

Risk Management with Process Hazards Analysis (PHA)

Tony Ciliberti, PE

574-274-3887

tony.ciliberti@rd-eam.com



BS Chemical Engineering, Texas A&M University, 1987

Licensed professional engineer in the State of Texas

Principle Engineer for Reliability Dynamics LLC

- *Primary business function: Integration of reliability engineering with corporate information systems*

24 years of domestic and international experience in equipment reliability engineering and risk management

- *Intermediate and specialty chemicals, oil and gas, refining, oil and gas E&P, public utilities*
- *Maintenance Engineer, Project Manager, Maintenance Superintendent, Principal Consultant and Solution Architect*
- *Very strong in relational data theory and data management*

Risk management

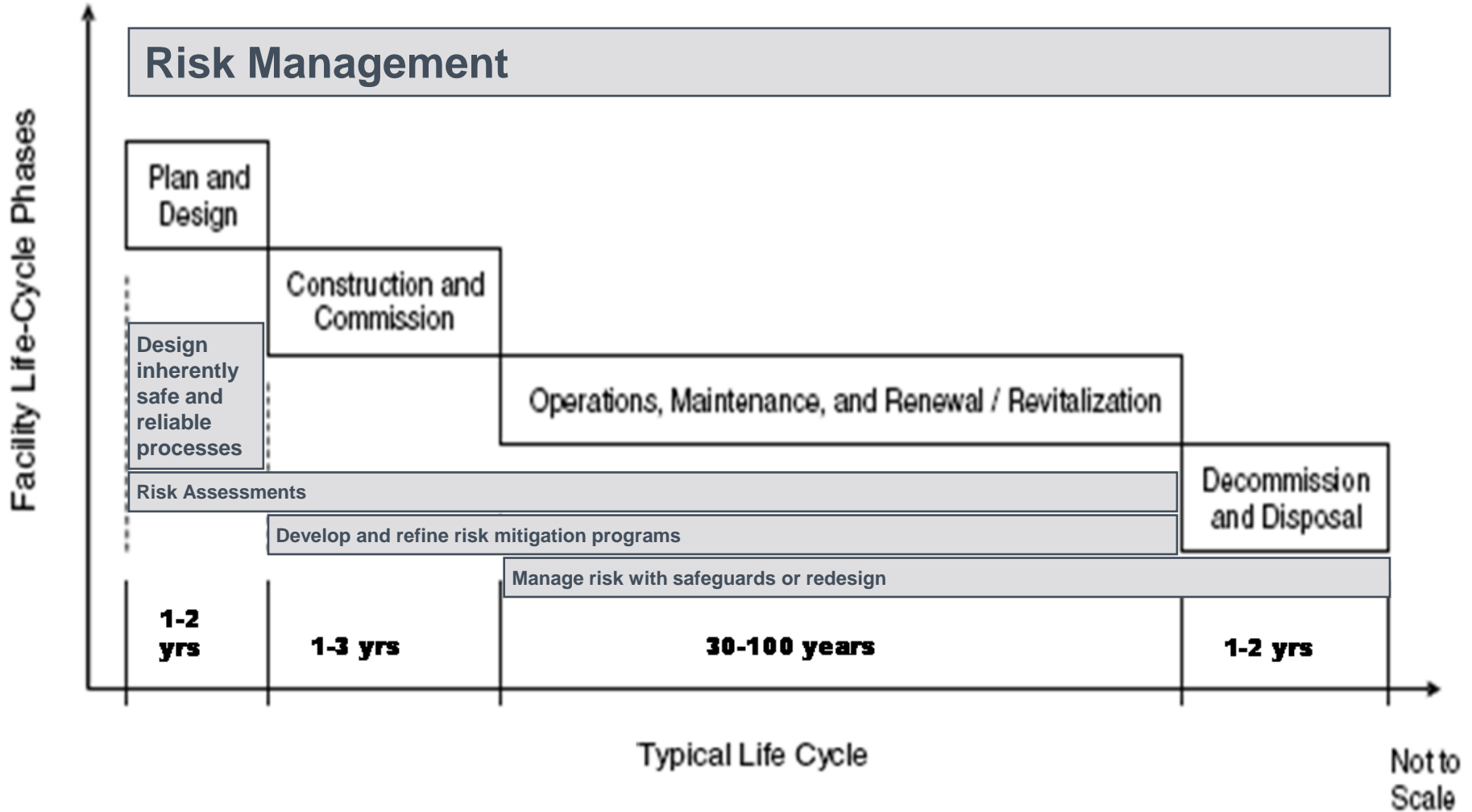
- Overview
- Safeguards
- 29 CFR §1910.119(e): risk management aspects
- Examples of possible violations

Preventive Maintenance

- Overview
- Common practices
- 29 CFR §1910.119(j): mechanical integrity requirements



Risk Management



Risk management: all activities or programs used to (1) define acceptable risk and (2) to ensure risk levels remain within acceptable levels

Risk assessment: a methodical process for identifying and tabulating scenarios for loss

Scenario: hypothetical depiction of a loss event, including identification of an event, faults/causes, and potential consequences. Consequences are frequently risk-ranked.

Risk = Consequence Severity x Likelihood (or Frequency)

Inherent Risk: risk before application of risk-reduction measures (safeguards).

In-place Risk: net risk after application of risk-reduction measures.

Safeguards: measures implemented to mitigate risk by reducing likelihood, consequence severity, or both.

Criticality: a measure of importance that is directly proportional to risk level.

Designing inherently safe and reliable processes

- Build-out the risk instead of managing it throughout the facility lifecycle

Developing risk mitigation programs

Tracking details on tens of thousands to millions of equipment items and related safeguards

- Data-driven decision-making
- Risk-based prioritization
- Real-time data
- Cockpit view

Engineering and administrative controls used to ensure safe operation and optimize production, e.g.

- Safe job procedures
- Training
- Preventive and predictive maintenance
- Inspection programs
- Installed protective equipment
- Spare equipment and parts

Each safeguard provides an incremental amount of risk reduction by reducing:

- The likelihood of a scenario and/or
- The potential consequences

For a tank containing a hazardous chemical

- Reducing inventory would reduce potential consequences of a spill
- Routine corrosion monitoring would reduce the likelihood of a leak
- Either way, the exposure level would be incrementally reduced and remains lower provided that the safeguard continues to give the intended/assumed risk reduction amount
 - Is inventory maintained at or below the reduced level?
 - Is the UT testing device calibrated properly/routinely?
 - Is the inspector properly trained?

