MARSH

Energy Practice

RISK ENGINEERING POSITION PAPER – 03

MANAGING THE DEFEAT OF SAFETY INSTRUMENTED SYSTEM TRIPS AND ALARMS

SOLUTIONS...DEFINED, DESIGNED, AND DELIVERED.

MARSH & McLENNAN COMPANIES

CONTENTS

1. BACKGROUND

Safety instrumented systems (SIS) are used extensively in the hydrocarbon processing industry to protect against hazardous events. A simple example is the filling of a vessel with a toxic chemical. The hazard in the process is the overfilling of the vessel leading to a release via the relief valve. The overfill cause could be an operator error or a failure of the level control instrumentation. A SIS can be designed to shut off the flow to the vessel if the level reaches a hazardous condition. Importantly, the SIS must operate independently of the process control system.

Typically a SIS will be automatically activated, returning the process or equipment to a safe condition without operator input. However in some applications, a SIS can also take the form of a shutdown system requiring manual activation.

Many of these systems are designed with built-in defeat facilities that make use of key locks, hard or software switches at the control station. Furthermore, they can also be physically defeated by:

- Disconnecting the loop either at the sensing element (e.g. level indicator) or at the final element (e.g. emergency shutdown valve).
- Fixing the final element in the inactive position by wiring it, clamping it or removing its motive power source.

Whenever a SIS is defeated, the risk exposure is increased to an extent that depends on the nature of the hazard involved. The heightened risk exposure must be fully recognised, assessed, and shown to remain within acceptable limits – this may require the application of risk mitigation measures. Additionally, consideration must be given to the number and nature of defeats in place as well as their duration.

The degree of increased risk should be reflected in the level of authority and the extent of the risk review required to sanction application of the defeat. For example, the risk of defeating a defective SIS for one day to perform minor corrective maintenance would be significantly lower than defeating it for 12 months due to inaccessibility to carry out repairs without a shutdown. However, depending upon the materiality of the increased risk, in some cases defeating a SIS, even for a single shift, could be deemed unacceptable and thus an enforced shutdown to carry out the maintenance might be the only acceptable solution.

It follows then, that opting to defeat a SIS should not be an ad hoc decision and in some cases may never be an acceptable course of action. A system for managing the defeat of SIS trips and alarms should be robust enough to cater for all eventualities.

2. OBJECTIVE

The objective of this position paper is to define the standards that would be expected of a SIS trip and alarm defeat system rated by Marsh as very good in the oil, gas, and petrochemical industry. These standards are incorporated in the Marsh Global Energy Risk Engineering (GERE) risk ranking criteria. They can be used to support and define risk improvement recommendations and also to provide detailed advice to clients seeking to improve their SIS trip and alarm defeat management system.

3. SCOPE

These guidelines apply to any SIS which includes:

- Process and equipment trip systems which automatically shut down a process or machine in response to a process variable reaching a pre-set value that is considered to present a hazard to the plant. For example, over-speed and vibration trips on rotating machinery, low flow trips for furnaces, high-high level trips on tanks and vessels.
- Process safety systems that are automatically activated in response to a process variable reaching a pre-set value that is considered to present a hazard to the plant. For example, emergency depressurisation systems, HIPPS (high integrity pressure protection system), chemical reaction kill systems.
- Automatic safety systems that are activated by sensing devices for fire, smoke, gas, toxins or preset process operating conditions. For example: automatic starting systems on a firewater pump, automatic deluge systems, instrument cabinet fire suppression systems.
- Manually activated emergency shutdown and safety systems; these may be standalone or require the manual operation of an automatic system. For example: emergency shutdown systems on machinery and furnaces, remote operated emergency isolation valves, and remote operated deluge systems.
- Safety critical alarms requiring an operator to take averting action.

These guidelines do not apply to non-safety critical software systems such as process alarms configured in the distributed control system (DCS); nor do they apply to non-instrumented safety systems such as pressure safety valves (PSVs) which should have their own in-service control system.

"...opting to defeat a SIS should not be an ad hoc decision and in some cases may never be an acceptable course of action."

4. SPECIFIC REQUIREMENTS

The following details describe the framework for a management system governing the control of SIS trip and alarm defeats.

