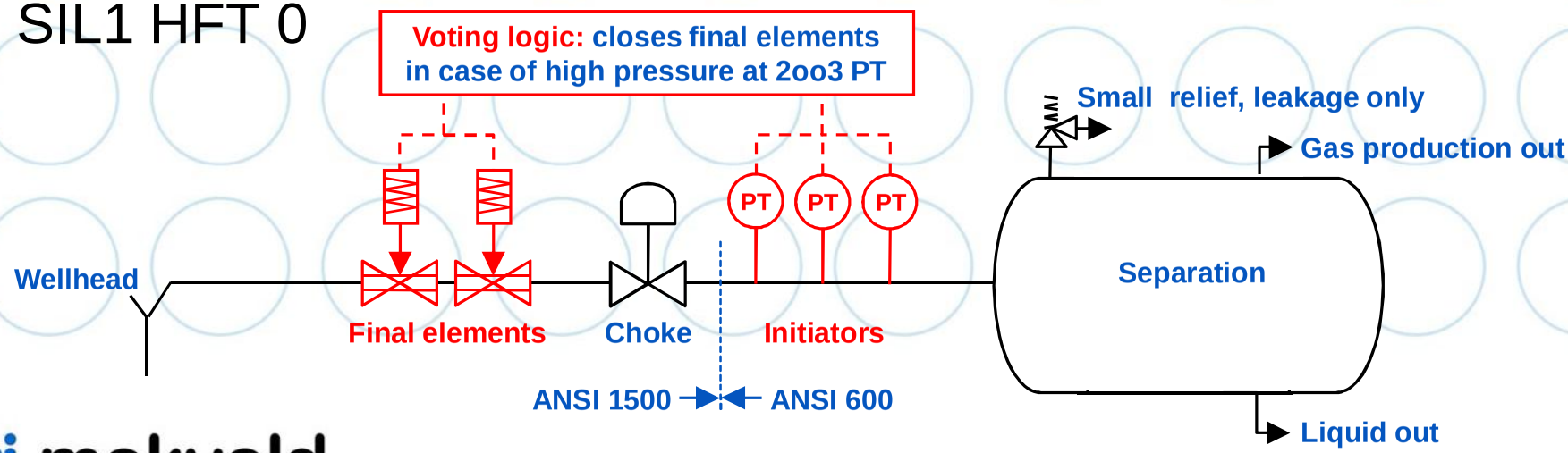
Table 2 Architectural constraints on type A safety-related subsystems

mokveld

2010: HFT increased for FE in route 2H IEC61511?

Proven in use concept

- For type A and B, where B has minimum DC of 60%.
- SIL4 HFT 2
- SIL3 HFT 1
- SIL2 HFT 1 High demand continuous mode
- SIL2 HFT 0 Low demand mode
- SIL1 HFT 0



mokveld

2010: Proven in use also defined in 61508

7.4.10.1 An element shall only be regarded as proven in use when it has a **clearly restricted and specified functionality** and when there is adequate documentary evidence to demonstrate that the likelihood of any dangerous systematic faults is low enough that the required SIL is achieved. Evidence shall be based on **analysis of operational experience of a specific configuration** of the **element** together with suitability analysis and testing **within the intended application**.

7.4.10.2 The documentary evidence shall demonstrate that the **previous conditions** of use of the specific element are **the same as,** or sufficiently close to, those that will be experienced by **the element in the safety-related system**;

mokveld

2010: Proven in use also defined in 61508

7.4.10.3 **When there is any difference** between the previous conditions of use and those that will be experienced in the safety-related system, then **an impact analysis on the differences shall be carried out**…

7.4.10.4 A proven in use safety justification shall be documented that the element supports the required safety function with the required systematic safety integrity. This shall include

- the suitability analysis and testing of the element for the intended application;
- the **demonstration of equivalence between the intended operation and the previous operation experience**, including the impact analysis on the differences;
- the statistical evidence.

mokveld

Proven in use in practice

- Certificates to be verified, Reports to be read
- Experience in Oil and Gas on similar applications required.
  (e.g. experience in abrasive mining applications not valid)
- Response times same as in the safety system
- Interaction of components (combination of Valve + Actuator) proven?
- Element would be valve + actuator
- Requires specific attention of engineer / end-user.