Develop risk rating process and determine acceptable risk threshold

Develop failure scenarios and assess in-place risk for each consequence

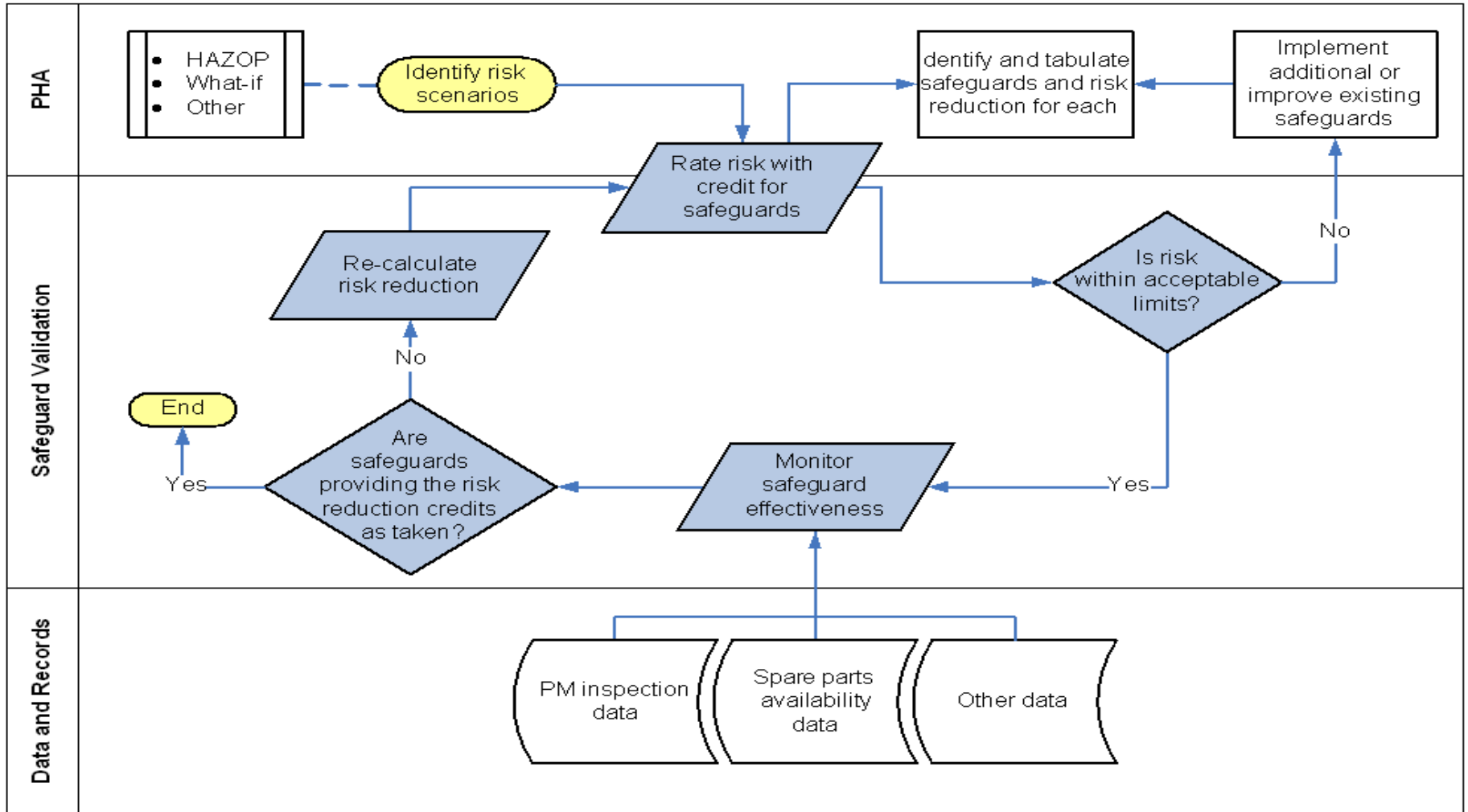
■ Risk = consequence severity * likelihood

Identify safeguards and quantify respective risk reduction amounts for each using reverse logic (delta risk with safeguard removed)

Apply risk-reduction measures for scenarios that exceed acceptable risk

Confirm risk-reduction taken for safeguards

Operational Experience and Process Data Feedback to Risk Assessment



For each safeguard:

- Assign a unique ID
- Define criteria for each safeguard to achieve the amount of risk reduction taken
- Determine how criteria will be monitored and how much risk reduction will be lost if criteria are not satisfied
- Prioritize safeguard based on amount of risk reduction

Safeguard effectiveness must be validated to ensure assumed risk reduction credit is actually achieved

- When safeguards do not provide their intended risk reduction, facility risk levels increase
- Facilities need to be aware of fluctuations in risk levels so appropriate remedial action can be taken when required

Relevant equipment tag numbers should be discretely specified for each scenario, not just referenced

- Also the related roles for each, e.g. fault, event, or safeguard

The focus of *criticality* should be scenarios and safeguards versus protected equipment

(3) The process hazard analysis shall address:

(3)(i) The hazards of the process;

(3)(iii) Engineering and administrative controls applicable to the hazards and their interrelationships such as appropriate application of detection methodologies to provide early warning of releases.

(3)(iv) Consequences of failure of engineering and administrative controls;

(3)(vii) A qualitative evaluation of a range of the possible safety and health effects of failure of controls on employees in the workplace.

Standard 1910.119(e)	What the PHA Team Is Required to Do to Comply with Each Specific 1910.119(e)(3) Standard. The PHA Team Must...
(3)(i)	identify each process hazard, deviation(departure from the design intention), etc. (hazard)
(3)(iii)	determine the engineering and administrative controls including safeguards (alarms, interlocks, blast-resistant walls, relief valves, etc.) that are related to each particular hazard they identify
(3)(iv)	identify hazardous process situations involving the failure of engineering and administrative controls and to identify the consequences of those failures. Also, minor consequences unrelated to the potential release of highly hazardous chemicals from the covered-process are usually not considered.
(3)(vii)	use the consequences of failure information developed under 1910.119(e)(3)(iv). This information is used by the team to conduct a qualitative evaluation of the possible safety and health effects related to the failure of the identified controls for each of the identified hazards. The purpose of this evaluation is to assist the PHA team in their decisions for prioritizing the planning for the control of the hazards they have identified (see discussion below and attached Appendix for more information).



Figure 1 - Example Worksheet Excerpt from What If/Checklist PHA Methodology
C = Consequence Class, L = Likelihood Class, R = Risk Class

What If...	Consequences/ Hazard	Safeguards	C	L	R	Recommendations/ Action
Emergency Shutdown Valve 23 (ESD - 23) fails to close when needed? (This can occur due to extremely cold weather, reliability due to inspection/testing/maintenance or design problems)	Release of highly flammable materials in the operating area. Potential for fire/explosion with employee injuries/fatalities 1 3	1. Specific Inspection/testing/maintenance program for ESDs 2. Valve actuator sizing 3. ESD-23 is fail closed design 2	4 4	2 4	B 4	1. Due to cold weather modify MI procedures to increase ESD valve testing to 1/2wks. 2. Inspection records for ESD 23 not in file, follow-up to assure ESD-23 inspected as required by MI procedures 3. No equipment data sheet was found for actuator for ESD-23, follow-up with engineering to assure design is correct. 4. Consider over sizing valve actuator

C = Consequences Class
L = Likelihood Class
R = Risk Priority Class

1 - 1910.119(e)(3)(i): address the hazards of the process
2 - 1910.119(e)(3)(iii): address engineering and administrative controls applicable to the hazards...
3 - 1910.119(e)(3)(iv): address consequence of failure of engineering and administrative controls
4 - 1910.119(e)(3)(vii): address a qualitative evaluation of a range of possible safety and health effects of failure of controls...