4.1 POLICY AND PROCEDURE

A SIS alarm and trip defeat management policy should define the background, scope, objectives, and requirements of the management system. Any follow-on procedure should be site specific and detail: the steps in the process; mitigation requirements; authorisation; time limitations and the recording process as outlined in the subsections below.

4.2 CATEGORIES

The reasons for defeating a SIS can be categorised as follows:

OPERATING DEFEATS

These are applied when the intended process conditions are expected to cause the SIS to be activated undesirably. In this instance, it should be the design intent that operating defeats are applied. Most likely, these defeats are used during start-up or planned shutdown operations and may incorporate a timer in the logic to regulate the duration of the defeat to fit the specific procedure. They could also be used during periodic operations such as a furnace de-coke or product changes.

Use of the defeat in such situations, including the reinstatement of the SIS after resumption of stable operation, should be included in the standard operating procedure (SOP). The SOP should also include the specific mitigating actions that need to be in place, such as a field operator on standby, or operating conditions to be maintained within strict limits in the absence of the SIS protection. The defeat and reinstatement steps in the procedure should be included in a "prompt and verification" sheet for operators to follow and use as a log for their actions during execution of the procedure.

MAINTENANCE DEFEATS

These are typically used for on-line testing and calibration of a SIS. They might be regularly applied and should be covered in the job plan and work instruction, and include detailed mitigating actions. As with operating defeats, the defeat application, and reinstatement steps in the work instruction should be included in a "prompt and verification" sheet for operators to follow and use as a log for their actions during execution of the procedure.

NON-ROUTINE DEFEATS

The circumstances requiring these defeats may vary considerably. An example might be faulty instrumentation awaiting investigation and repair.

There should be distinction between routine operating and maintenance defeats and the open-ended nature of non-routine defeats. Importantly, clear guidance should be given on the procedure to be followed for each category of defeat.

4.3 RISK ASSESSMENT AND MITIGATION

All defeats should be subject to a risk assessment and consideration should be given to the use of safety integrity level (SIL) ratings to determine the magnitude of the risk. A resulting risk mitigation plan should form part of the operating instruction and permit issue conditions (in the case of maintenance defeats) associated with the action being taken.

Given that operating and maintenance defeats are planned events rather than reactive responses, risk assessment, and associated mitigation steps should be prepared in advance. The mitigation steps should be embedded in the corresponding standard operating procedure (SOP) and work instruction. The risk assessments for maintenance defeats should be referenced in the permit covering the work and the mitigation steps should be listed in the permit issue conditions.

The nature and level of the risk determined prior to mitigation will inform which disciplines within the organisation should participate in the risk assessment and formation of the mitigation plan. Disciplines are likely to include a combination of operations, maintenance, inspection, engineering, and health safety and environment (HSE). Importantly, the level of authority required to approve the outcome of the risk assessment and mitigation should reflect the magnitude of the unmitigated risk. Once the risk assessment and initial mitigation plan have been developed, the risk level should be separately reviewed with mitigation in place to confirm that the risk is acceptable.

Consideration should be given to defining which safety instrument systems, or combination of systems, are not to be defeated during operation under any circumstances. Additionally, consideration should also be given to setting a limit for the maximum number of defeats that can be in place at any one time.

4.4 AUTHORISATION

There should be clear requirements regarding authorisation to both approve and carry out SIS defeats.

Operational and maintenance defeats within standard time limits should be approved by the senior person on shift. If the defeat duration exceeds the standard time limits, approval should escalate to a member of the site senior management team according to the level of risk. All non-routine defeats should be approved by a member of the site's senior management team.

Circumstances may arise where the emergency application of a SIS defeat is considered necessary to avoid an unplanned plant shutdown. Where the SIS is covered by an existing operating or maintenance defeat risk assessment, the senior person on shift should first confirm that the defeat is valid for the prevailing conditions before approving it.

"There should be clear requirements regarding authorisation to both approve and carry out SIS defeats."

Where the emergency application of a SIS defeat is not covered by an existing operating or maintenance defeat risk assessment, application simply to avoid a plant shut down should be managed with extreme care. The senior person on shift should gather all relevant information and carry out a dynamic risk assessment to determine the course of action. The evidence to support the risk assessment and mitigation in this instance should be compelling.

