

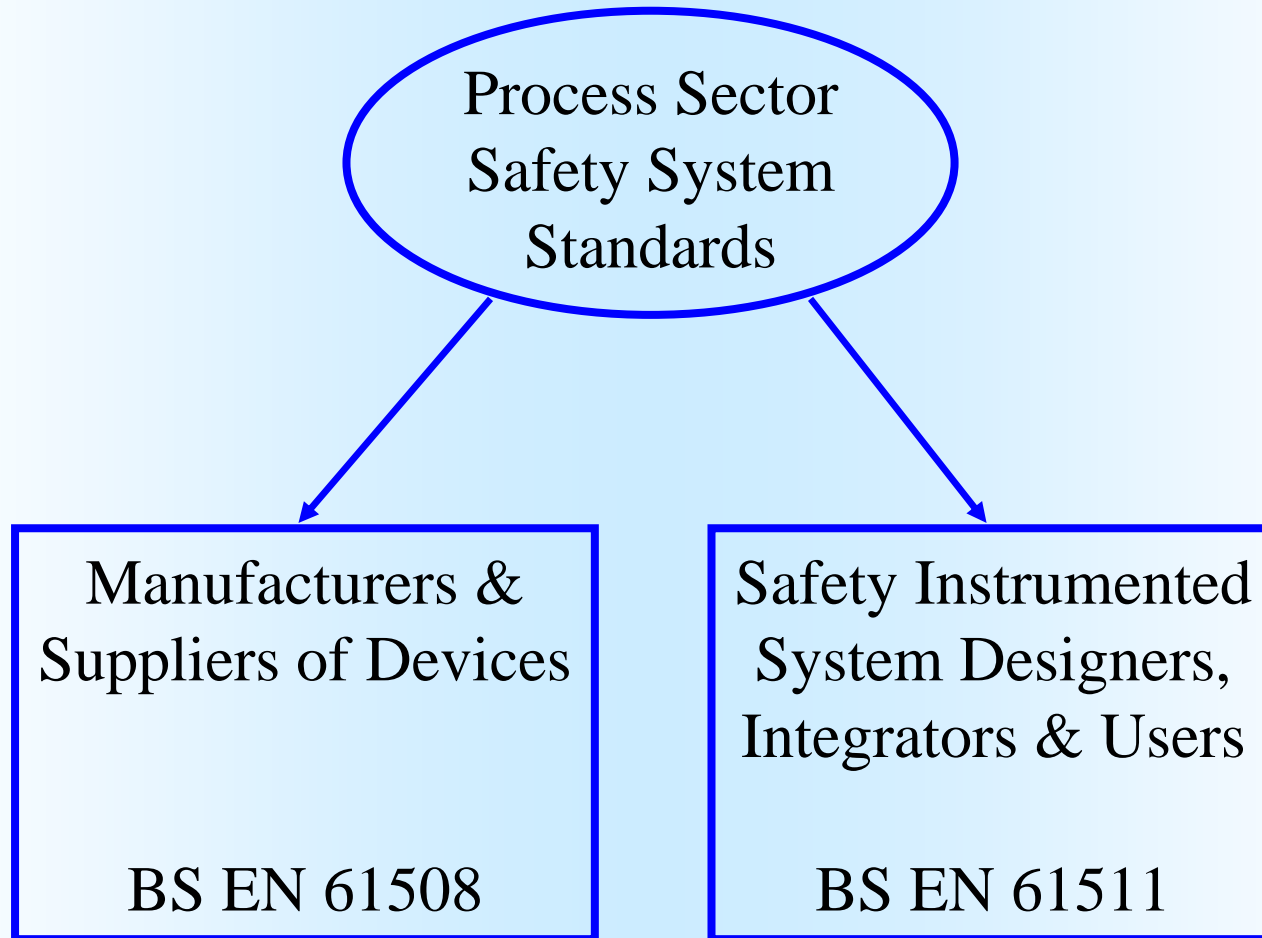
David Ransome
P&I Design Ltd

Automatic shut down
Industry example systems
& Methodology

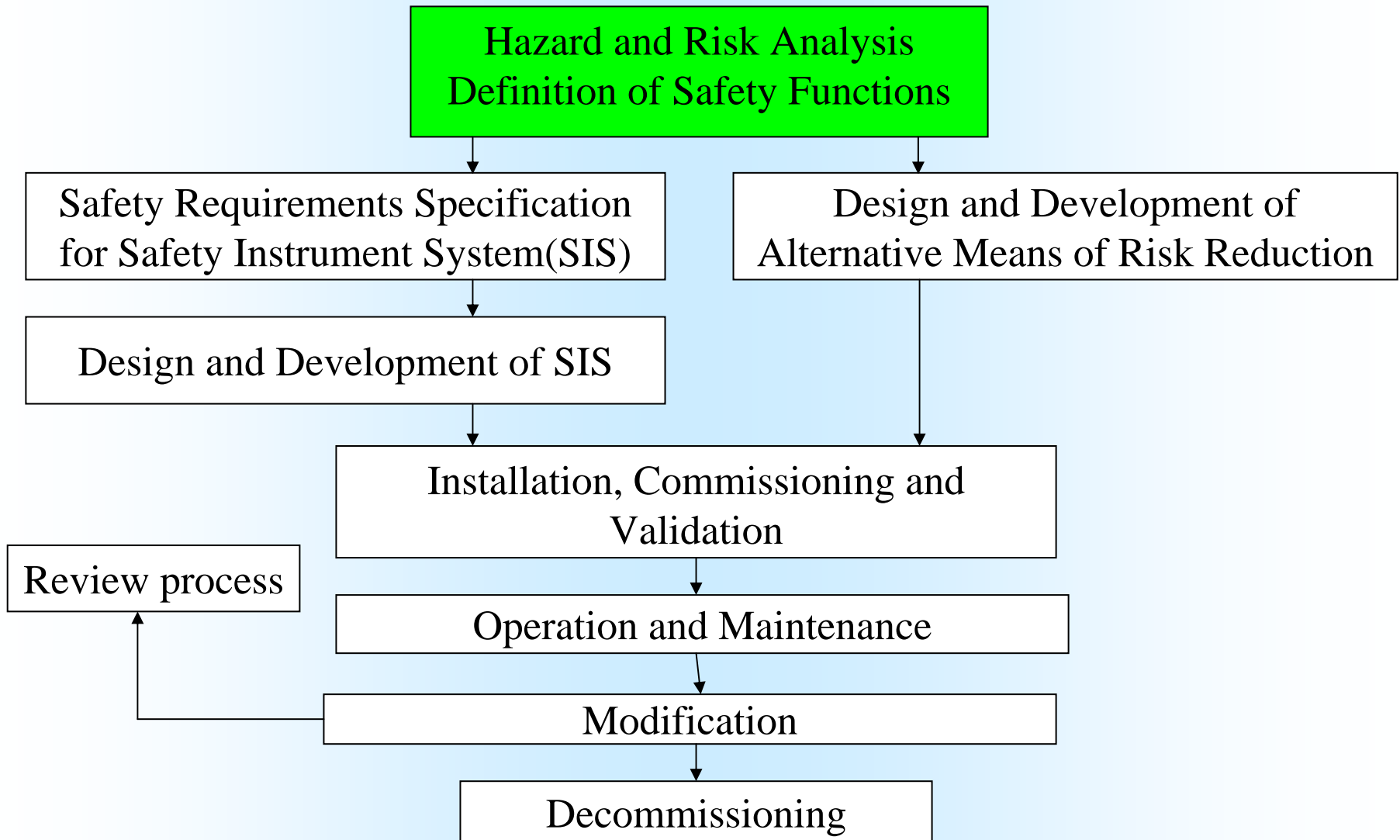
OBJECTIVES

1. To provide an overview of the BS EN 61511 Lifecycle approach for automatic shutdown systems with a brief description of what each stage requires
2. To illustrate the difference in types of facility – Rail, Ship & Pipeline (Refinery transfers are excluded from this presentation)
3. To discuss suitable methods to achieve automatic shutdown relevant to type of facility