Figure 2 - Example Excerpt from HAZOP PHA Methodology
C= Consequence Class, L= Likelihood Class, R = Risk Class

Deviation	Causes	Consequences	Safeguards	Recommendations/ Actions	C	L	R
Loss of Agitation ①	Agitator motor fails Electrical utility lost Agitator mechanical linkage fails Operator fails to activate agitator ① ②	Un-reacted HHC in the reactor carried over to Storage Tank 3 (ST-3) and is released to the enclosed work area. Probable injuries or fatalities to workers due to highly acute toxic material hazard ③	HHC detector and alarm ②	1. Consider adding alarm/shutdown of the system for loss of agitation to the reactor 2. Ensure adequate ventilation exists for enclosed work area and/or use an enclosed ST-3 3. Update PSI file and Op. Procedure HHC-39 to include consequence of deviation, engineering controls including safety system information, e.g. SIS and emergency ventilation	4 ④	2 ④	B ④

C = Consequences Class
L = Likelihood Class
R = Risk Priority Class

① - 1910.119(e)(3)(i): address the hazards of the process
② - 1910.119(e)(3)(iii): address engineering and administrative controls applicable to the hazards...
③ - 1910.119(e)(3)(iv): address consequence of failure of engineering and administrative controls
④ - 1910.119(e)(3)(vii): address a qualitative evaluation of a range of possible safety and health effects of failure of controls...

Figure 3 - Consequence Table

Consequence Class	Qualitative Employee Safety Consequence Criteria
1	No employee injuries
2	One Loss Time Injury or Illness
3	Multiple Lost Time Injuries or Illnesses
4	Multiple Lost Time Injuries or Illnesses w/one or more fatalities

Figure 4 - Likelihood Table

Likelihood Class	Qualitative Likelihood Criteria
1	Not expected to occur during the lifetime of the process. Examples – Simultaneous failures of two or more independent instrument or mechanical systems
2	Expected to occur only a few times during the life of the process. Examples – Rupture of product piping, trained employees w/procedures injured during LOTO operation
3	Expected to occur several times during the life of the process. Examples – hose rupture, pipe leaks, pump seal failure
4	Expected to occur yearly. Examples - instrument component failures, valve failure, human error, hose leaks

Figure 5 - Example Risk Priority Matrix

Consequences ↑	4	C	B	A	A
	3	C	B	B	A
	2	D	C	B	B
	1	D	D	C	C
		1	2	3	4
Likelihood →					

Figure 6 - Example Risk Priority Legend

Priority ↑	Risk Class	Explanation of Risk
	A	Risk intolerable - needs to be mitigated within 2 weeks to at least a Class C, if that cannot be accomplished, process needs to be shutdown
	B	Risk undesirable - needs to be mitigated within 6 months to at least a Class C
	C	Risk tolerable with controls (engineering and administrative)
	D	Risk acceptable - no further action required

Safeguards: Examples of Possible Violations

OSHA DIRECTIVE NUMBER: CPL 03-00-010, A-23

21

- a. 119(e)(1) – if: 1) the employer identified/credited a safeguard that was ineffective or inappropriate for the hazard/deviation when it conducted the PHA; or 2) the employer did not adequately evaluate the identified/credited safeguard ("...shall identify, evaluate and control...") when it conducted the PHA;
- b. 119(e)(3)(iii) - the employer used an inadequate engineering or administrative control/safeguard to protect against a hazard/deviation it identified in its PHA;
- c. 119(d)(3)(ii) - the employer did not design or document that the PHA identified/credited safeguard complies with RAGAGEP;
- g. 119(j)(4)(i) – (iv) – the employer did not inspect and test a safeguard to ensure it functions as intended when it identified/credited the safeguard in its PHA as protection against an identified hazard/deviation; or
- h. 119(l)(1) - the employer changed the safeguard prior to conducting an MOC procedure.

Company: Process Company
 Facility: Standard Wellsite Glycol Dehydrator

Session: 1 03-25-93 Revision: 0 03-24-93
 System: 1 Wet gas inlet and 112-V-001

Subsystem: Feed line to the column

Drawn: ESD-063-S

WHAT IF...	HAZARD	CONSEQUENCES	SAFEGUARDS	S	L	R	RECOMMENDATIONS	REMARKS	BY
1. Hydrates form and don't release?	Operability problem may occur	1. Blockage due to hydrate could cause loss of production.	1. Piping will be designed for full wellhead pressure 2. Methanol injection upstream of 112-V-001 3. PSH/L on wellhead would cause ESD	1	3	4	1. Indicate that the feed line to the 112-V-001 column is sloped toward the column	Check GS-43	BNP
2. hydrate forms and then releases and flows downstream violently?	Impact damage to the piping	1. Rupture of the piping and release of hydrocarbon to the atmosphere. Probable fire damage. 2. Potential for equipment damage due to the hydrate impact 3. Potential injury or fatality to operator	1. Same as cause #1 above 2. Safe operating practice (SOP) to depressure 3. Pressure indicators on the column would indicate lower pressure	1	3	4	2. If hydrates are prevalent, consider additional safeguards such as heat tracing of lines.		OPS
3. ESD valve fails to close when needed? (This may occur due to extremely cold weather, or ESD reliability or design problems)	Release of highly hazardous material	1. Probable more significant fire damage 2. Greater potential for injury or fatality 3. Production loss	1. Preventative maintenance 2. Sizing of the actuator 3. ESD valve is fail closed design	1	3	4	3. If the dehydration unit is provided in an area subject to extremely cold weather, consider frequent testing of ESD valves, oversizing of the actuators, or other means		OPS
4. liquid slug occurs?	Operability problem may occur	1. High level in the separator. Operability problem only 2. Glycol contamination.	1. High level switches 2. Level controller	4	3	8	4. If well is subject to liquid slugs, then consider a slug catcher		OPS

Worksheet

Company: ALC Refining Inc.
 Facility: Amine A unit

Session: 1 08-08-94

Revision: 0 08-01-94 Dwg#:

Node: 1 Sour gas feed to F-627A

Intention: The flow rate is 3.5-5MMSCFD make gas from Lean gas scrubber F-203A.

Parameter: Flow

GW	DEVIATION	CAUSES	CONSEQUENCES	SAFEGUARDS	S	L	R	RECOMMENDATIONS	REMARKS	BY
No/Less	No/Less Flow	1. Block valves (3) closed by operator or left closed prior to start-up	1.1. Loss of feed to the Amine plant	1.A. Operating procedures are in place and operators are trained in their use 1.1.1. FC-611A will alarm on low flow 1.1.2. FC-611B will alarm on the Amine B Train on high flow	4	4	9	No Recommendations-Safeguards considered adequate		
			1.2. Pressure increase on Gas recovery unit and coker	1.2.1. PC-602 will alarm on high pressure						
			1.3. Pressure increase on Amine unit Train B if block valve downstream of tie-in before F-627A is closed.	1.3.1. PC-601 will open PV-601 to maintain system pressure 1.3.2. PDI-628 will alarm on high differential pressure						
			1.4 Pressure decrease on Amine unit Train B if block valve upstream of tie-in before F-627A is closed.	1.4.1. PC-601 will close PV-601 to maintain system pressure						
			1.5. Excessive flaring.	1.5.1. Operating flare						
			1.6 Potential environmental incident.	1.6.1. Environmental procedures are in place						
			1.7 Potential upset/shutdown of the SRU unit which is operating on pressure. The SRU operating on flow will remain online.	1.7.1. Problems with Amine unit are communicated with other units via radio, phone, and process information 1.7.2. Emergency shutdown procedures are in place						