The senior person on shift should inform a site senior manager of the defeat application – ideally prior to application, but if that is not possible, soon afterwards and preferably prior to the end of the shift. The defeat management system should consider the point at which an on-call duty manager should be informed of a non-routine defeat application when outside of normal day work hours.

A point to note is that such emergency (i.e. non-routine) defeats of a SIS without a pre-existing risk assessment should be extremely rare. Each instance should be followed up afterwards (within a defined duration) by a formal risk assessment involving the appropriate team disciplines, with the results and any lessons learnt recorded, distributed, and acted upon accordingly.

All persons involved in the authorisation of the application of defeats should be identified and authorised to undertake the role. Qualification should encompass training, experience, and competency assessment.

All persons involved in the authorisation of the application of defeats should be identified and authorised to undertake the role.

4.5 TIME LIMITS FOR THE APPLICATION OF SIS DEFEATS

All defeats should have set time limits. Operating and maintenance defeats should be returned to active status within the working shift and working day respectively. Minor extensions should be approved by the senior person on shift in the event of short-lived work completion requirements.

Variable time limits for non-routine defeats should be set according to the level of risk they present post-mitigation. However, there should be a maximum time limit for any one defeat to be in place (ideally between one to four weeks). Beyond this, the defeat should be classified as a temporary management of change (MoC). The aim should always be to minimise the duration of a defeat application. Where it is known that the duration is likely to exceed the maximum time limit, a temporary MoC should be pursued from the outset.

Upon reaching the maximum time limit, extension of the defeat should be subject to the temporary MoC process. This should involve a multi-disciplinary review of the defeat risk assessment and mitigation plan, with mandatory approval required by the process safety or HSE discipline.

It would be expected that the temporary MoC process itself would have a maximum time limit before a permanent solution should be implemented.

“All defeats should have set time limits.”

4.6 SIS DEFEAT REGISTER

A formal method for registering, tracking, and reporting the status of defeats should be in place. The defeat register should be a dedicated entity, stored in an easily accessible location in the control room – readily available to provide a clear account of the individual and collective status of defeats across the site.

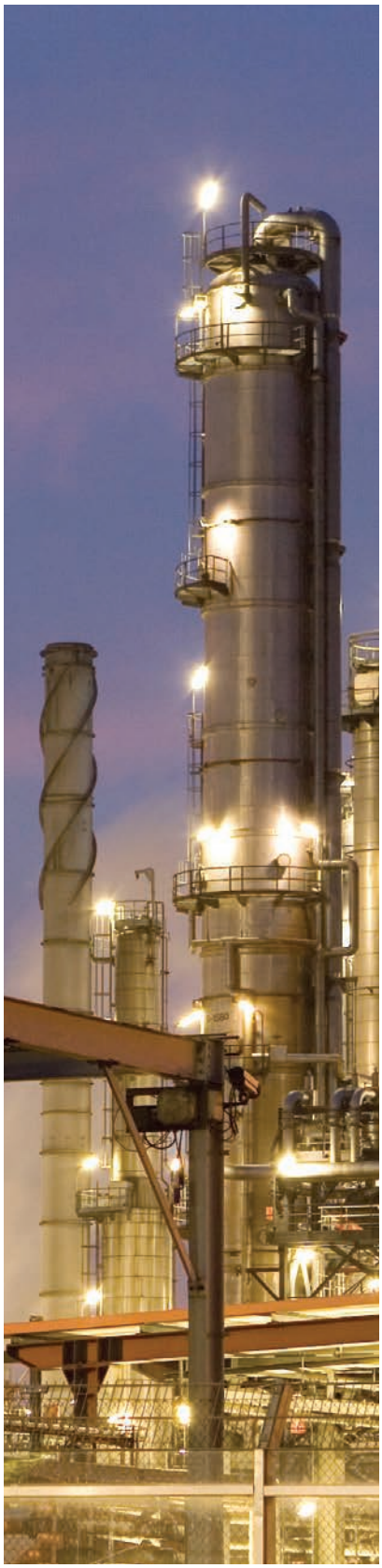
The register should comprise a control sheet for each defeat, detailing the following information:

- Details of the SIS to be defeated.
- SIL rating.
- Reason and purpose for the defeat.
- Time and date of the action.
- Method of the defeat.
- Reference to the risk assessment and risk mitigation plan (for maintenance and operating defeats).
- Confirmation that the risk assessment and risk mitigation plan (for non-routine defeats) is attached to the control sheet.
- Reference to the corresponding work permit number (where appropriate).
- Summary of the risk assessment and the mitigation actions required.
- Time limit (i.e. latest time and date to be reinstated).
- Defeat proposer name, signature plus time and date of signing.
- Defeat authorisation name(s), signature(s) plus time and date of signing.
- Senior person on shift.
- Senior manager (where appropriate).
- Time and date of reinstatement.
- Reinstatement names, signatures plus time and date of signing.
- Person undertaking re-instatement.
- Senior person on shift.