BS EN 61508 – BS EN 61511



SAFETY LIFE CYCLE

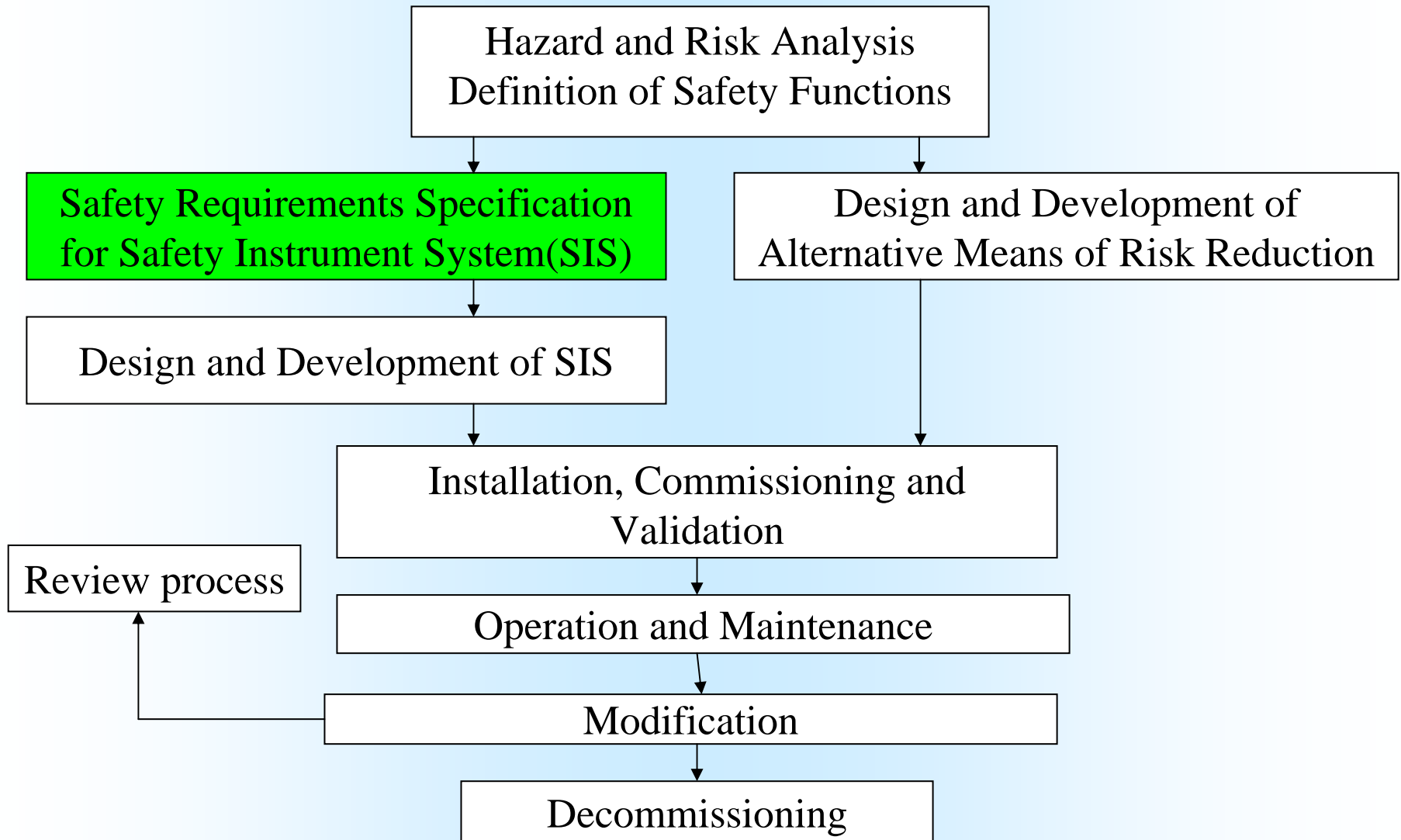


Hazard & Risk Assessment

BS EN 61511-1 Clause 8

- to determine the hazardous events
- to determine the sequence of events leading to the hazardous event
- to determine the process risks associated with the hazardous event
- to determine any requirements for risk reduction
- to determine the safety functions required
- to determine if any of the safety functions are safety instrumented systems

SAFETY LIFE CYCLE



Safety Instrumented Functions & Safety Requirements Specifications

Develop safety instrument system specification

Each safety function requires defining, stating exactly when and what should happen, together with the timescale of events (timescale is important to ensure that the SIS can perform the function required safely and within an appropriate time frame)

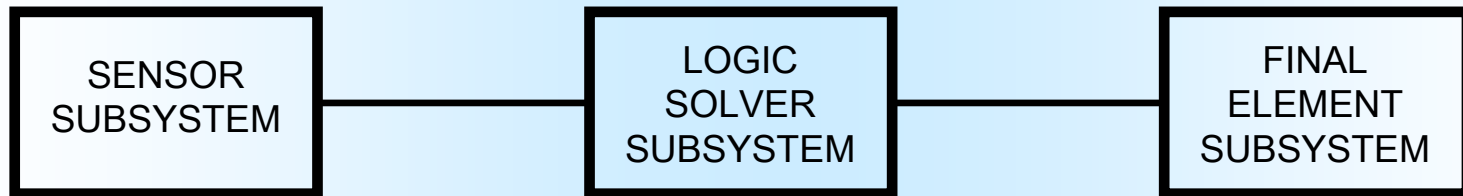
Each safety instrumented function should be allocated a Safety Integrity Level (SIL)

Safety Integrity Levels

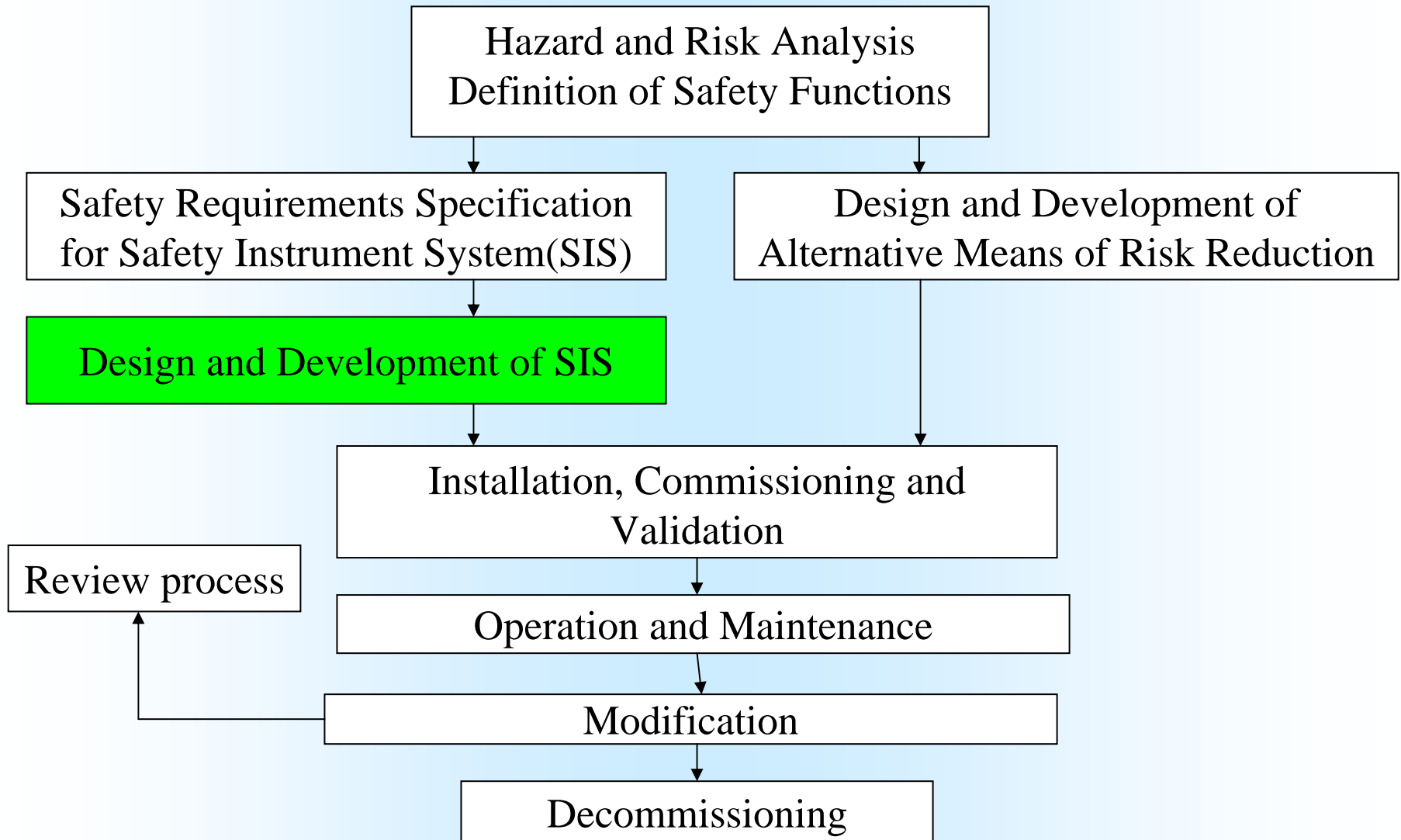
Safety Integrity Level	Probability of failure on demand	Availability %	Non Availability Continuous Demand	Risk Reduction Factor
SIL 1	0.1 to 0.01	90 to 99%	876 to 87.6 hours/year	10 – 100
SIL 2	0.01 to 0.001	99 to 99.9%	87.6 to 8.76 hours/year	100 - 1000
SIL 3	0.001 to 0.0001	99.9 to 99.99%	8.76 to 0.876 hours/year	1000 - 10000
SIL 4	0.0001 to 0.00001	99.99 to 99.999%	52 to 5.2 minutes/year	>10000

SIL 4 is not normally used in the process industry.

Safety Instrumented Function



SAFETY LIFE CYCLE



Safety Instrumented Functions & Safety Requirements Specifications

BS EN 61511-1 Clause 11

to design a system in that the Safety Instrumented Functions meet the
specified Safety Integrity Levels

Design of Safety Instrumented System

Prepare all documentation and detailed specifications for
the SIS

Typical Documentation includes:
Functional Description Specification
Loop Drawings
Logic Drawings
Installation Documentation
Equipment Specifications
Failure rate Data for equipment

Design of Safety Instrumented System

Ensure that the system complies to the standard and satisfies the required Safety Integrity Level

Typically:

Functional Safety Assessment and Design Reviews
Reviews against the standard

Calculation of Probability of Failure on Demand values

Compliance to hardware fault tolerance criteria

Assessment for proven in use and process conditions

Design of Safety Instrumented System

Calculate the nuisance trip levels for the system

Nuisance tripping is when the systems trips when it is not in a dangerous state.

Nuisance trips are much more likely than the system failing to danger, due to the relatively high safe fail fraction of the

SIF

1002 systems have double the nuisance trips of a 1001 system.

Design of Safety Instrumented System

Prepare testing and validation method statements

Typical Documentation includes:

SIS Panel FAT

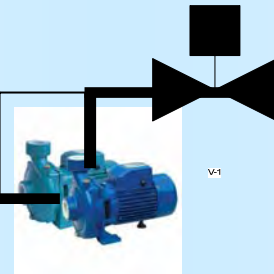
Equipment Failure Conditions Functional Test Document