Preventive Maintenance

API RP 580, Risk-based Inspection, Section 12.1

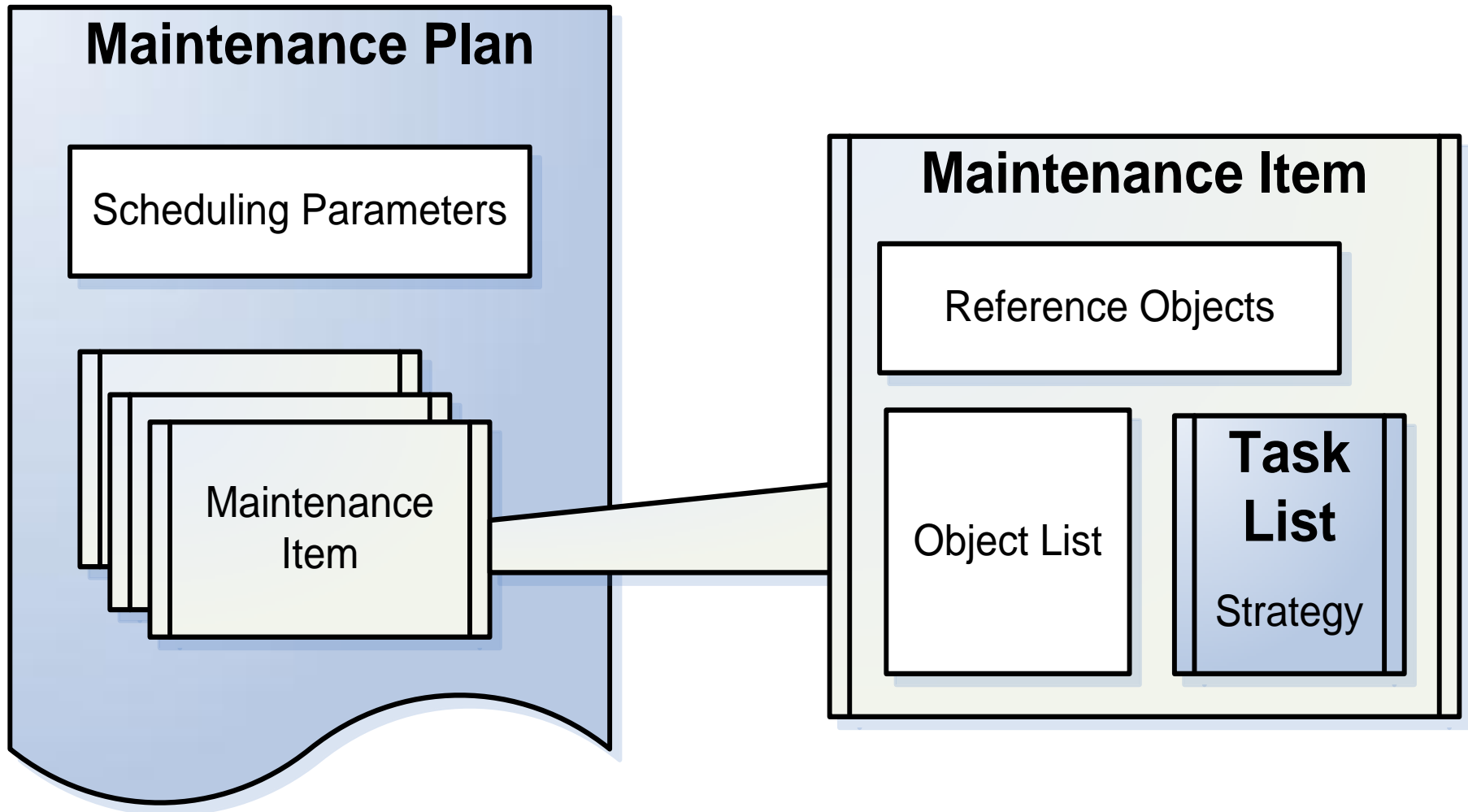
- Risk mitigation achieved through inspection presumes that the organization will act on the results of the inspection in a timely manner
- Risk mitigation is not achieved if inspection data that are gathered are not properly analyzed and acted upon where needed. The quality of the inspection data and the analysis or interpretation will greatly affect the level of risk mitigation

Routine and scheduled maintenance work on equipment

- Planned refurbishment
- Functional testing
- Inspections

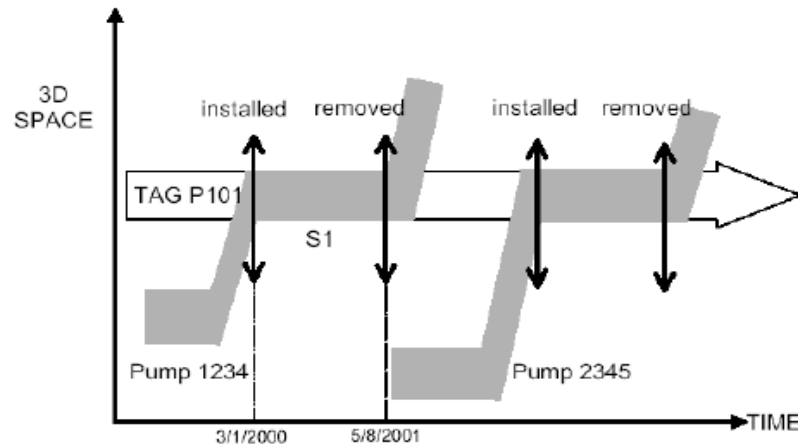
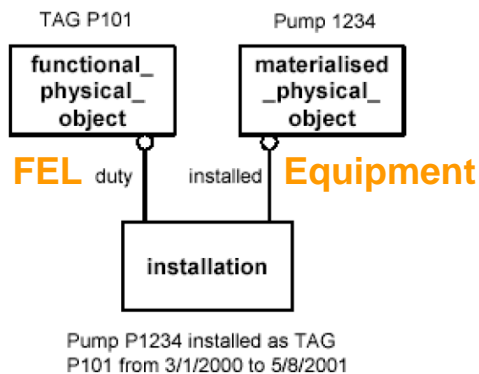
Key considerations

- Explicit means to report pass/fail inspection results
- Documentation of any failed inspection as an equipment malfunction
- Ability to capture quantitative inspection values for each step in a task list
- Evaluation criteria for measured values, with pass/fail assessment on both individual measurements and for the equipment item as a whole
 - When measured values are out-of-tolerance, the following questions must be answered:
 - Is the equipment suitable for continued service?
 - Does the inspection interval or scope need to be changed?
- Ability to analyze results en masse
 - If you can't analyze 1000 things at once, you're not doing it right



Functional equipment location Tag P101 is an intangible object that defines process requirements for a particular pumping service, e.g. pressure, temperature, flow, fluid type (Tag P101 in the example below)

