Risk Matrix for SIL allocation (HES) according to IEC 61511

Consequence classes								Frequency classes of the hazardous event		
								Return period (x times / year)	Demand Rate (every *x* year)	Examples
acceptable no action	**change design b)** (1 IPL)	**change design b)** (3 IPL)	**Unacceptable change design c)** (4 IPL)	**Unacceptable change design c)** (4 IPL)	**Frequency Go one step down for "Rare Mode of Operation"**	probable	more than once per year	**F4**	> 2	< 0.5	* failure of analyzer or gas chromatograph (all types)
acceptable no action	**Transition**	**Medium 2 IPL** (SIL2)	**High 3 IPL** (SIL3)	**Unacceptable change design c)** (4 IPL)		likely	once per year	**F3**	2 to 0.25	0.5 to 4	* operator failure (no established procedures available) * failure of rotating equipment (e.g. pump, compressor, blower) * power supply local failure
acceptable no action	**Transition**	**Low 1 IPL** (SIL1)	**Medium 2 IPL** (SIL2)	**High 3 IPL** (SIL3)		possible	once in a turnaround period	**F2**	0.25 to 0.05	4 to 20	* control loop failure or critical failure of a BPCS * control valve fails to regulate * shut-off valve, ESD-valve or control valve with solenoid valve moves to unwanted or fail position * operator failure (fail to follow established procedures) * tube leak within a heat exchanger * failure of 2* 100% pumps with auto start with independent power supply * failure of expander/turbine with autom. 100% bypass
acceptable no action	**acceptable no action**	**Transition**	**Low 1 IPL** (SIL1)	**Medium 2 IPL** (SIL2)		unlikely	once in plant lifetime	**F1**	0.05 to 0.01	20 to 100	* tube rupture within a heat exchanger * leak in a plate (fin) heat exchanger (< 100 mm²) * occurs once in the lifetime of the plant
acceptable no action	**acceptable no action**	**Transition**	**Transition**	**Low 1 IPL** (SIL1)		very unlikely	once in the lifetime of 10 plants	**F0**	*< 0.01*	*> 100*	** double/multiple jeopardy (quantitative assessment)*

		Consequence classes				
		negligible	minor	moderate	serious	major
		C1	**C2**	**C3**	**C4**	**C5**
Injury to Personnel (first party)		no injuries	slight and reversible injuries	irreversible injuries like burns or inhalation of toxic gases	serious permanent injuries to max. two persons	heavy permanent injuries to several persons (≥3)
Fatalities (first party)		no	no	no	single fatality (1-2)	multiple fatalities (≥3)
Public (third party)		no impact	no impact	no injuries minor impact	injuries major nuisance	one or more fatalities
Environment (water, air, soil)		no release expected	On-site: small contained non reportable release or reversible soil contamination	On site: large contained reportable release or Off-site: minor, but reportable release or moderate flaring	Off-site: moderate reportable release or temporary harmful environmental affects (e. g. agricultural areas cannot be used at least one year for cultivation). or serious and long-lasting flaring	Off site: large reportable release off-site or permanently high harmful environmental affects or heavy and long-lasting flaring
Stress Classes	Operation range		up to allowable design conditions	up to test pressure or yield stress conditions	above the test pressure or yield stress conditions	
	Pa achievable pressure		$P_a \le P_D$ *1,1	P_D *1,1 < $P_a \le$ P_D*1,5 (min. SIL 1, note *8)*	$P_a > P_D$ *1,5 (note *7)*	
	Ta high achievable temp. *note 4), note 5)*		$T_a < T_D$ + 50 K *note 4), note 5)*	T_D + 50 K < T_a $T_a \le T_D$ + 200 K *note 4), note 5)*	$T_a > T_D$ + 200 K *note 4), note 5)*	
	Ta low achievable temp.			$T_D > T_a \ge$ MDMT – 10 K *note 6)*	$T_a <$ MDMT -10K *(note 6)*	
Personnel Risk Examples	**Physical energy release (all type of fluids)**		unwanted operational condition	leakage at flange causing injury to personnel by e.g. hot steam, high pressure liquid	equipment failure causing fragmentation, shrapnel and blast	n/a
	Risk of explosion or fire		unwanted operational condition	Leakage at flange Defined leak flow rate small restricted fire	formation of explosive gas/air mixtures with a flammable gas quantity (note 1) of **less than 5000 kg**	formation of explosive gas/air mixtures with a flammable gas quantity (note 1) of **more than 5000 kg**
	Risk of asphyxiation (lack of oxygen)		one person exposed to less than 19.5% vol% of O2	one person exposed to less than 17% vol% of O2	one person exposed to less than 12% vol% of O2	more than 3 persons exposed to less than 12% vol% of O2
	Oxygen enrichment Risk of fire of clothing of exposed personnel (dispersion calculation required) (note 9)		one person exposed to more than 23.5% of O2 (note 10)	one person exposed to more than 30% of O2	one person exposed to more than 35% of O2	more than 3 persons exposed to more than 35% O2
			For group of persons, who - are not aware being exposed to O2, and do not know how to behave after exposure - are not generally trained for use of O2 - are outside the fence or outside of the process plant (e.g. ASU) or any third party or any public area - are additionally exposed to uncontrollable ignition sources, like sparks, ash from smoking, oil and dirt, the oxygen level should be as close as possible to a limit of 21% O2 but shall never be higher than 23%.			
	Risk of Toxication (dispersion calculation required)		n/a	persons exposed to	persons exposed to	persons exposed to
	outside process plant (outside fence)		n/a	> AEGL 1	> AEGL 2	> AEGL 3
	within process plant complex		n/a	> AEGL 2	> AEGL 3 (limited area, e.g. < 2500 m^2)	> AEGL 3