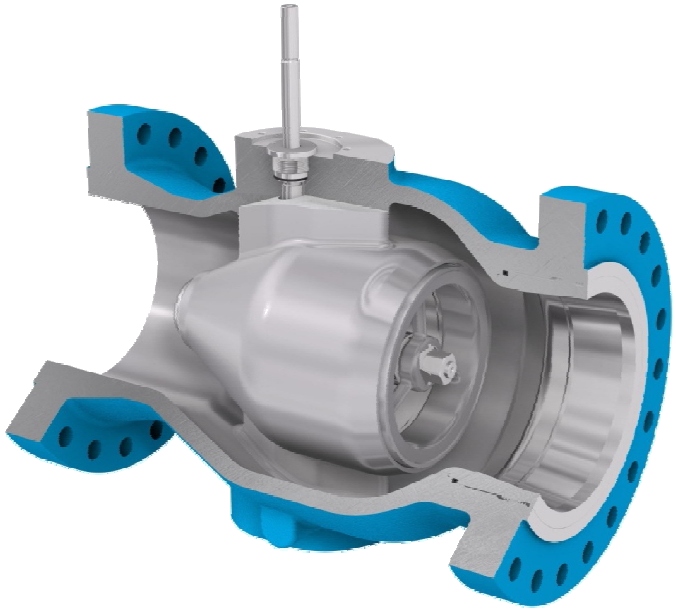
mokveld

Summary 61508 2010 on Final Elements

- Major impact on Safe Failure Fraction
- Impact on Partial Stroking
- Basically mechanical equipment requires Route 2H
- Proven in use required
- SIL3 HFT 1 (1oo2)

mokveld

Axial on-off valve



‘on’ function

‘off’ function

Axial excellence

mokveld

Axial on-off valve: main benefits summarized

Operational benefits

- Opens easily against full differential pressure (fully pressure balanced piston design)
- Reliable tight shut-off function (dual protection of main seal)
- Negligible pressure loss as result of streamlined flow path through full-port expanded body

Significant cost savings

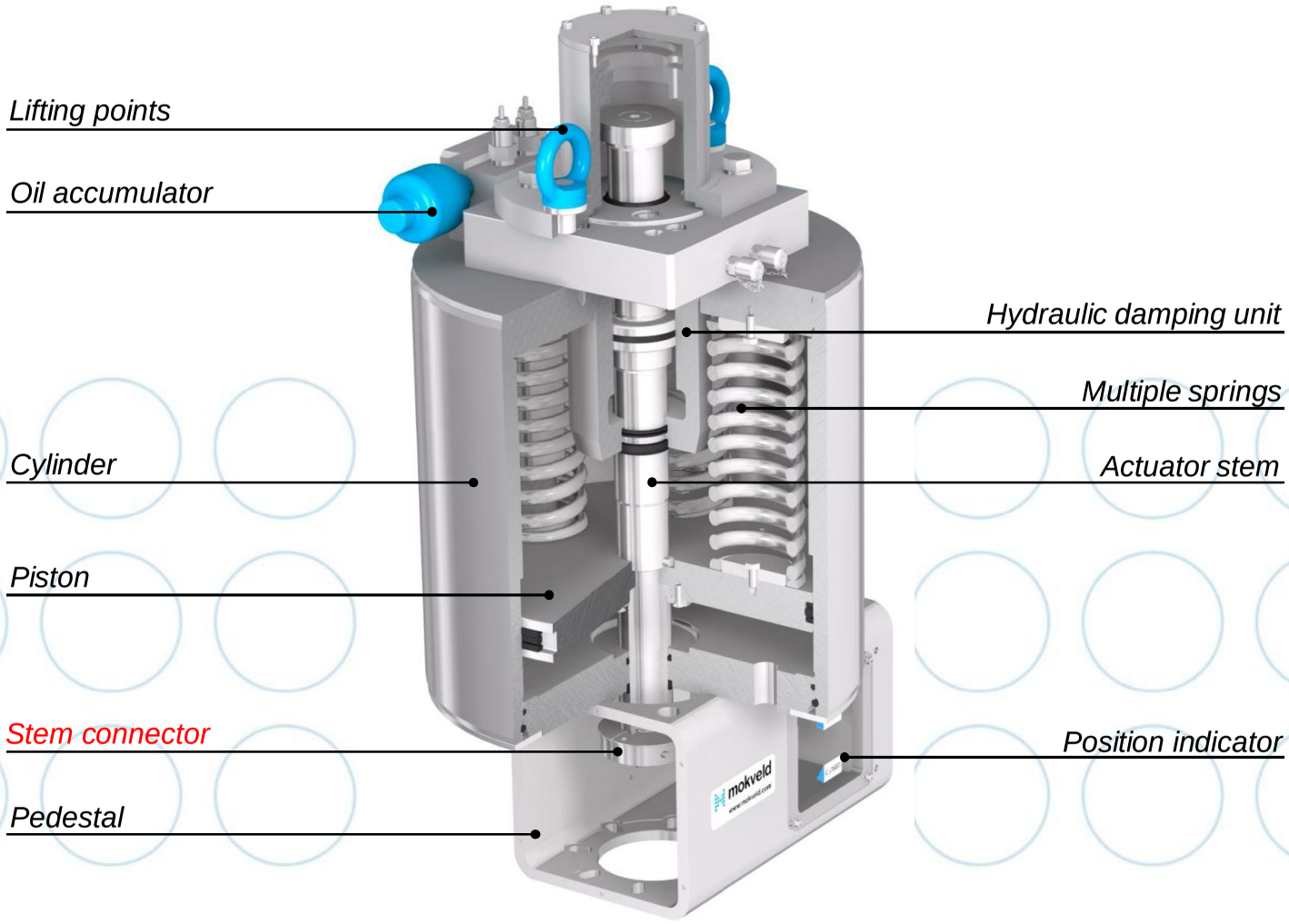
- No by-pass system and down time for pressure equalization
- Compact and low weight valve design with small actuators
- Reduced total cost of ownership