For operating and maintenance defeats, the corresponding risk assessment and mitigation plan should be referenced in the defeat control sheet. For non-routine defeats, copies of the risk assessment and risk mitigation plan should be attached to the defeat control sheet.

The defeat management system should ensure that the operator who physically implements the defeat has all of the relevant information available to them. Additionally, there should be an indication of the defeat in the shift log for the duration that it is in place. Importantly, a permanent record of the defeat should be recorded in the defeat register. To aid monitoring of defeats, entries in the register for live defeats should be segregated from closed (i.e. reinstated) defeats.

It should be noted that the defeat register should be the master controlling record of defeats. Other documentation such as shift logs, permits and work orders should be considered secondary to the defeat register.



The defeat register may take the form of loose-leaf printed paper, a pre-printed book or an electronic system (with the ability to print hard copy records).

4.7 MONITORING, REPORTING AND PERFORMANCE INDICATORS

Defeats should be monitored closely by the shift team – paying strict attention to the requirements of any specific mitigating actions. The status of all active defeats should be communicated at the formal shift handover; with the oncoming shift personnel reviewing the defeat register. Where there are status indicators for defeats on the instrument or DCS panel, these should be checked against the status according to the register and any variances investigated.

Irrespective of the various means of indicating the status of the defeats, the shift panel operator should maintain a list of the defeats that are in place for their particular area of responsibility in their shift log. They should verify this with the visible status indications (e.g. panel lights, DCS, key positions, etc.), and reconcile this with the defeat control sheet entries in the defeat register. This will ensure that the defeat status is tracked at all times.

As well as the inclusion of defeat control sheet copies, reference to all live defeats should additionally be recorded in the shift handover log.

The review of the defeat register by a senior manager should be a standing agenda item at the weekly operations meeting.

Process safety performance indicators (PSPIs) for defeat management should be developed and form part of the suite of PSPIs regularly reviewed by the site management (at least monthly). Defeat management PSPIs would typically include (but not be limited to):

- The number of defeats applied (broken down by type e.g. operating, maintenance, non-routine).
- The number of emergency defeats applied (broken down to show those that employed standard risk assessments, and those that did not).
- The number of time limit extensions.
- The number of overdue defeat reinstatements.
- Count of repeat application of specific non-routine defeats.

All non-compliances relating to defeat management should be reported as near-miss incidents and investigated accordingly.

4.8 AUDITING

Safety instrumented systems are identified as key layers of protection in controlling major accident hazards, hence inadequate management of defeats will lead to greater risk exposure. Auditing is a critical aspect of maintaining the standards for safely controlling SIS defeats; an audit plan would typically include the following:

- Weekly audit of the defeat register (part of a weekly operations audit).
- Annual audit of the defeat policy, procedure and register by the site process safety or HSE team.
- Periodic auditing of the defeat policy and procedure by the corporate audit team.
- Periodic auditing of the defeat policy and procedure by external agency auditors.

"Auditing is a critical aspect of maintaining the standards for safely controlling SIS defeats."

5. REFERENCE TO INDUSTRY LOSSES

EVENT DATE	21/03/1987
Country	United Kingdom
Location	Grangemouth, Scotland
Unit Type	Hydrocracker
Event	Explosion
Description	One person was killed following a major explosion and fire at the Grangemouth oil refinery. The incident occurred in the hydrocracker unit which was being recommissioned following repairs. Debris weighing several tonnes was propelled up to 1km away, in some instances off site. Rupture of a vessel occurred following breakthrough of high pressure hydrogen. A control valve did not close automatically because the low-low level trip on the HP separator had been disconnected several years earlier.
Position Paper Comment	The UK Health and Safety Executive final report concluded that the long term defeat of the low-low level trip on the HP separator contributed to the loss.