Shutdown Conditions Functional Test Document

Process Conditions Functional Test Document

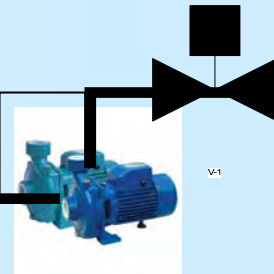
Analysis and Appraisal Documentation

Rail Tanker off-loading

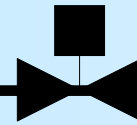


Rail Tanker off-loading

Full terminal control of
off-loading pumps and valves



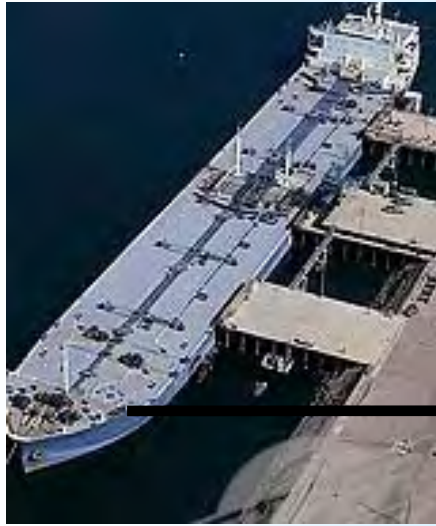
Ship off-loading



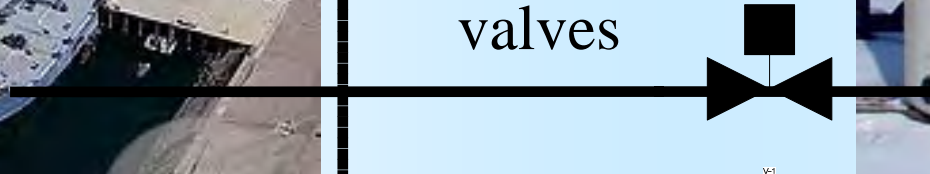
V1



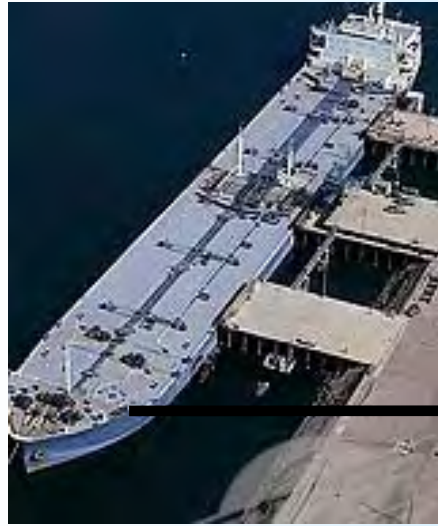
Ship off-loading



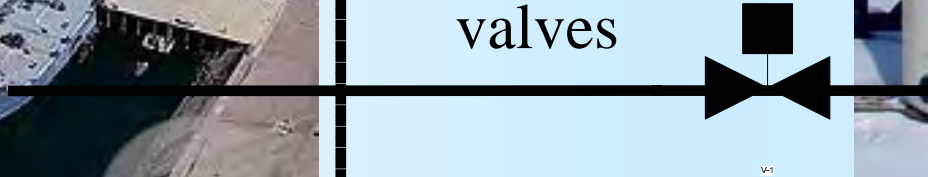
Split control
of
off-loading
pumps and
valves



Ship off-loading

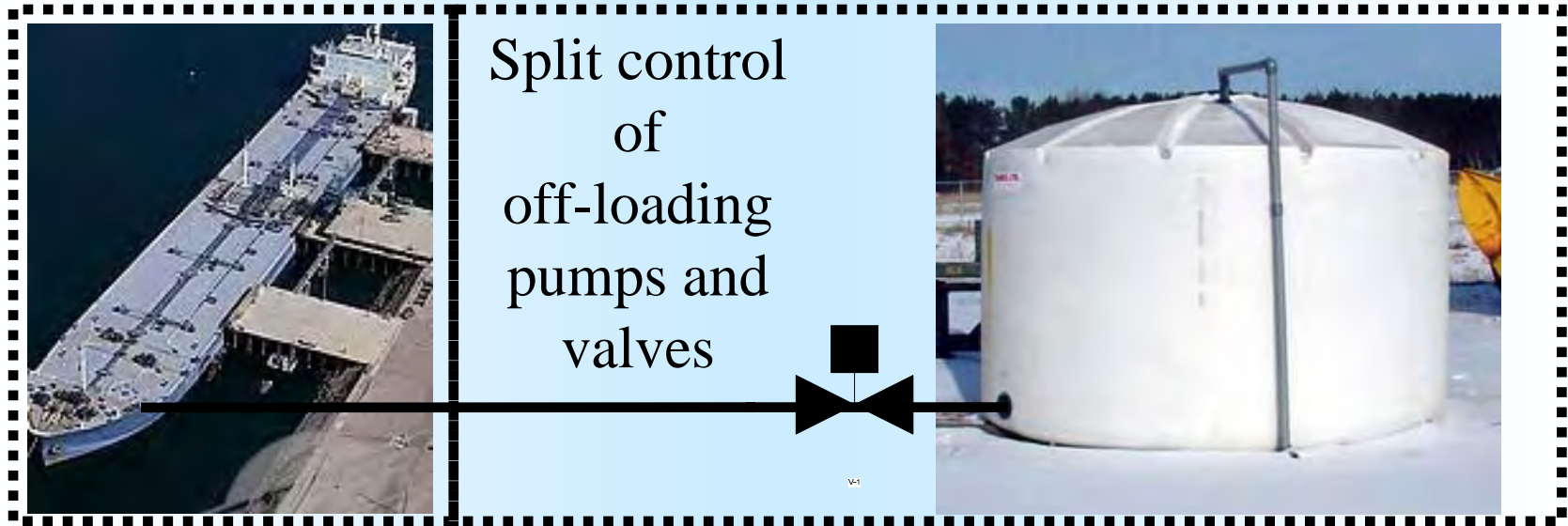


Split control
of
off-loading
pumps and
valves



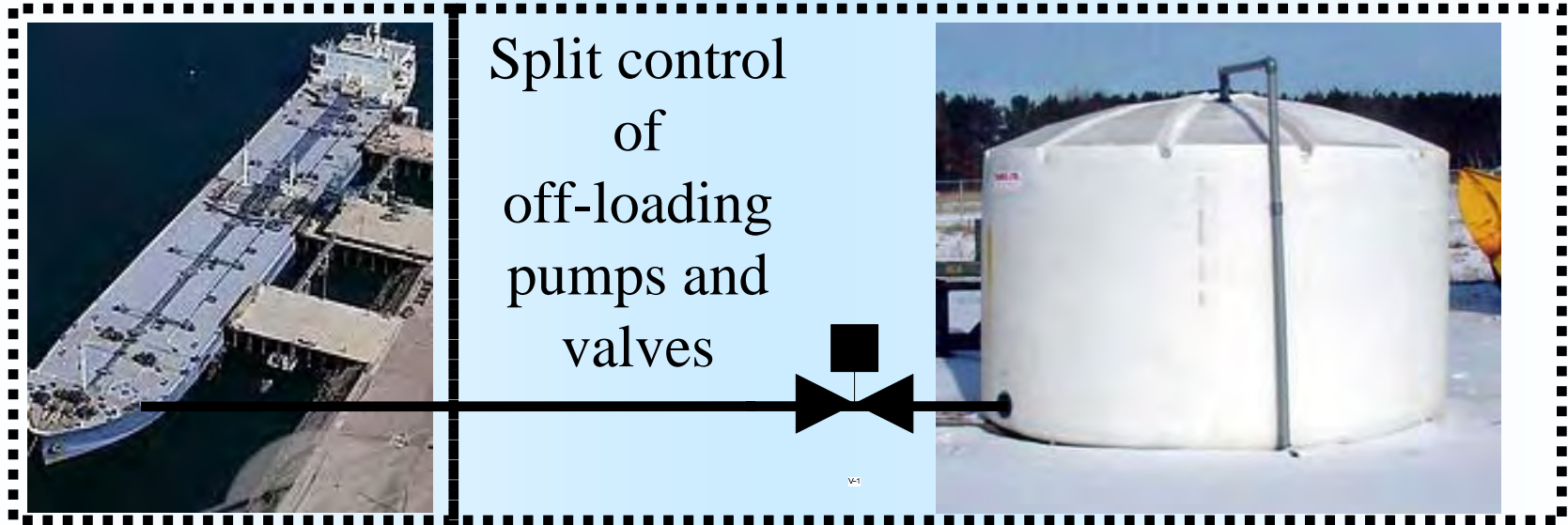
Surge Pressure Problems

Ship off-loading



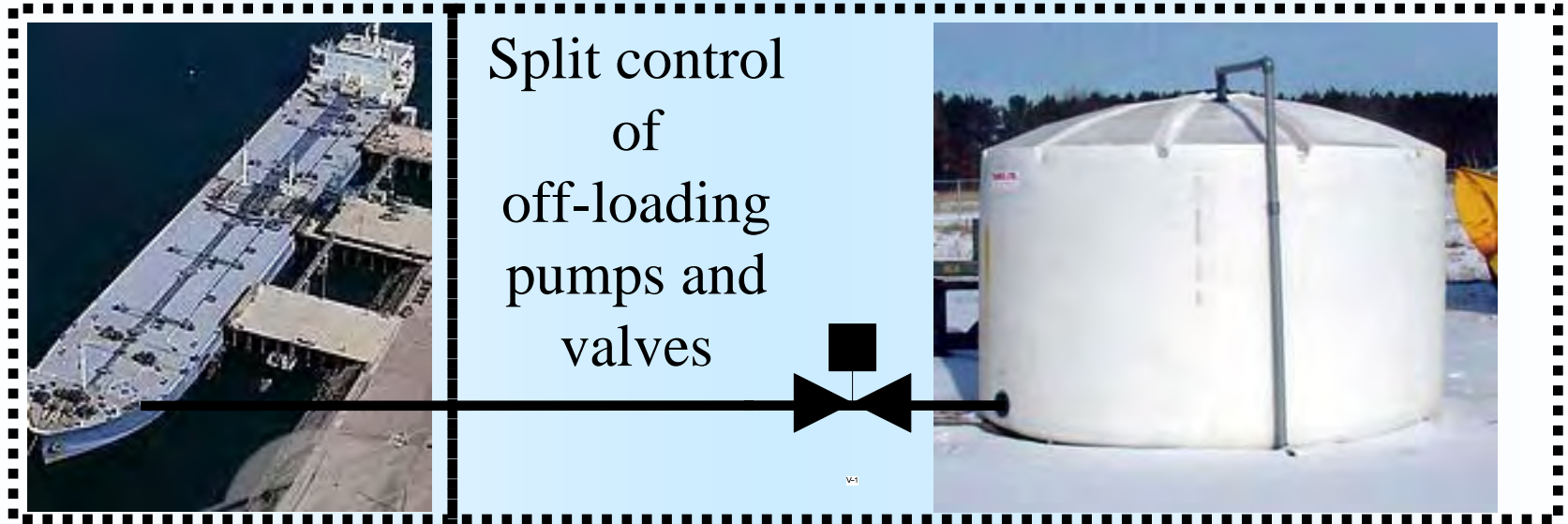
1. Linked shutdown system between ship and shore, with correct shutdown sequence.