Remarks

Transition: Risk reduction by a (safety) protection function and/or mitigation feature with an effort as low as reasonable practicable (e.g. trip function in BPCS, control valve to be closed via solenoid, high priority alarm etc.) without providing an (additional) SIL classified safety instrumented function. The used protection function and/or mitigation feature including the acceptability of its risk reduction ability shall be agreed in the project´s SIS Safety Team.

b) other risk reduction measure (other than SIS) to be installed

c) change in concept, design or construction

Notes:

1) gas quantity = equipment content * flash rate + gaseous flows for 5 minutes coming from connected items.

2) not used

3) LOC (loss of containment) is a spontaneous release of the gaseous or liquid inventory of a vessel and the subsequent leak flow rate fed by the connected systems.

4) only for Carbon Steel and Stainless Steel T_a < 250 °C, not for Aluminum

5) valid for vessel code AD2000;
exception: for carbon steel vessel accord. to ASME VIII Div. 1 :
for T < 310 °C no LOC

6) Ta < MDMT accord. to ASME UCS66 curve. Excess of MDMT is possible in case of reduced stress like lower pressure

7) Factor 1,5 may be increased up to the limit of yield strength.
(Factor 1.5 is the min. safety margin related to the yield strength. The factor is related to the ratio "pressure at yield strength"/"design pressure")

8) The minimum requirement SIL 1 is only required if a safety valve is replaced by a SIS or the size of the safety valve is reduced by the SIS (not valid for tube rupture)

9) EIGA Position Paper PP-14 –August 2006

10) Generally a concentration of 23.5% O2 shall not be exceeded in 2 m above ground and on any working platform. Only for discontinuous release (less than 20% of the time) a limit of 25 % O2 may be used for working platforms with access control (limited access).

Abbreviation:

HES	Health, Environment and Safety
HMI	Human Machine Interface
ESD	Emergency Shut-Down
ASU	Air Separation Unit
IPL	Independent protection layer
SIF	Safety Instrumented Function
SIS	Safety instrumented system
SIL	Safety integrity level
PFD	Probability of failure on demand
BPCS	Basic process control system
PLC	Programmable Logic Controller
T_D	Design Temperature (MAWT=Maximum Allowable Working Temperature)
P_D	Design Pressure (MAWP Maximum Allowable Working Pressure)
LOC	Loss of Containment
MDMT	Minimum Design Metal Temperature (certified)
n/a	not applicable

AEGL:	AEGL Acute Exposure Guideline Levels. Other exposure times can be used for AEGL evaluation after detailed scenario analysis. If AEGL values are not available, ERPG levels can be used instead.
AEGL-1:	Threshold for notable discomfort (based on 1 hour exposure)
AEGL-2:	Threshold for serious, long-lasting effects or an impaired ability to escape (based on 1 hour exposure)
AEGL-3:	Threshold for lethal effects (based on 1 hour exposure)