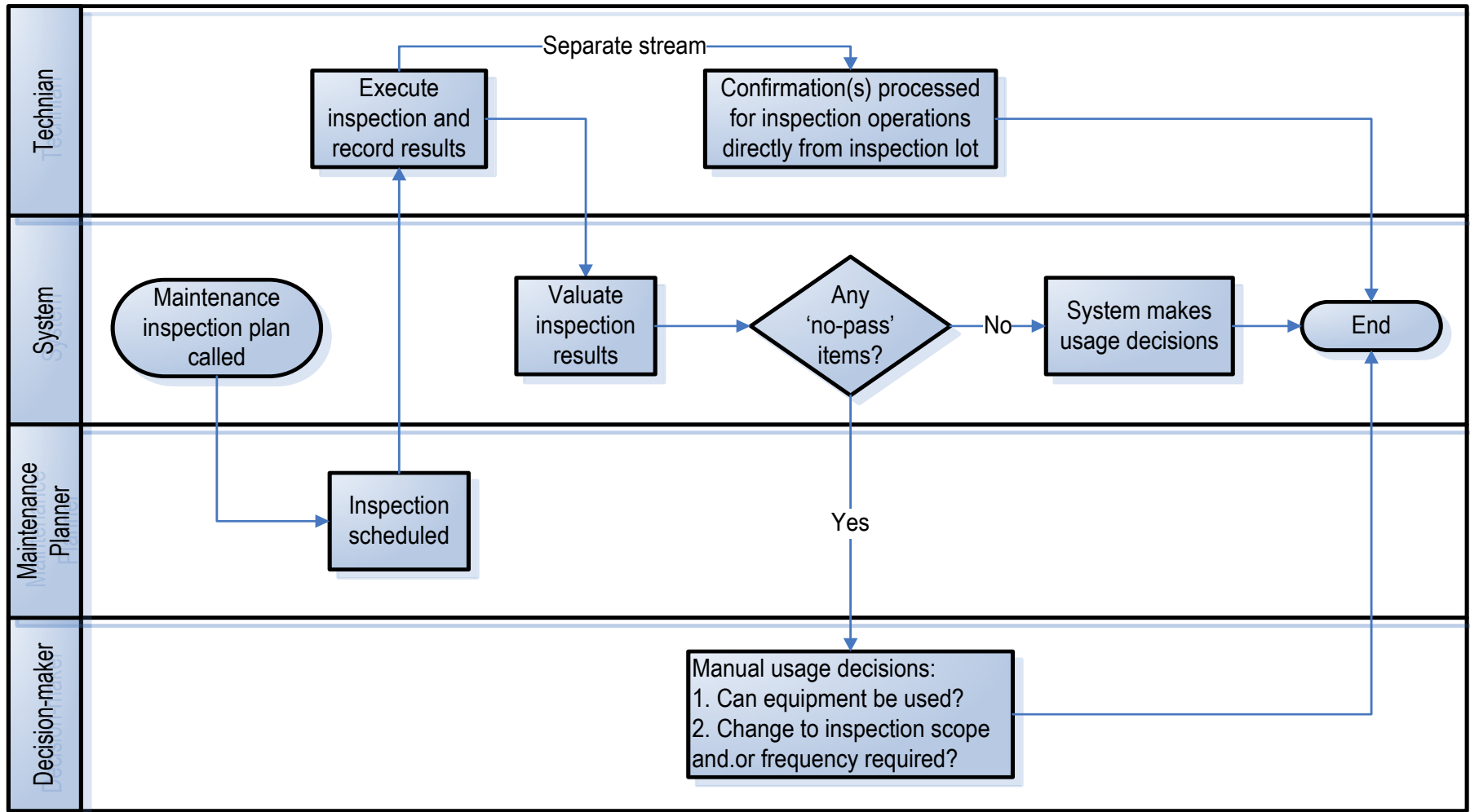
Equipment items (serial numbers 1234 and 2345) define specific materialized objects that execute process requirements



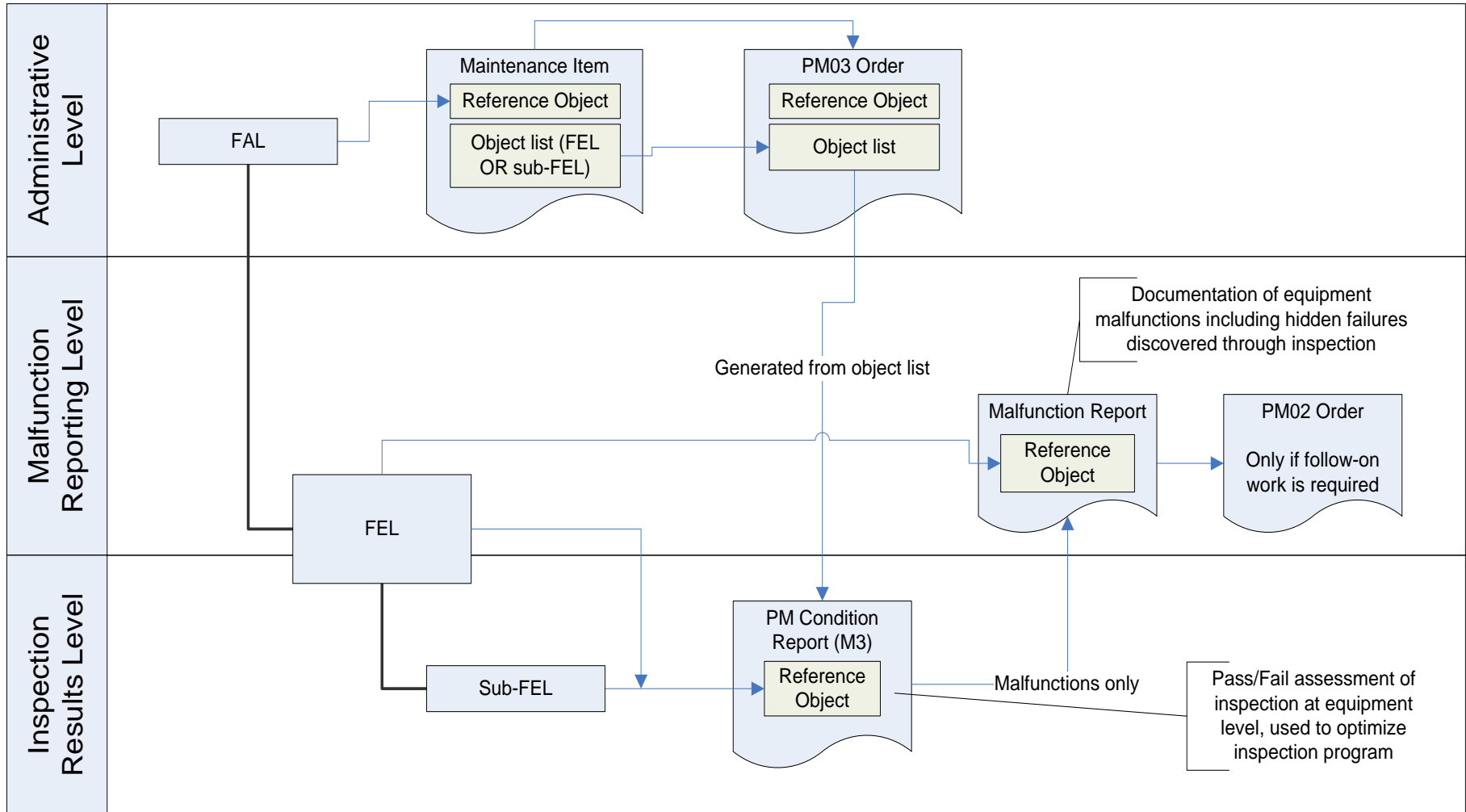
The duty represented by TAG P101, and Pump 1234 are coincident for the period of the installation, i.e. the state S1 of Pump 1234 that is installed as TAG P101 is in fact also a state of TAG P101. TAG P101 consists of those states of the pumps that are installed in this location.

Inspection Processing Flow

29



ISPM Preventive Maintenance and Inspections Administration and Reporting Processes



Create PM Notification: PM Condition Rating

Partner

Notification: %000000000001 CR Vibration inspection: rotating weekly

Status: NOPR ORAS

Order: 40000044

Condition report | Inspection details | Activities | All tasks | Documents

Reference object

Functional loc.: E62B-23DT001 TURBINE DRIVER, RES...