Ship off-loading



2. Closing time of valves comparable to discharge flow rate to avoid surge pressures.

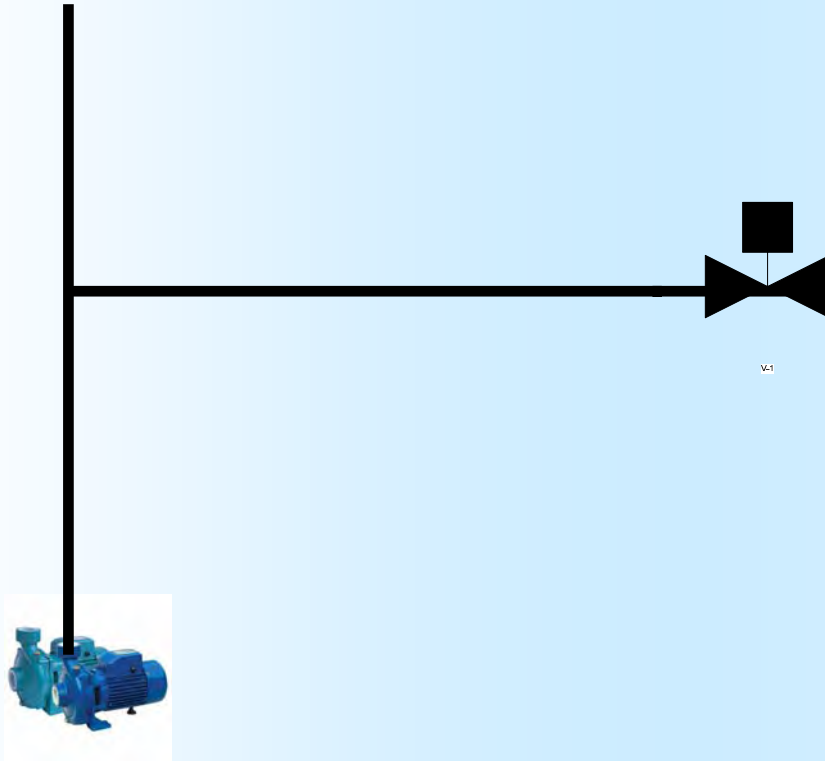
Ship off-loading



3. Shore to ship checklist and communications to ensure shutdown

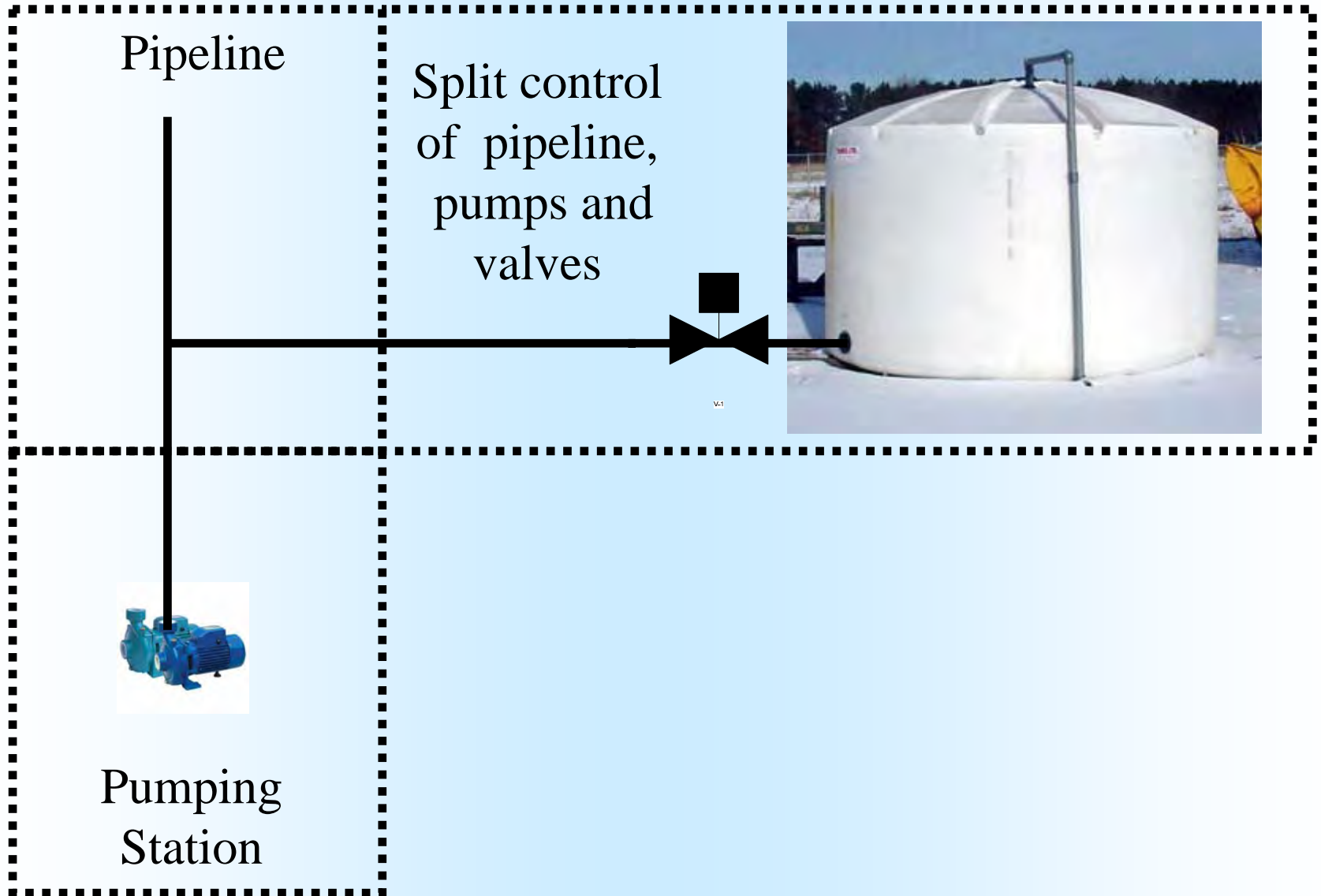
Pipeline transfer

Pipeline