Table: Independent protection layers

Type	Description	IPL value[1]
Standard design features	Two check valves in series (untightness to be considered)[2]	**1**
Safety protection installation	Independent SIF having SIL1 classification	**1**
	Independent SIF having SIL2 classification	**2**
	Independent SIF having SIL3 classification	**3**
	Independent hardwired relay switch function having SIL1 classification	**1**
	Independent hardwired relay switch function having SIL2 classification	**2**
	Independent hardwired relay switch function having SIL3 classification	**3**
	Safety valves or rupture disc sufficiently sized for the scenario Provided that clean service (i.e. purged if necessary for severe service e.g. dirt, polymers), proper selection, proper installation (including adjacent piping) and adequate maintenance are ensured.	**3**
	Flame arrestor	**1**
	Interlocking acc. LS 802-23 or key-locking devices with clear operating procedure (e.g. LO - locked open) The lock shall be direct-mounted on the valve and shall not be removable. The key position shall be indicated on the key cabinet in the control room.	**3**
	Simple locking device with clear operating procedure (e.g. CSC - Car Seal Closed, shackle lock). The use of this type shall be approved by the plant owner and shall be according to the plant owners operation and maintenance philosophy. [3]	**1**

[1] In case of deviation from the given IPL values, a separate risk assessment shall be conducted and documented.

[2] For check valve leakage and failure refer to API 521: "The user might want to consider dissimilar reverse flow prevention devices (e.g. swing check and a piston check valve). For two or more check valves in series that are internally inspected and maintained to demonstrate reliability, only normal check valve leakage may be assumed."

[3] Simple locking device with clear operating procedure may be rated higher than 1 IPL if accepted by the plant owner and local authorities. When used for over pressure protection it shall be allowed by the applicable code for pressure vessels.

Type	Description	IPL value[1]

Operator action	The use of an operator as one independent protection layer (IPL) is acceptable if all following points are fulfilled:
	• the process is operated by skilled personnel
	• the sensor used for the alarm system is not used for control purposes where loss of control would lead to a demand on the SIF
	• alarm signal routed via safety system or different / independent BPCS controller (independent of system which initiates the hazard, incl.HMI (e.g. different HMI for PLC and BPCS))
	• common cause issues have been considered
	• alarms alert before reaching the hazardous event (fully independent from the safety instrumented function, i.e. the sensor used for the alarm system is not used as part of the SIF)
	• there is a direct connection between the alarm, which indicates the hazardous event, and the measures to be taken by operator to avoid the event
	• classification of the alarm as “high priority”
	• description of the alarm and the measures to be taken in the safety chapter of the operating manual and training of the operator to carry out the required actions
	• enough time to carry out the necessary measures to avoid the hazardous event (slow development of the hazardous event)
	Herein the following time periods apply (to be clarified with client):
	  • 10 minutes for routine operation (more than once a week)
	  • 30 minutes for seldom operation (more than 4 times a year) and those which are part of the frequent training program
	
	Use of this IPL is not permitted to delete an instrumented function. Separate risk assessment to be conducted if no instrumented function to be installed.
		1

Type	Description	IPL value[1]
Occupancy (for risk to personnel only)	Rare to more often exposure in the endangered zone (~up to 20% of the time), e.g. • only during supervision rounds or maintenance within normal plant layout design (non-compact layout) • if the clearance of the dangerous situation does not require the presence of staff on the scene of action	**1**
	Frequent to permanent exposure in the endangered zone, e.g. • manned local control stands for machinery • operating staff, if the clearance of the dangerous situation does require the presence of staff on the scene of action • unprotected control room within the endangered area • population of housing areas, if the endangered area will extend over the complex border line • very compact plant design • if the hazardous event occurs during start-up the occupancy may be higher than during normal operation	**0**
Other IPLs	Other non-listed protection measures (e.g. use of BPCS functions, mitigation measures like safe location, dike wall, hazardous area classification) can be used as layer of protection to reduce the overall risk. The number of IPLs for such non-specific protection measure shall be carefully discussed and agreed within the SIS Safety Team including the plant owner. Criteria like e.g. common cause failure, human factor or instrument reliability issues need to be considered with due care.	**To be agreed in SIS Safety Team**