EVENT DATE	23/04/2004
Country	United States
Location	Illiopolis, Illinois
Unit Type	Plastics
Event	Explosion
Description	Five people were killed and two seriously injured following an explosion at a plastics plant producing 200 million bbls/yr of speciality grade PVC. The highway was shut and local residents evacuated. The explosion occurred in a chemical reactor where vinyl chloride and vinyl acetate where being mixed. Up to 75 percent of the plant was destroyed in the explosion. The explosion was felt 8 km away.
Position Paper Comment	The US Chemical Safety and Hazard Investigation Board (CSB) final report concluded that defeat control contributed to the loss.

EVENT DATE	28/08/2009
Country	United States
Location	Institute, West Virginia
Unit Type	Chemical
Event	Vessel rupture
Description	Eight people were injured and two killed following a vessel rupture event at a chemicals plant producing agricultural specialty products. The vessel ruptured as a runaway reaction created extremely high heat and pressure. The vessel, known as a residue treater, ruptured and flew about 50-feet through the air and demolished process equipment, twisted steel beams, and broke pipes and conduits.
Position Paper Comment	The US Chemical Safety and Hazard Investigation Board (CSB) report concluded that inadequate defeat control contributed to the loss.

THE ENGINEERING SERVICES TEAM

Marsh's Risk Engineering Services team has been established for over 25 years and is uniquely qualified to provide risk managers and underwriters with the essential information they need to determine the right limit and scope of cover and the right price.

Each member of the team is a qualified engineer, with practical experience in design, construction, operation, and maintenance across a broad range of oil, gas, and petrochemical risks.

They have all been trained in advanced insurance skills, in the ability to assess and analyse risk, and to communicate effectively and frequently in more than one language.

The goal is to build bridges between risk engineering, insurance and risk management, and between the client and the underwriter. At the same time, the comparative skills of the team permit a benchmarking system which gives a global opinion of the risk, assessed against peer plants world-wide.

From the earliest planning stage to the last operational phase, the engineering services team is able to contribute practical and cost-effective advice, and assistance.

In addition to tailored programmes, the team has a series of core packages, covering everything from managing a major emergency to risk reduction design features, and safe working practices.

The Engineering Services team uses its breadth of expertise, experience, and its practical knowledge and skills to communicate a real understanding of physical risks, your insurance implications and the commercial operating environment.

MARSH

For further information, please contact your local Marsh office or visit our web site at: marsh.com

BEIJING
Tel: +86 10 6533 4070
Fax: +86 10 8529 8761

CALGARY
Tel: +1 403 290 7900
Fax: +1 403 261 9882

CAPE TOWN
Tel: +27 21 403 1940
Fax: +27 21 419 3867

DUBAI
Tel: +971 4 223 7700
Fax: +971 4 227 2020

HOUSTON
Tel: +1 713 276 8000
Fax: +1 713 276 8888

LONDON
Tel: +44 (0)20 7357 1000
Fax: +44 (0)20 7929 2705

MADRID
Tel: +34 914 569 400
Fax: +34 913 025 500

MOSCOW
Tel: +7 495 787 7070
Fax: +7 495 787 7071

MUMBAI
Tel: +91 226 651 2900
Fax: +91 225 651 2901

NEW YORK
Tel: +1 212 345 6000
Fax: +1 212 345 4853

OSLO
Tel: +47 22 01 10 00
Fax: +47 22 01 10 90

PERTH
Tel: +61 8 9289 3888
Fax: +61 8 9289 3880

RIO DE JANEIRO
Tel: +55 21 2141 1650
Fax: +55 21 2141 1604

SAN FRANCISCO
Tel: +1 415 743 8000
Fax: +1 415 743 8080

SINGAPORE
Tel: +65 6327 3150
Fax: +65 6327 8845

Marsh is one of the Marsh & McLennan Companies, together with Guy Carpenter, Mercer, and Oliver Wyman.

The information contained herein is based on sources we believe reliable and should be understood to be general risk management and insurance information only. The information is not intended to be taken as advice with respect to any individual situation and cannot be relied upon as such.

In the United Kingdom, Marsh Ltd is authorised and regulated by the Financial Conduct Authority.

Copyright © 2015 Marsh Ltd
All rights reserved.