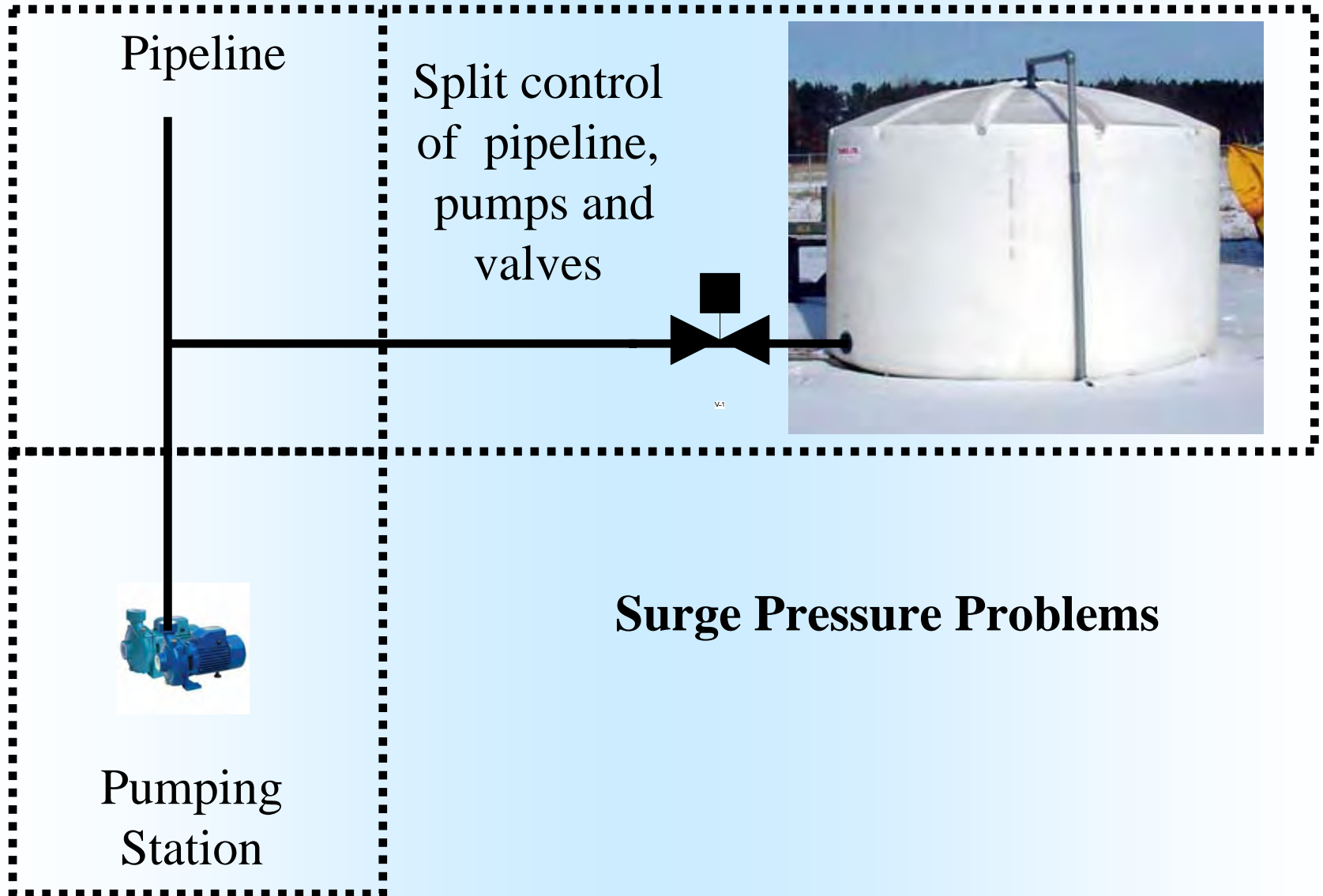


Pumping
Station

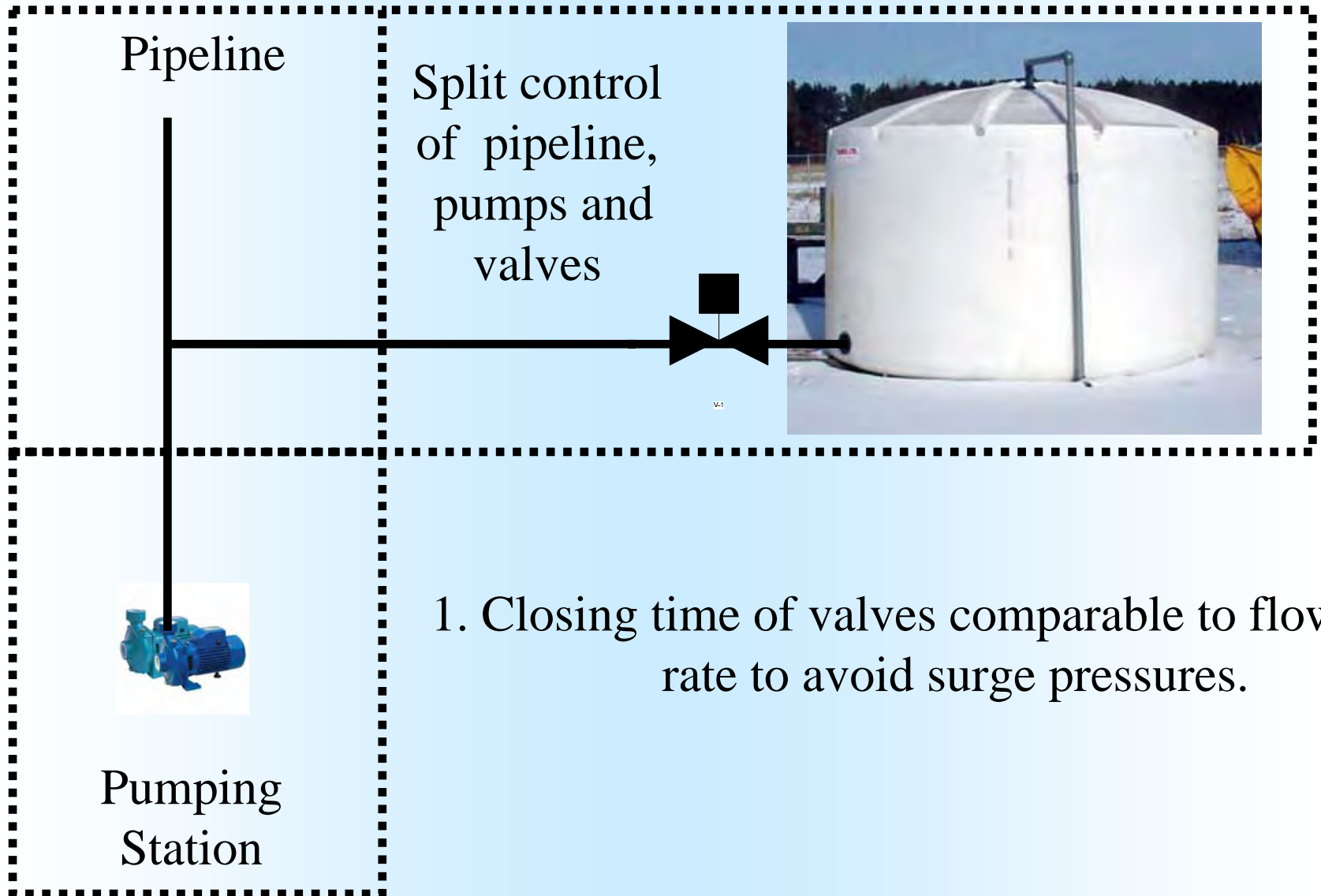
Pipeline transfer



Pipeline transfer

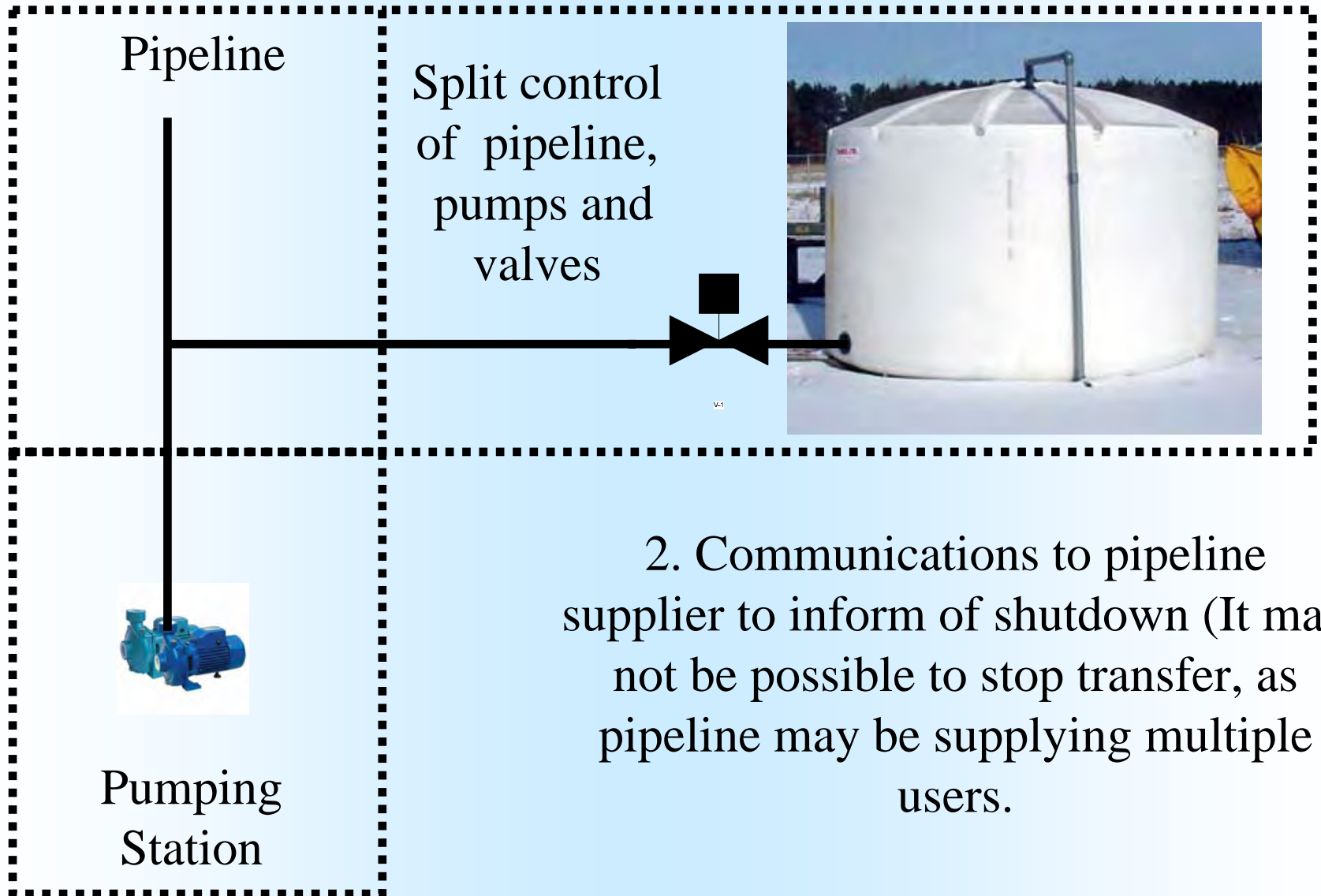


Pipeline transfer

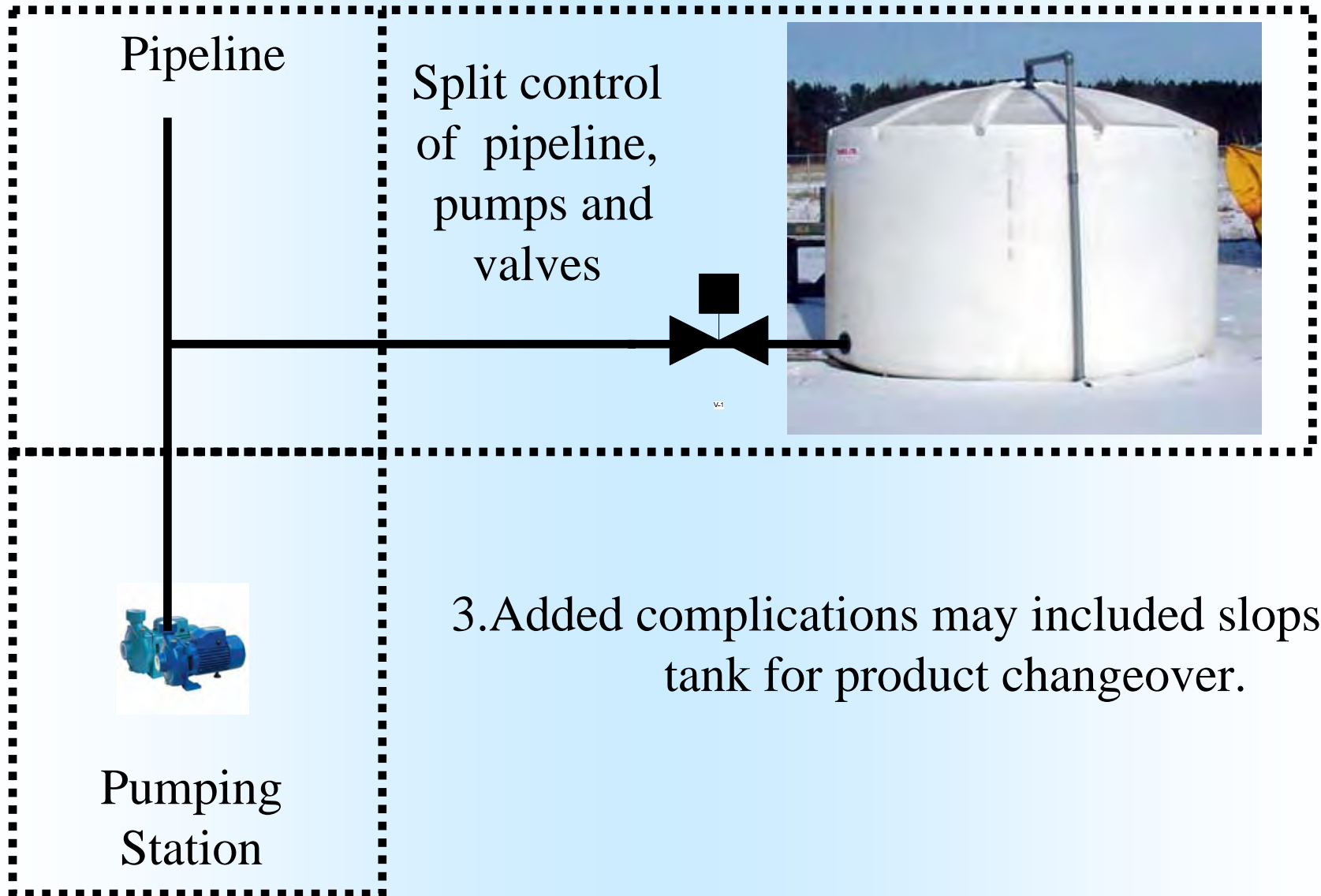


1. Closing time of valves comparable to flow rate to avoid surge pressures.