Subject

Cond. rating: CR000200 CR01 Acceptable/Normal: test passed

Description: Vibration inspection: rotating weekly

Responsibilities

Planner group: MNT / 7770 Maintenance

Main WorkCtr: MECH_SUP / 7770 MECHANICAL SUPV. O&M (EC)

Department resp:

Person respons.: 63049 Bruce Martin Green

Reported by: Ciliberti Notif.date: 12/14/2009

Catalog Selection

- Cond. rating Equipment condition rating
 - CR000200 General assessment
 - CR01 Acceptable/Normal: test passed
 - CR02 Acceptable until next mtce interval
 - CR03 Unacceptable: revisit prior to next PM
 - CR04 Unacceptable: test failed, repair now

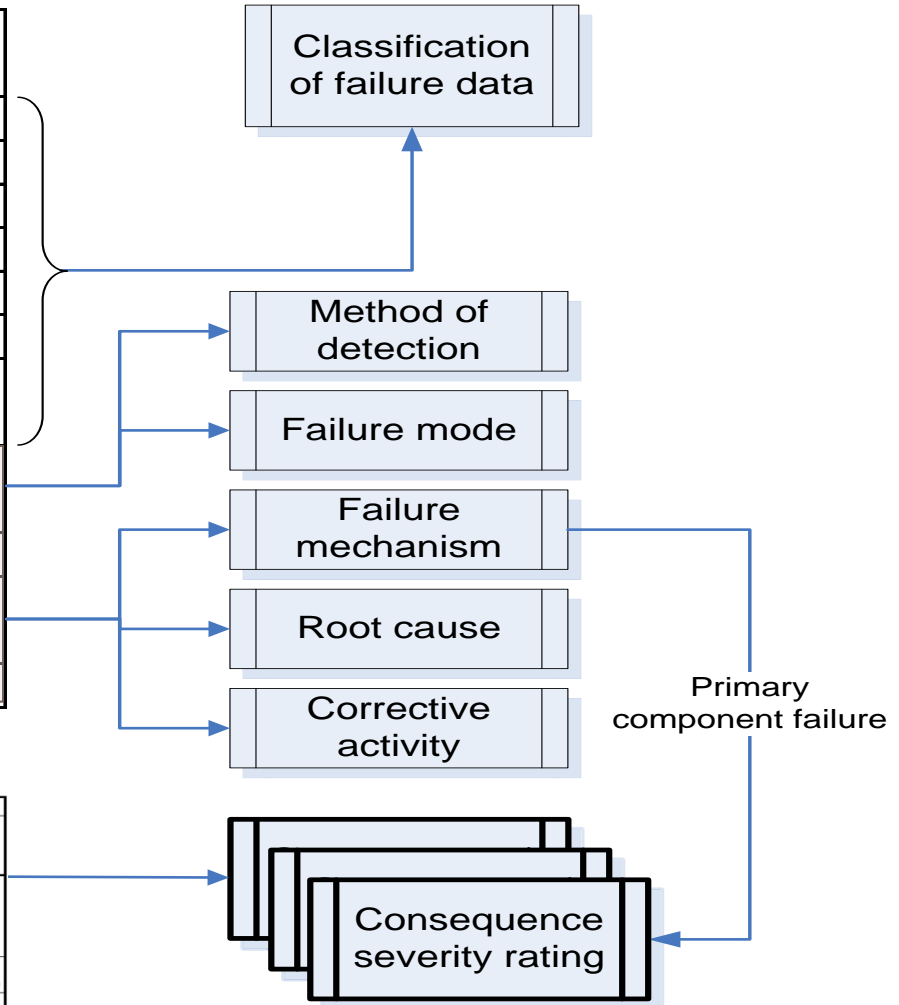
Main category	Level	Taxonomy hierarchy
Use/location data	1	Industry
	2	Business category
	3	Installation category
	4	Plant/Unit category
	5	Section/System
	6.1	Equipment Class
Equipment subdivision	6.2	Equipment Unit functional spec.
	6.3	Equipment Unit Asset (S/N)
	7	Subunit
	8	Component/Maintainable item
	9	Part

ISO 14224:2006(E)

Table C.1 — Failure-consequence classification

Consequences	Category			
	Catastrophic Failure that results in death or system loss	Severe Severe injury, illness or major system damage (e.g. < USD 1 000 000)	Moderate Minor injury, illness or system damage (e.g. < USD 250 000)	Minor Less than minor injury, illness or system damage (e.g. < USD 50 000)
Safety	I — Loss of lives — Vital safety-critical systems inoperable	V — Serious personnel injury — Potential for loss of safety functions	IX — Injuries requiring medical treatment — Limited effect on safety functions	XIII — Injuries not requiring medical treatment — Minor effect on safety function
Environmental	II Major pollution	VI Significant pollution	X Some pollution	XIV No, or negligible, pollution
Production	III Extensive stop in production/operation	VII Production stop above acceptable limit ^a	XI Production stop below acceptable limit ^a	XV Production stop minor
Operational	IV Very high maintenance cost	VIII Maintenance cost above normal acceptable ^a	XII Maintenance cost at or below normal acceptable ^a	XVI Low maintenance cost

^a It is necessary to define acceptable limits for each application.



ISO 14224 Gas Turbine Equipment Subdivision

Equipment unit	Gas turbines						
Subunit	Starting system	Air intake	Combustion system	Compressor	Power turbine H P turbine	Control and monitoring	
Maintainable items	Starting motor Start control Piping Filter(s) Valve(s) Pump(s) Start energy (e.g. battery, air)	Air cooling Anti-icing Filters Intake duct Inlet vanes	Combustor Fuel nozzles Seals	Rotor Stator Cooling system VGV system Anti-surge valve Aux. bleeding system Anti-icing valve Casing Radial bearing Thrust bearing Seals Piping	Rotor Stator Casing Radial bearing Thrust bearing Seals Valves Piping	Control unit Sensors ^a Wires Actuating devices Monitoring Valves Internal power supply Seals	
	Lubrication system	Fuel system	Water/Steam injection ^b	Fire and gas protection	Accessory drive	Exhaust	Miscellaneous
	Heater Reservoir(s) Pump(s) Motor Filter Temperature control Valves Piping Oil cooler Oil Sensors Wires	Fuel control Piping Valves Seals Pump(s)/Gas compressor Filter(s)/Separators Wires Fuel properties measurement	Pump(s) Piping Valves Filter(s) Seals Wires	Control unit Pipes Valves Sensors Wires Tank(s)/Storage	Gearbox Bearing Seals Casing	Diffuser Exhaust collector Compensator/bellows Ducting Emission monitoring Silencer Thrust bearing Valves Waste heat recovery unit	Enclosure Hood Purge air Flange joints Ventilation fan Water-wash system
^a Specify type of sensor, e.g. pressure, temperature, level, etc. ^b Only relevant for gas turbines with NO _x -abatement control with steam or water.							

Relief valve inspection on two-year interval generates one order for a plant section, e.g. Distillation, with instructions to “test/inspect all relief valves”

- No tag numbers given

Devices pulled from field, replaced with spares, and sent for testing to external service provider

- No checklist to ensure all devices are pulled
- Loss of traceability: where did each valve come from?

Devices sent back from supplier with test results affixed to them

- Some reports get lost
- Failed tests may not be addressed: may not get reviewed, may sit in a pile on an engineers desk, etc.

