Guidance Sheet SMP08/G/01 – Risk Reduction Checklist

The following paragraphs present a generic checklist for use in identifying options for reducing the risks associated with Hazards and Accidents relating to a system. Any such checklist must be used in a "brainstorming", imaginative way to stimulate discussions between stakeholders who have a good understanding of the system, its context and usage/maintenance environment. Checklists application in a narrow way or by those with an incomplete appreciation of the system will be very much less effective.

The checklist is for use in considering specific Hazards and Accident sequences identified for the system of interest. Safety Management requires that the Project development must also be subject to overarching good practices, including:

a. Quality;

b. Configuration Management;

c. Design Reviews;

d. Independent Review;

e. Closed-loop problem reporting and resolution;

f. Use of Suitably Qualified and Experienced Personnel (SQEP);

g. Focus on Safety Culture.

Order of Precedence for Risk Reduction Strategies

1. Eliminate the Hazard, possibly by re-specification or re-design of the system;
2. Incorporation of safety feature;
3. Incorporation of warning devices;
4. Operating and training procedures;
5. Warning signs and notices.

1. Hazard Elimination Strategies:

a. Eliminate the Hazardous substance or procedure;

b. Achieve the required capability by a different means;

c. Reduce the performance required.

2(a). Incorporate Safety Features Strategies (Hazard Controls):

a. Passive control – process inherently cannot run-away (laws of physics etc);

b. Hazard detection and automatic shutdown (eg trip systems, circuit breakers);

c. "Friendly design" such as:

i. Smooth control system response;

ii. Tolerance of mal-operation (design for recovery);

iii. Inability to mis-assemble;

iv. Design for disposal/dismantling;

v. Clear status visible on system components (eg valves);

d. Increased Integrity of Safety functions, through:
   i. Redundancy[1];
   ii. Diversity (different technology to achieve same function);
   iii. Failsafe design[2];
   iv. System monitoring (including Health and Usage Monitoring);
   v. Reallocate function to a different technology;
   vi. Increased Safety factors or margins;
   vii. Increased Reliability through stress de-rating;
   viii. Increased Reliability through improved component quality (including stress screening)
   ix. Increased Reliability through improved maintenance;
   x. Improved design for Human Factors for human Safety functions.

e. Increased integrity of Safety functions realised in software, through:
   i. Error detecting/correcting codes (eg parity or CRC check, hamming codes);
   ii. Full diversity (different software language running on different technology processor);
   iii. Software diversity[3] (not full diversity as same processor is used);
   iv. Defensive programming (ensure that variables cannot go out of range);
   v. Graceful degradation (if there are insufficient resources, prioritise functions and perform high priority ones);
   vi. Exception handling/error trapping. Trap run-time errors, then fail safe or reset[4];
   vii. Watchdog[5].

f. Physical protection measures such as barriers, shields, firewalls, blastwalls, guards, enclosures, interlocks, lock-off systems, exclusion zones, special atmosphere;

g. Remove people from Hazardous area (include making system remotely operated);

h. Reduce number of people exposed to Hazard;

i. Relocate Hazard away from other activities;

j. Controlled entry to Hazardous areas;

k. Automate certain functions or procedures;

l. Reduce Hazard in scale, eg:
   i. Substitute with a less Hazardous replacement (eg alternative substance, alternative technology);
   ii. Reduce inventory of Hazardous material;
   iii. Reduce Hazardous aspect (eg energy, pressure, voltage, temperature, height, speed, toxicity);

m. Attenuation – use material in least Hazardous form (eg slurry not dust);

n. Reduce usage rate of Hazardous aspect or frequency of Hazardous activity[6];

o. Special handling/support equipment or facilities;

p. Weak points/relief systems (eg fuses, Pressure Relief Valves, bursting discs);

---

[1] Must also consider vulnerability to dependent failures.

[2] Must consider all failure modes and wartime operation if relevant

[3] Implementing the same function in software two or more times on the same processor and using voting

[4] Often switched off because code runs too slowly.

[5] A process dedicated to monitoring the critical process, resets the critical process if it fails.

[6] Must beware of loss of skills.

q. Design for preferential lower severity failure mode (eg pressure vessel "leak before break");
r. Special coatings and treatments (eg fire-retardant, slip resistant, anti-bacterial);
s. Personal Protective Equipment (including harnesses);
t. Defence in depth (including physical measures such as containment or bunds for leakage).

2(b) Incorporate Safety Features Strategies (Accident Controls):

a. Emergency plans;
b. Evacuation plans;
c. Safe refuge;
d. Post-accident response;
e. Personal Protective Equipment (including harnesses);
f. First aid provision;
g. Fire-fighting arrangements;
h. Deluge/fire suppression;
i. Survival equipment;
j. Life-saving equipment.

3. Incorporate Warning Devices Strategies:

a. Alarm systems (including failsafe alarms which are normally active);
b. Warning buzzers, beacons and lights;
c. Stop lights.

4. Procedural Strategies:

a. Permit to work system;
b. Additional manpower to support operator during hazardous operations (eg safety man, banksman, banksman/slinger etc);
c. Independent review/checking of Safety-related tasks[7];
d. Inspection or functional test for dormant failures of Safety functions;
e. Inspection for incipient failures of Safety functions;
f. Human monitoring of Hazard areas;
g. Hazard control procedures in specific circumstances (eg de-icing);
h. Increased competence of personnel (eg through selection, training);
i. Refresher training to retain competence;
j. Emergency exercises/drills to examine competence.

5. Warning Information Strategies (not suitable as sole strategy for accident sequences with high severity consequences):

a. Warning signs and notices[8];
b. Warnings in manuals and written instructions[9].
c. Marked Hazard areas.

[7] Must consider vulnerability to dependent failures.

[8] Use standardised symbols, implemented to minimise probability of incorrect reaction.

[9] Must use standard notation and language for documented warnings.