Pipeline transfer

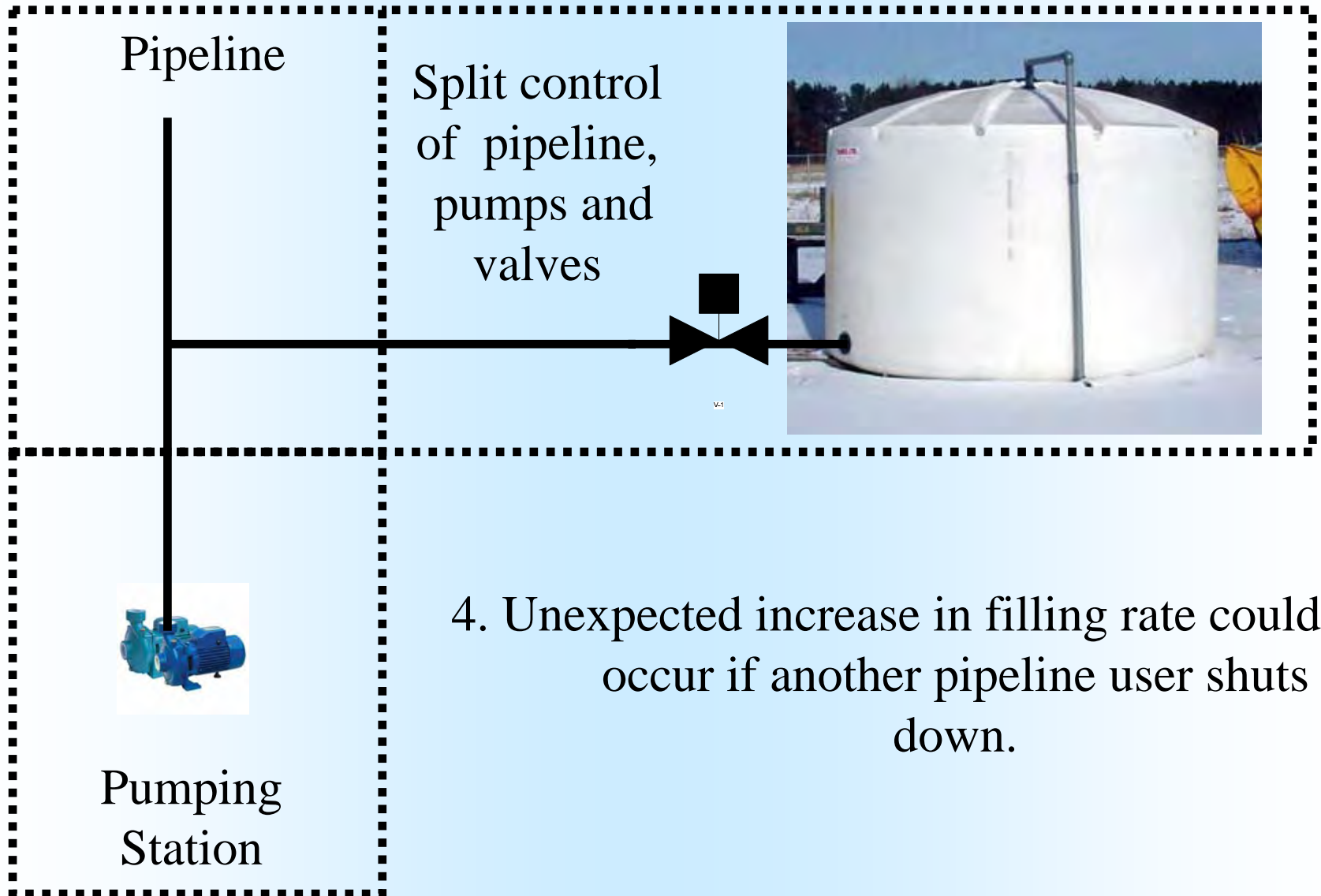


Pipeline transfer

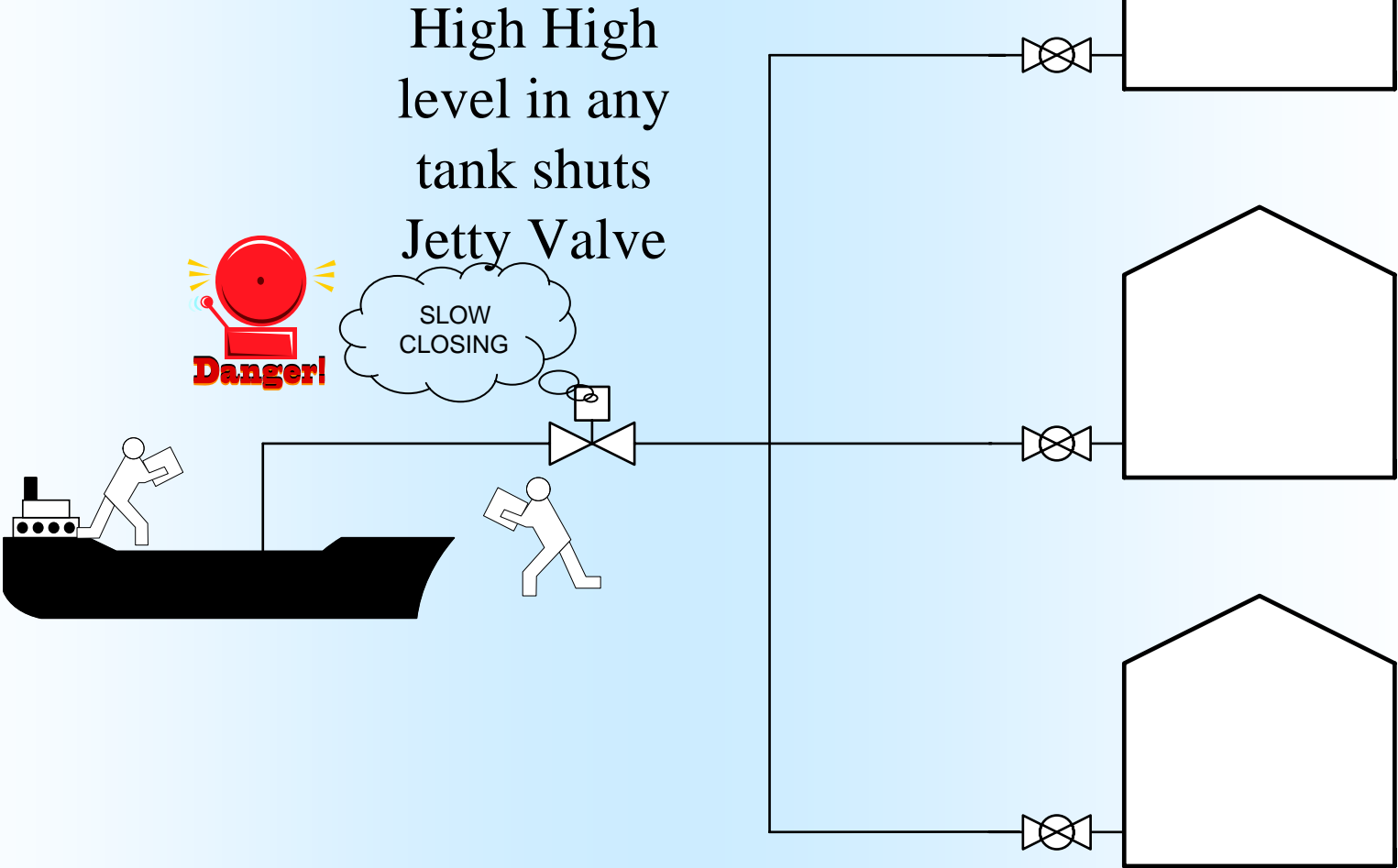


3. Added complications may included slops tank for product changeover.

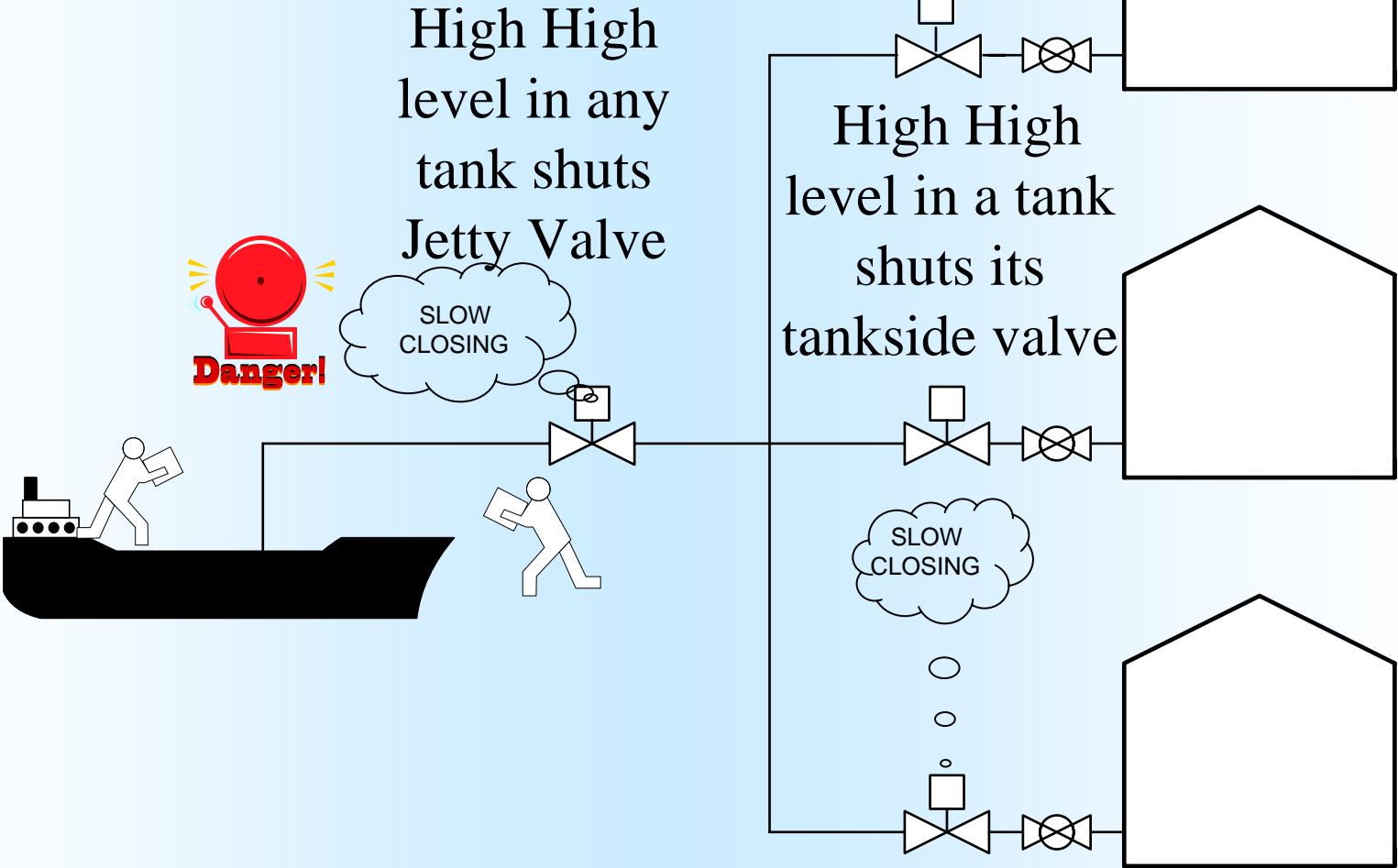
Pipeline transfer



Jetty transfer system



Jetty transfer system