Inspection results scanned and attached electronically to relevant equipment objects

- The wrong object type may be used

Regardless of results, the inspection is reissued two years later

Inspection Scope

- 6.2.3 Note operating conditions/relieving events while in service
- 6.2.6 Inspection adjacent piping
- 6.2.8 As-received pop-pressure
- 6.2.9 Visual inspection
- 6.2.11 Inspection of components

6.4.1 Frequency of Shop Inspection/Overhaul


6.4.1.1 Normal Basis

Normally, the interval between shop inspection/overhaul of pressure-relieving devices should not exceed that necessary to maintain the device in satisfactory operating condition. The frequency of shop inspection/overhauls is normally determined by operating experience in the various services involved. Normally, the interval of a device in a corrosive and/or fouling service would be shorter than the interval required for the same device in a clean, non-fouling, non-corrosive, service. Likewise, more frequent inspection and testing may be needed for pressure relief valves subject to vibration, pulsating loads, low differential between set and operating pressures, and other circumstances leading to valve leakage and poor performance.

Where an adequate inspection or test history extending over a long period of time reflects consistent "as received" test results that coincide with the CDTP (see 6.2), where no change in service is to be made, and where no conflict in jurisdictional requirements exists, an increase in the test interval may be considered. Conversely, if the "as received" test results are erratic or vary significantly from the CDTP, the inspection interval should be decreased or suitable modifications to improve the performance should be made. If a valve fails to activate on the test block at 150% or more of CDTP, it can be assumed that it would have failed to activate on the unit during an overpressure event.

Where corrosion, fouling, and other service conditions are not known and cannot be predicted with any degree of accuracy (as in new processes), the initial inspection should be accomplished as soon as practical after operations begin to establish a safe and suitable testing interval.

Sample Relief Device Inspection Report

 Score AIS <small>Relief Valves and Gas Turbine Solutions™</small> <small>www.scoreais.com</small>		Tel: +47 51 43 23 00 Fax: +47 51 43 23 23 Email: scoreais@score-group.com	Field: <u>Alvheim</u> Report No: <u>1376287</u>
PSV Certificate and Report			
Tag No: <u>44-PSV-0134 A</u>	Customer Ref: <u>N/D</u>	Score Job Number: <u>220083</u>	
Sap No: <u>11680078</u>	Location: <u>ALVICIM</u>	Equipment Line: <u>WATER DEGASSING DRUM</u>	
Date Last Inspection: <u>N/D</u>	Service Duty: <u>GAS</u>		
Type of Inspection: <u>TEST & CERTIFY</u>			
Date of Inspection: <u>03.04.2009</u>			
Nameplate Details			
Make: <u>CROSBY</u>	Set Pressure: <u>14 BARG</u>		
Model: <u>8TJBS-E-45-J-SPL</u>	C.D.T.P.: <u>14.14 BARG</u>		
Serial No: <u>321410</u>	Back Pressure: <u>2 BARG</u>		
Inlet Size: <u>8" 300# RF</u>	Orifice: <u>T</u>		
Outlet Spacco: <u>1C" 150# RF</u>	Spring Range: <u>N/D</u>		
Body Material: <u>N/D</u>	Trim material: <u>ST/ST</u>		
Belows Fitted: <u>YES</u>			
Pre Overhaul Test Results			
Pre Pop Lift 1: <u>14.2 BARG</u>	Pre Pop Lift 2: <u>14.2 BARG</u>	Pre Pop Lift 3: <u>14.2 BARG</u>	
Conventional / Bellows Valve Seal Leakage at 90% C.D.T.P.: <u>ZERO</u>			
Pilot Operated Valve Nozzle/Seat Test at 55% C.D.T.P.: <u>N/A</u>			
Back Pressure Test: <u>1 BARG</u>	Vacuum Test: <u>N/A</u>		
Test Details			
Test Specification: <u>API-527</u>			
C.D.T.P.: <u>14.14 BARG</u>	Test Medium: <u>NITROGEN</u>		
1 Lift: <u>14.14 BARG</u>	2 Lift: <u>14.14 BARG</u>	3 Lift: <u>14.14 BARG</u>	
Back Pressure Test: <u>2 BARG</u>	Blow Down Rings Set: <u>AS SET</u>		
Leakage at 90 % of C.D.T.P.: <u>N/A</u>	Seal Leakage: <u>N/A</u>	CC's: <u>ZERO</u>	BPM: <u></u>
Remarks/Recommendations:			
VALVE PRE POP FINE, VALVE TESTED TO SPECIFICATION. ALL TESTS PROVED SATISFACTORY. VALVE WIRELOCKED, LEADSEAL ED AND FITTED WITH A SCORE TEST DATA TAG.			
Inspection Engineer, Sign/Date: _____	Tested By: <u>H. Henriksen</u>		
Inspection Period: _____	<u>KLTA</u>		
Limitations: _____	Witnessed By: <u>R. Blaw</u>		
Date Next Inspection Major: _____	<u>Richard Blaw</u>		
Date Next Inspection Special: _____			
Senior Inspection Engineer, Sign/Date: _____			
Comments: _____	DCC Onshore: _____		

1910.119(j)(4) Inspection and testing.

1910.119(j)(4)(i) Inspections and tests shall be performed on process equipment.

1910.119(j)(4)(ii) Inspection and testing procedures shall follow recognized and generally accepted good engineering practices.

1910.119(j)(4)(iii) The frequency of inspections and tests of process equipment shall be consistent with applicable manufacturers' recommendations and good engineering practices, and more frequently if determined to be necessary by prior operating experience.

1910.119(j)(4)(iv) The employer shall document each inspection and test that has been performed on process equipment. The documentation shall identify the date of the inspection or test, the name of the person who performed the inspection or test, the serial number or other identifier of the equipment on which the inspection or test was performed, a description of the inspection or test performed, and the results of the inspection or test.

1910.119(j)(5) Equipment deficiencies. The employer shall correct deficiencies in equipment that are outside acceptable limits (defined by the process safety information in paragraph (d) of this section) before further use or in a safe and timely manner when necessary means are taken to assure safe operation.

Advantages

- Administered at a high level (e.g. area) with reporting at the individual equipment level
 - Multiple equipment inspections grouped into one plan/inspection order
 - All equipment items can be identified by unique tag numbers
 - All inspection steps apply to all equipment objects
 - Assign inspection characteristics to one or more inspection steps
 - Equipment-specific findings are documented with notifications and, where applicable, inspection lots and measurement points
 - Findings can be documented either (1) for all inspected objects or (2) only for exceptional conditions

Disadvantages

- Difficult to change inspection frequency for individual equipment items
- Change to inspection scope requires an assessment of impact to all affected items
 - Should be addressed with Management of Change

1910.119(I)(1) The employer shall establish and implement written procedures to manage changes (except for “replacements in kind”) to process chemicals, technology, equipment, and procedures; and, changes to facilities that affect a covered process.

1910.119(I)(2) The procedures shall assure that the following considerations are addressed prior to any change:

1910.119(I)(2)(i) The technical basis for the proposed change;

1910.119(I)(2)(ii) Impact of change on safety and health;

1910.119(I)(2)(iii) Modifications to operating procedures;

1910.119(I)(2)(iv) Necessary time period for the change; and,

1910.119(I)(2)(v) Authorization requirements for the proposed change.