Safety benefits

- Quick and reliable open and close operation
- Dependable reliability data (HIPPS)
- Fire-safe certified

mokveld

Pneumatic actuator (double acting or spring return)



mokveld

Introduction into HIPPS

Mokveld history in pressure protection safety applications:

- Final element (valve + actuator) certified since 1974 in acc. DIN 3381 / EN14382 / EN 12186
- Third Party (AEA) validated failure rates since 1995
- TUV validated for SIL3 since 2002
- Failure data for clean duty and unclean duty
- Integrated mechanical HIPPS since 1974
- Integrated electronic HIPPS since 2000

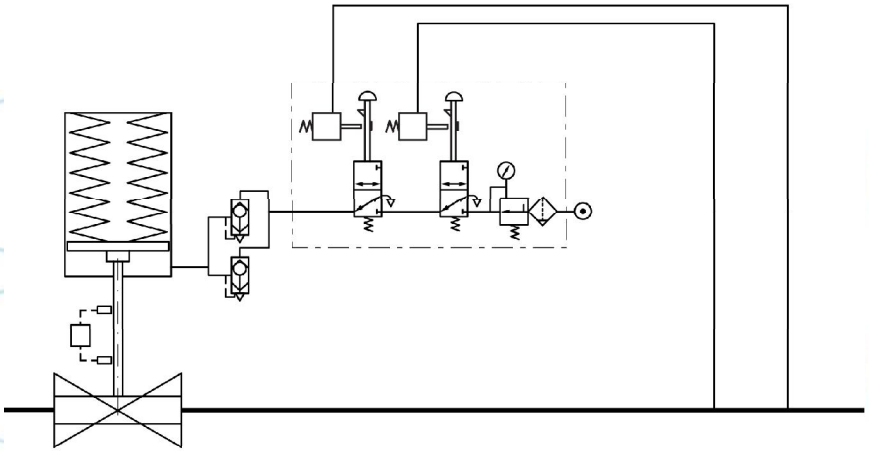
Failure rate final element delivering full stroke within 2 seconds:

- Unclean duty: λ = 2,98 E-4 / year
- Clean duty: λ = 1,63 E-4 / year
- SIL 3 and 4 can be achieved with a proof test interval of 1 year.

mokveld

Mokveld mechanical HIPPS

- Mechanical initiator with 1% accuracy
- Completely integrated safety shut-down system
- Stand-alone system operated with line gas without permanent gas consumption