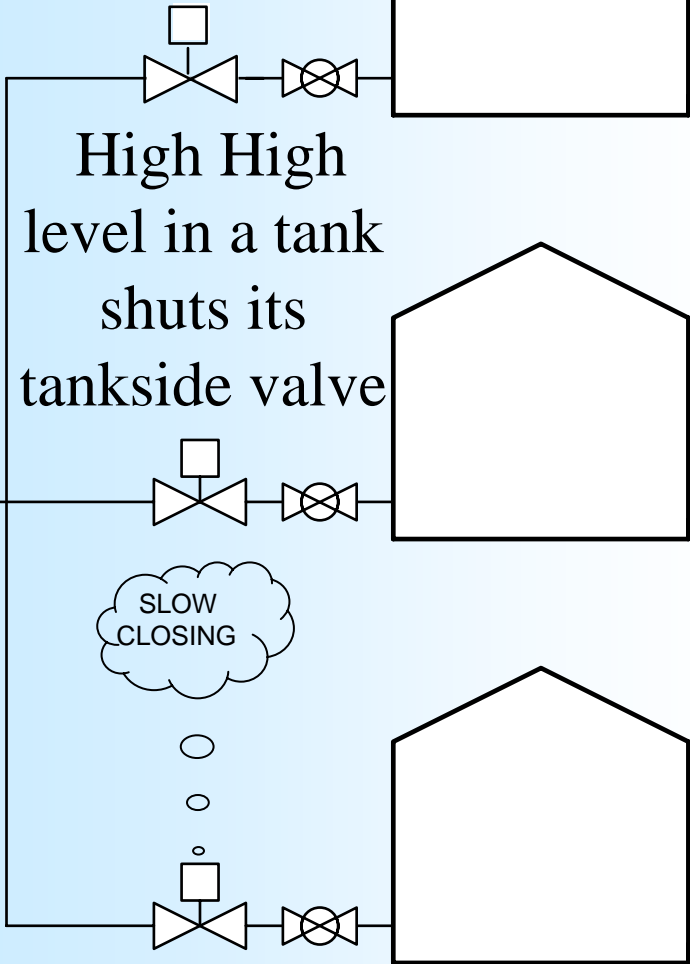
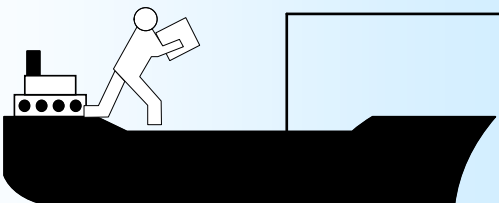


Jetty transfer system

High High level in any tank stops ships pump

High High level in any tank shuts Jetty Valve

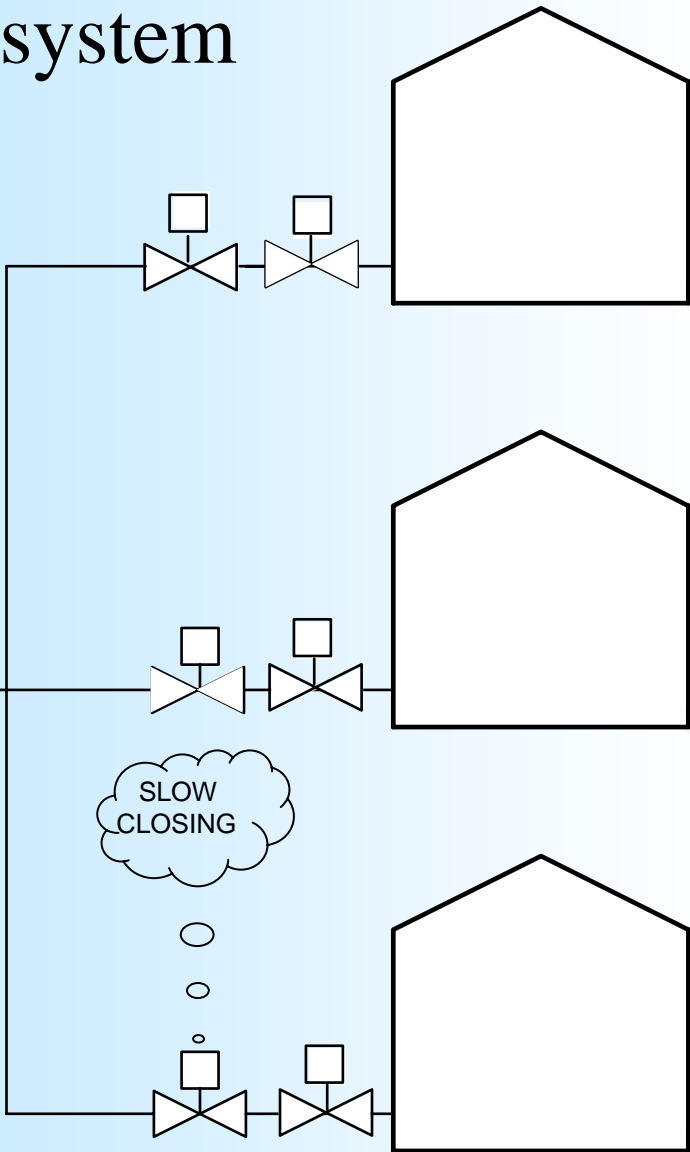
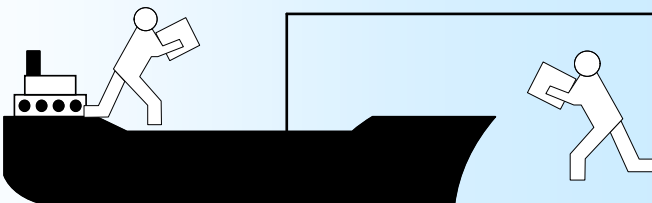
High High level in a tank shuts its tankside valve