Appendix

Examples of Risk Management

Very High (VH)

- Major production loss: 2,000,000 ++ BBLs.
- Financial impact at a corporate level: >\$10,000,000 USD

High (H)

- Significant loss of production capacity (50-100%) for short term (<10 days): 200,000-2,000,000 BBLs.
- Loss of production capacity (10-50%) for long term (>10 days): 200,000-2,000,000 BBLs.
- Financial impact at a facility level: >\$1,000,000 USD

Medium (M)

- Loss of production capacity (10-50%) for short term (<10 days): 20,000-200,000 BBLs.
- Minor loss of production capacity (<10%) for long term (>10 days): 20,000-200,000 BBLs.
- Financial impact at a unit level: >\$100,000 USD

Low (L)

- Minor loss of production capacity (<10%) for short term (<10 days) or minor financial impact

Negligible (N)

- Process capability not impacted or repair costs <\$10,000 USD

Very High (VH)

- Multiple fatalities of company or associated personnel.
- Severe injury, illness, or fatalities of one or more members of the community.
- Catastrophic environmental impact requiring a full-scale response by outside agencies.

High (H)

- Death of one company or associated person.
- Severe injury or illness of multiple plant personnel.
- Major reportable environmental incident resulting in action by regulatory agencies, significant media and/or company resource commitment.

Medium (M)

- Severe injury or illness of one company or associated person. Medical treatment required for multiple plant personnel.
- Major reportable environmental incident unlikely to result in action by regulatory agencies and would attract little or no media attention.

Low (L)

- Minor medical treatment required for one or more company or associated personnel.
- Minor reportable environmental incident: an incident that would not cause regulatory action and would attract no media attention.

Negligible (N)

- Minimal safety consequences. Non-reportable environmental incidents.

Very High (VH)

- One or more occurrences are credible annually.

High (H)

- Several occurrences are credible in the facility lifetime.

Medium (M)

- One occurrence is credible in the facility lifetime.

Low (L)

- Not expected to occur in the facility lifetime but not impossible.

Negligible (N)

- Practically impossible

Normalizing Risk Rating: Qualitative and Quantitative Data

Consequence/ Economic Loss	VH	1.00E+08	\$1,000	\$10,000	\$100,000	\$1,000,000	\$10,000,000
	H	1.00E+07	\$100	\$1,000	\$10,000	\$100,000	\$1,000,000
	M	1.00E+06	\$10	\$100	\$1,000	\$10,000	\$100,000
	L	1.00E+05	\$1	\$10	\$100	\$1,000	\$10,000
	N	1.00E+04	\$0	\$1	\$10	\$100	\$1,000
Order-of-Magnitude Exposure		1.00E-05	1.00E-04	1.00E-03	1.00E-02	1.00E-01	
		N	L	M	H	VH	
		Likelihood					

- Red Zone: risk mitigation required
- Gray Zone: risk mitigation recommended
- White Zone: acceptable risk

Safeguards should be discretely identified and given risk reduction credit for each scenario in which they are involved.

$$S_T = \sum_{i=1}^n \{(L_i C_i - l_i C_i) + (L_i C_i - L_i c_i)\}$$

Where:

- S_T = Total safeguard risk reduction for n scenarios
- = Safeguard priority rating
- L_i = Likelihood of consequence i before application of safeguard i
- C_i = Consequence of scenario i before application of safeguard i
- l_i = Likelihood of consequence i after application of safeguard i
- c_i = Consequence of scenario i after application of safeguard i

Risk of Operating Harley Davidson FXDWG

Safeguards

- **Helmet**
- Protective clothing
- Motorcycle safety class
- Defensive driving

Consequence/ Economic Loss	VH	1.00E+08	\$1,000	\$10,000	\$100,000	\$1,000,000	\$10,000,000
	H	1.00E+07	\$100	\$1,000	\$10,000	\$100,000	\$1,000,000
	M	1.00E+06	\$10	\$100	\$1,000	\$10,000	\$100,000
	L	1.00E+05	\$1	\$10	\$100	\$1,000	\$10,000
	N	1.00E+04	\$0	\$1	\$10	\$100	\$1,000
HD Wide Glide with Helmet			1.00E-05	1.00E-04	1.00E-03	1.00E-02	1.00E-01
			N	L	M	H	VH
			Likelihood				
Consequence/ Economic Loss	VH	1.00E+08	\$1,000	\$10,000	\$100,000	\$1,000,000	\$10,000,000
	H	1.00E+07	\$100	\$1,000	\$10,000	\$100,000	\$1,000,000
	M	1.00E+06	\$10	\$100	\$1,000	\$10,000	\$100,000
	L	1.00E+05	\$1	\$10	\$100	\$1,000	\$10,000
	N	1.00E+04	\$0	\$1	\$10	\$100	\$1,000
HD Wide Glide without Helmet			1.00E-05	1.00E-04	1.00E-03	1.00E-02	1.00E-01
			N	L	M	H	VH
			Likelihood				

Remove each safeguard one at a time while holding the others constant

Calculation of safeguard priority for motorcycle helmet

- $C = c = \$10,000,000$
- $L = 0.1$
- $I = 0.001$
- Since $C = c$ and only one consequence is considered, the formula reduces to:
 - $S_T = C(L - I) = \$10,000,000 * (0.1 - 0.001) = \$990,000$

But...how effective is the helmet?

- Does the rider wear it?
- Has it been dropped?
- Is the chin strap properly secured?
- Assumed risk reduction is \$990,000...what is the realized risk reduction?

Table 1. Examples of Benefit-to-Cost (BTC) Evaluations for Safeguards.

Item notes (risk zones for items not shown):

1. The BTC Ratio is low and pre-safeguard risk is in the white zone. No action recommended.
2. The BTC Ratio is greater than 0.5 and pre-safeguard risk is in the gray zone. The safeguard (spare bundle) lowers risk into the white zone. This action is recommended.
3. This item evaluates risk associated with removal of a safeguard. Risk would increase from white zone to red zone if this change was made. No action/change to PM recommended.

Item	Exposure	Scenario ID	Event Description	Action	Cost	New Exposure	Risk Delta	BTC Ratio
1	\$ 1,100	1817	Failure of TP2 crude feed/cold residue exchanger	Add tube bundle to stock	\$ 13,000	\$ 1,010	\$ 90	0.007
2	\$11,000	1821	Failure of one desalted crude/hot residue exchanger	Add tube bundle to stock	\$ 13,000	\$ 2,000	\$ 9,000	0.692
3	\$ 2,000	2434	Common cause failure of Caterpillar field gensets	Increase service interval to 3000 hours versus current 1500-hr interval	\$ (876,000)	\$ 2,000,000	\$(1,998,000)	-2.281

Table 2. Example of an Automated Safeguard Effectiveness Report for Materials Safeguards.

Risk Delta (US\$)	Scenario	Consequence Description	Material	Material Description	On Hand
\$ 9,000	Failure of one TP1 crude feed/hot residue exchanger	Topping Plant 1 shutdown	108182	Exchanger, bundle & exchanger head crude feed/hot residue Product & Diesel PLT# e-21034A/B dwg#925-209-a w/ bundle & exchanger head gaskets	0
\$ 90,000	Failure of topping plant residue pump(s)	Topping Plant 1 shutdown	128186	Pump, centrifugal 2x3x13 model VLK I/ motor duplicate of S/N CH92290AX ATM residual 158 GPM API class S-6 steel casing material 12% chrome SS impeller 12% chrome SS wear ring 12% chrome SS shaft 300 ANSI RF flanges carbon 316 SS backed throat bushing di	0
\$ 90,000	Failure of topping plant residue pump(s)	Topping Plant 1 shutdown	129848	Seal, mechanical John Crane 609 (715) tandem drawing #HSP-1005864-1 w/ pumping rings / glands / heads with mating rings f/ 3 x 4 x 13C VLK pump	0