Integral mechanical HIPPS 1oo2, pneumatic version

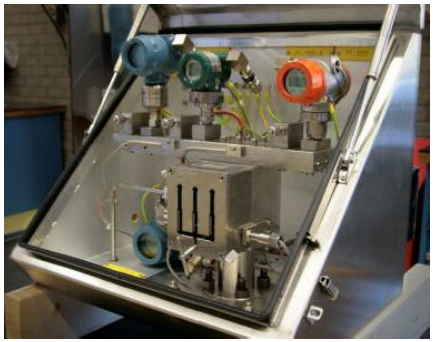
Mechanical initiator

Mechanical Hipps movie

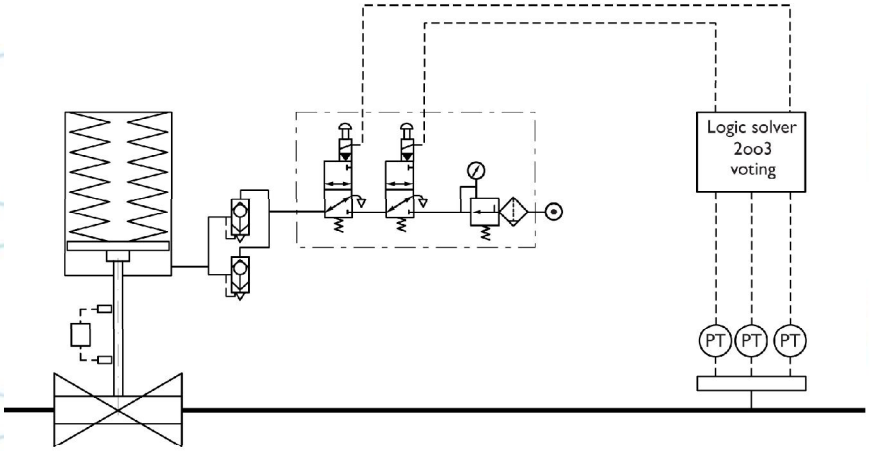
mokveld

Mokveld electronic HIPPS

- Safety pressure transmitters
- Hard-wired solid state (non-programmable) logic
- Fully fail safe



High integrity manifold block with key interlock system



Full electronic HIPPS 2oo3, pneumatic version

Voting logic

mokveld

Typical application reference

16” / ANSI 600 Axial On-Off Valves

Application	:	2 x 1oo2 Mechanical HIPPS protecting low pressure system from high pressure compressor
Challenge	:	Subsurface installation and long proof test interval
Location	:	VNG Verbundnetz Gas

mokveld

Typical application reference

6” / ANSI 900 Axial On-Off Valves

Application : 1 x 1oo2 Mechanical HIPPS protecting ANSI 900 pipeline against pressure from ANSI 2500 wellhead

Challenge : Compact design and low failure rate

Location : NAM Netherlands mobile production unit

mokveld

Typical application reference

16” / ANSI 900 Axial On-Off Valves

Application	:	1oo2 Electronic HIPPS protecting ANSI 600 onshore installation against pressure from ANSI 900 offshore pipeline
Challenge	:	Compact design and low failure rate
Location	:	Dong Denmark Nybro

mokveld

Thank you for your attention

mokveld

Elango Pushpalingam - TUV Functional Safety Engineer ID 2212/10
Regional Sales Manager – South & Southeast Asia.

Welcome to Presentation on Sonic Leak Detection System

NEXTGEN OIL & GAS PRIVATE LIMITED

About Us

Dodhia Group, ISO 9001 certified, broadened their spectrum by setting up a dedicated entity for each of its specialized products/systems

What began as a setup with initial investment of Rs.10 cr. Now valued at Rs.140 cr.

Dodhia Innovative Equipments Ltd. (DIEL) formed in 2009 with an idea to become high-quality distribution house offering

world-class products catering to needs of markets related to

SAFETY, DETECTION EQUIPMENTS & PROTECTIVE SYSTEMS.

This background gave an existence to Nextgen Oil & Gas Pvt. Ltd.

NEXTGEN OIL & GAS PRIVATE LIMITED

We are Distributors world leaders in Safety, Detection equipments, Protective Systems such as :

Company	Products
Tyco Thermal Controls – USA	MICC- Fire Survival Cable, Water & liquid hydrocarbon Leak detection system
Honeywell International USA	LHS Cable & Smoke detection & fire alarm systems
Indelac – France	Lightning Arrestor
Ansul Incorporated USA (TYCO Fire Protection Product)	Clear agent Gas Suppuration, Vehicle Fire suppuration Clean Agent Fire Extinguisher
Perma Pure- USAHALMA Group of Companies	Gas Sampling System, Instrumentation
Sky Petrochem	SPS, Turbine Oil, Oil additives,

we have joined hands with

Asel-Tech Technologia e Automacao Ltda, Brazil

To represent Their Products
on
Sonic Leak Detection System for Pipelines

List Of Clients

CLIENT	PROJECT	PIPELINE	LENGTH
PETROBRAS	Peroa - Cangoa	Multiphase	56 km subsea + 32 km buried
PETROBRAS	Manati	Multiphase	145 km subsea and buried
PETROBRAS	Tecarmo	Crude oil	8 km subsea
PETROAMAZONAS	Pañacocha	Multiphase	32 Km
ENAP	Bio Bio	Poliduct	6 lines, 9.6 km
BRASKEN	Camacari	Naphtha	2 lines, 40 km buried
USP-BRASIL	Laboratory	Water and Gas	1.5 km
LOGUM	Ribeirão Preto - Paulínia	Ethanol	200km, buried
ODEBREACH	Aquapolo	Water	2 lines,17km buried
SECRET CLIENT	Theft detection	Gasoline	267 km, buried

NEXTGEN
OIL & GAS PRIVATE LIMITED

Thank You

Level | Pressure | Flow | Temperature | Liquid Analysis | Registration | Systems Components | Services | Solutions

Wireless Technology

… for oil & gas industry

Hemal Desai

Endress+Hauser
People for Process Automation