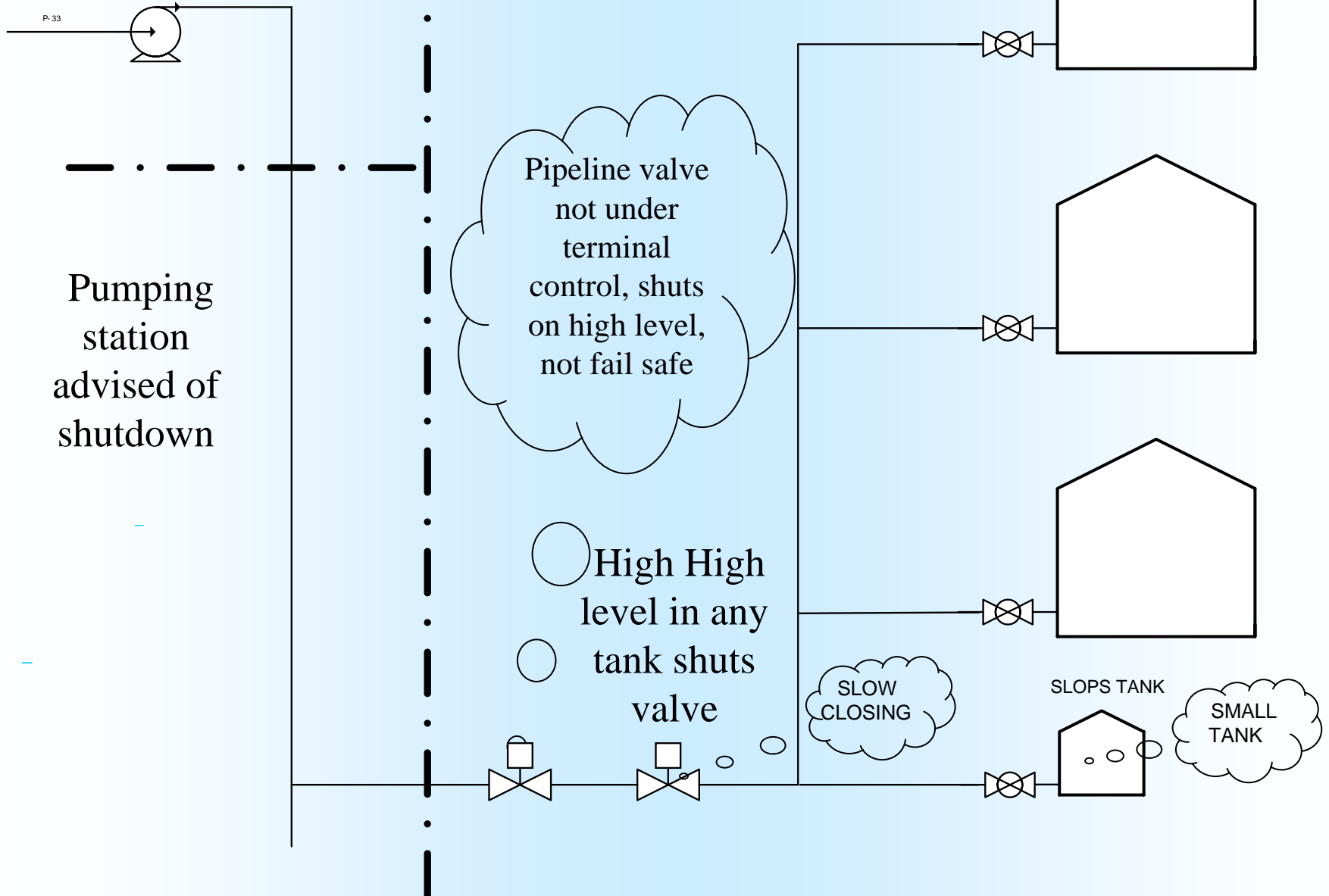
Jetty transfer system

High High level in any tank stops ships pump

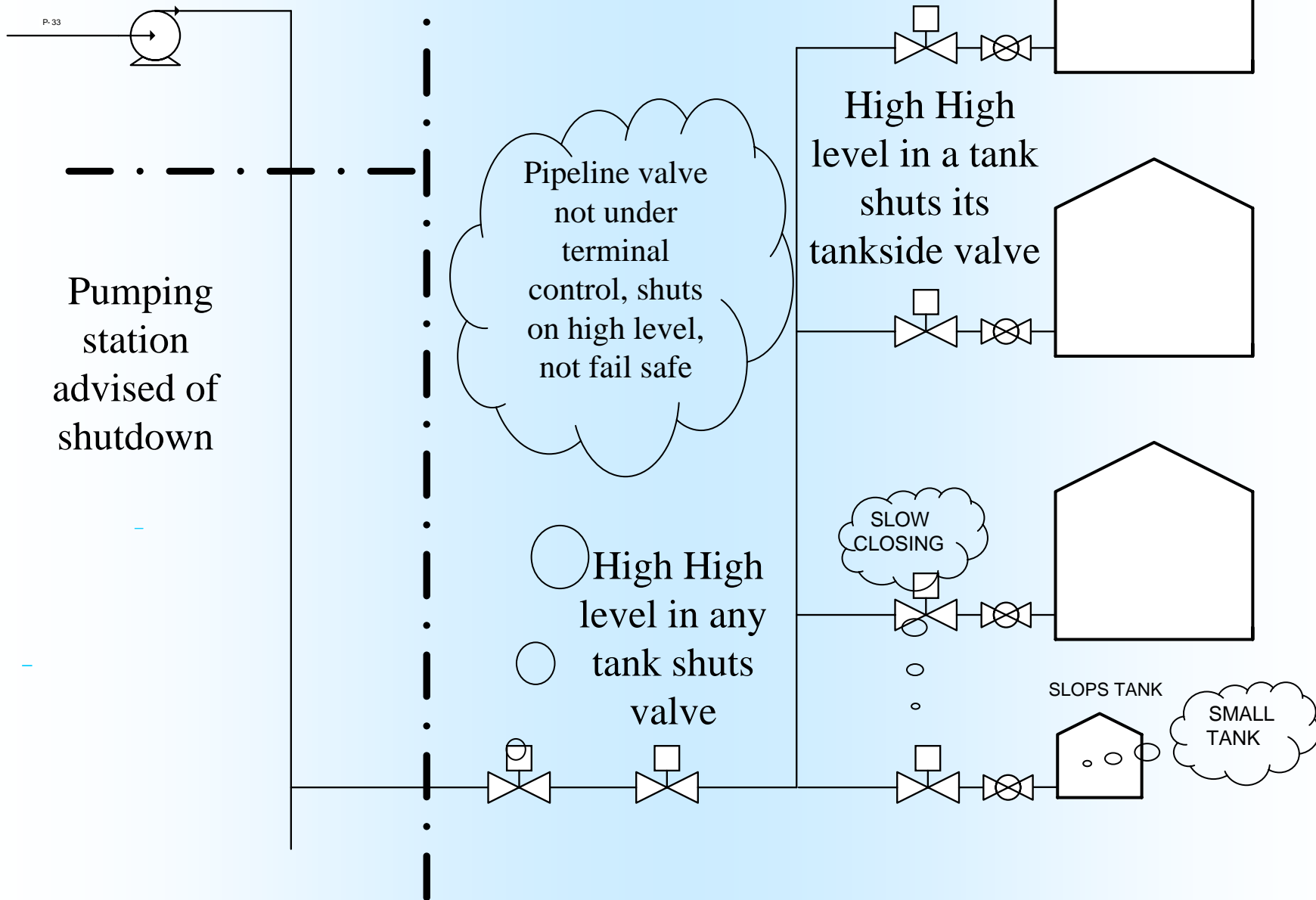
High High level in a tank shuts its tankside valves



Pipeline transfer system



Pipeline transfer system



Equipment

Sensors

Different techniques may be required for fixed roof and floating deck

Example Techniques: Vibronics, Displacer, Radar

Ensure manufacturers reliability data is fully understood, e.g it may be that on a Radar Gauge that the reliability data and PFD quoted are on internal relay outputs of the gauge and not necessarily on the “analog” or comms output.

Equipment

Logic Solvers

Simple systems – utilise non programmable systems

If programmable system – BS EN 61511 Clause 12 applies

Equipment

Final Elements

Fail Safe actuated valves – Pneumatic or electric

Pump Motors and motor control equipment, ensure independence, if BPCS stops the pump on high level, then the system will not be independent if the high high level operates the same motor contactor

If using a 1oo2 final element architecture ensure that process conditions testing tests each valve separately. If not you will not know the first valve has failed until the second fails

MIIB Recommendation 6

If Ship off-loading, it is essential to ensure that the ship and loading arms etc. are protected if the terminal shuts down, remember it could be a nuisance trip where no high high level alarm is activated

Similarly for pipeline transfers, ensure the pipeline supplier knows the consequences of the terminal shutting down and that the shutdown will not cause off-site incidents.

Summary

- Safety Instrumented Systems must be designed, installed, commissioned and maintained in accordance with BS EN 61511 (Life Cycle)
- Selection of suitably reliable equipment which will provide the level of protection suitable for the SIL
- Ensure that process conditions will not degrade or impair the equipment from performing the required function
- Proof testing is essential and continual assessment and analysis on reliability is required
- Ensure that the inclusion of an SIS does not provide other related problems

The End

Thank You

Safety IntelliPoint RF™ Series

Two-Wire, Point Level, SIL Conforming Safety Switch



One of the Drexelbrook RF Point Level Switches You Won't Have to Calibrate

The only RF switch you won't calibrate. Simply install the IntelliPoint RF Series into the tank and apply power...that's it! Unlike other RF or capacitance systems that require calibration via setpoint potentiometers, jumpers, magnets, or pushbuttons, the IntelliPoint RF Series reliably detects the absence or presence of material without any adjustments.

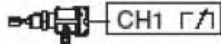
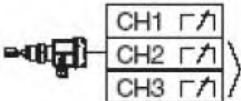
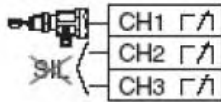
The IntelliPoint RF Series software continuously monitors the application for changes in composition, dielectric or conductivity, and maintains a repeatable trip point on the probe. Other RF and capacitance systems require calibration adjustments when the process material is changed. Since the the IntelliPoint RF Series recognizes changes in material, it is ideal for non-dedicated tanks that are used for a wide variety of products.

Intelligent Electronics

- For use in safety related systems with requirements for functional safety for SIL2 (SIL 3 with Redundant Switch) In accordance to IEC61508-2, Sec. 7.4.3.1 1999 (Conforms to SIL, FMEDA Requirements - Exida)
- No calibration or setpoint adjustments.
- Ignores changes in dielectric or conductivity.
- Automatically recognizes and ignores coatings to prevent false alarms.
- Continuous self-test monitors circuits and sensing elements for faults.

Self-Test Feature

Automatic and manual test functions ensure proper system operation. An AutoVerify™ self-check circuit continuously monitors that the complete system is functioning properly. The Manual Certify not only checks the function of the system, but also checks the AutoVerify self-test circuits to make sure

Liquiphant M FTL5x, FTL5xH, FTL51C, Liquiphant S FTL7x + Nivotester FTL325P-x1x1 (single channel device/ Einkanalgerät)	
Liquiphant M FTL5x, FTL5xH, FTL51C, Liquiphant S FTL7x + Nivotester FTL325P-x3x3 (triple channel device in single channel mode with two output relays in parallel/ Dreikanalgerät im Einkanalmodus mit zwei parallelen Ausgangsrelais)	
Liquiphant M FTL5x, FTL5xH, FTL51C, Liquiphant S FTL7x + Nivotester FTL325P-x3x3 (triple channel device in single channel mode/ Dreikanalgerät in Einkanalmodus)	
valid configurations/ zulässige Ausprägungen	FTL5x-xxx7xx, FTL5xH-xxx7xx, FTL51C-xxx7xxx, FTL7x-xxx7xxx + FTL325P-x1x1 or/oder FTL325P-x3x3
electronic/ Elektronik	FEL57 (2-wire PFM/2-Draht PFM)
safety-related output signal/ sicherheitsbezogenes Ausgangssignal	pulse-frequency-modulation/Puls-Frequenz-Modulation (PFM)
Safety Manual	SD111F
type of assessment/Art der Bewertung	IEC 61508 (full assessment)
Assessor	TÜV Rheinland (TÜV certificate/TÜV-Zertifikat: 968/EL 133.01/01)
SIL	2
type/Typ	B
HFT	0
mode of operation/Betriebsart	low demand mode
safety function(s)/ Sicherheitsfunktion(en)	Level MAX (e.g. overflow protection/z.B. Überfüllsicherung)
configuration/Einstellung Liquiphant	density/Dichte 0.7 density/Dichte 0.5
SFF	> 90 %
PFD _{av} (for/für T _i = 1 year/Jahr)	1.5 x 10 ⁻³ 2.0 x 10 ⁻³
functional test with push button/ Funktionstest mit Prüftaster	annual/jährlich annual/jährlich
complete functional test	not necessary within normal

SPRING RETURN ELECTRIC QUARTER TURN ACTUATOR (380 TO 7397Nm)

Rotork Skilmatic **SI** intelligent actuators offer a unique combination of the renowned features of Rotork actuation, such as the double sealing system and non-intrusive infrared commissioning capability, with the benefits of control and safety from Skilmatic range.

The **SI-2Q** are the higher torque actuators in the SI range. They are compact and robust electrically operated fail-safe spring return quarter turn units. Designed to provide a 90-degree travel for two-position, ESD or modulating applications. The actuators are suitable for all types of 1/4 turn valves

The **SI-2Q** is watertight and dusttight up to IP67 / NEMA 6 with the option of IP68 and includes the Rotork double seal system with separated termination and cable gland compartment. The actuators are also available certified explosionproof for hazardous area applications.

Consisting of a self-contained Electro-hydraulic control module and Scotch yoke spring return drive. The actuators combine the simplicity of electrical operation, with the precision of hydraulic control, and reliability of spring-powered fail-safe action. The spring return mechanism provides the most reliable means of positioning a valve to the safe condition and can be provided as fail-safe close, open or lock in last position on power or signal failure. The actuators are available as spring return clockwise or anticlockwise, with end of spring torque from 380 Nm (3363 inlbs) to 7397 Nm (65,469 inlbs)

The actuators can be programmed with the infrared setting tool to accept an analogue or digital input, with ESD and partial stroking or network cards options. A wide range of functions can also be selected through the setting tool such as zero & span limits, deadband, hysteresis, slow band, and partial stroke position. Optional internal fieldbus communication boards are also available for the Rotork Pakscan, DeviceNet, Profibus, Foundation fieldbus and Modbus digital control systems.

Specifically designed for on/off duties particularly where fail-



Safety Integrity: - Designed to SIL 3

FEATURES

- Self-contained electrically operated with internal low pressure Electro hydraulic control module.
- Spring return, Fail - Safe or lock in position