European Commission

Number 1
May 2013

MAHB Major Accident Hazards Bureau
Security Technology Assessment Unit

SEVESO COMMON INSPECTION SERIES CRITERIA

Safety Instrumented Functions

This publication of the European community on Common Inspection Criteria is intended to share knowledge about technical measures and enforcement practices related to major hazard control and implementation of the Seveso II Directive. The criteria were developed by Seveso inspectors to aid in dissemination of good enforcement and risk management practices for the control of major industrial hazards in Europe and elsewhere.

This particular issue highlights a number of issues that are critical for successfully reducing risks using safety instrumented functions. Note that this document is not intended as a technical standard nor as a summary or replacement of any existing standards on the matter.

Definition

A safety instrumented function (SIF) is a safety measure that senses a potentially hazardous condition and automatically performs an action to return the process to a safe condition. A SIF is implemented as a functional combination of one or more sensors, a logic solver and one or more final elements. A SIF will typically interrupt a chain of events, starting with a process upset and leading to a potentially hazardous situation. For a given SIF, this chain of events is referred to as the SIF-scenario (although the SIF in question might not be the only safety measure featuring in this scenario). A typical example of a SIF is a high level protection comprising one or more level detectors, a programmable logic controller (PLC) and one or more valves in the feed line that will be closed when the liquid level reaches the trip point. Another example might be a high pressure protection on a reactor that initiates an action to stop the reaction when temperature in the reactor reaches the trip point. This action can be: closing a valve or stopping a pump in the feed line, opening a valve in an emergency dump line, opening a valve to inject a killing agent to stop the reaction.

Identification and documentation

The operator should identify all SIFs preventing major accidents. Each SIF should have a unique identification code. The functionality of each SIF should be clearly described, establishing a clear link between the SIF and the SIF-scenario it is designed for. Design considerations that are discussed below, such as effectiveness, fault tolerance, response to failure and risks introduced by the SIF should be properly documented.

The technical details of the implementation of the SIF should also be properly documented, including an identification of all of its components and a description of its functional logic (trip point, voting logic for sensors and final elements, etc.).

Independence

Each SIF should use components (sensors, logic solvers and final elements) whose failure will not initiate the SIF-scenario. In most cases this means that a SIF should have components that are used for safety purposes only (and not for process control). Sharing components between process control systems and SIFs can lead to a situation where the control and safety functions are lost simultaneously by a single fault in a common component.

If for a given scenario several independent SIFs are required to reduce the likelihood of its occurrence, then these SIFs should not share sensors or final elements.

Effectiveness

Operators should be able to demonstrate that each SIF is effective. Sensors should be installed on a location where they give significant and conservative readings of the process parameter to be monitored. Trip points should be selected sufficiently below the maximum allowable values in order to take into account the response time of the SIF and the process. The action by the SIF should have sufficient 'impact' on the process to effectively interrupt the SIF-scenario.

Joint Research Centre

Fault tolerance

An operator should be able to justify the fault tolerance (0, 1, 2, ...) for the sensors, the logic solver and the final elements. A fault tolerance of 1 for the sensors means that 2 sensors are used to trigger the SIF, so that if one sensor fails, the other sensor can still trigger the SIF. Similarly, a fault tolerance of 1 for the final elements means that 2 redundant final elements are installed. The need for fault tolerance depends on the likelihood and the consequence of the SIF-scenario and the existence of other safety measures (e.g. safety valves) that can interrupt the SIF-scenario. Operators can refer to the standard IEC61511 (Functional safety - Safety instrumented systems for the process industry sector) that establishes a relationship between fault tolerance and the safety integrity level 1[1] (SIL) of a SIF. Alternatively operators can elaborate type-architectures for SIFs and link them to an evaluation of the SIF-scenario.

Response to failure

For each SIF the operator should determine and document the response of the SIF to an out of range signal (coming from the sensors, indicating a sensor malfunction). Implementation of on-line diagnostics by comparing readings from different sensors should be considered. Response to deviation alarms should be documented. The required fail state of the final elements (e.g. for a valve: open, closed, last position) should be determined, justified and documented.

Risks introduced by the SIF

When a SIF is activated, it performs automatically one or more actions (e.g. closing or opening valves, starting or stopping motors, etc.). These actions are intended to stop the SIF-scenario, but sometimes can create a (new) hazardous situation. For example, closing a valve can cause fluid hammer or a deadheading pump. The risks of the action(s) by a SIF should have been identified and additional measures should be taken to manage these risks.

Commissioning

Before taking into service a newly installed SIF, the complete functionality of the SIF should be tested. This test should confirm the correct functioning of all the components and the correct implementation of the complete functional logic. After modifications, repair or maintenance, those parts of the SIF that have been affected, should be tested. All test results should be properly documented to demonstrate the scope and the quality of testing.

[1] The IEC61511 defines 4 discrete safety integrity levels. Each level corresponds to a range in failure rate. The higher the SIL, the lower the failure rate.

Periodic testing

Each SIF should be tested regularly. The test should cover the complete 'chain' of components: from the sensor(s) to the logic solver and from the logic solver to the final element(s). The test of a SIF should be described in an instruction. The test results should be properly documented and have sufficient detail to demonstrate quality and completeness of the test. Operators should be able to justify the test interval. This can be done by performing reliability calculations or by referring to proven practices.

Deactivation

Operators should restrict and control access to the logic solver used by the SIF in order to avoid uncontrolled modifications in settings or temporary deactivation (bypassing). Temporary deactivation should require formal permission by line management. Alternative measures should be considered, documented and implemented before deactivation of the SIF. The personnel operating a process installation should have at any time an overview of all deactivated SIFs. Operators should have a system in place to guarantee the open position of any valves isolating sensors from the process.

Management of change

Permanent and temporary changes to a SIF should fall within the scope of a management of change procedure. The operator should asses whether the modifications have an impact on the reliability of the SIF, its effectiveness and on the risks introduced by the SIF. After modification, all documents describing the SIF and the test instructions should be reviewed and updated.

Contact

This bulletin is a product of the EU Technical Working Group on Seveso Inspections. For more information related to this bulletin or other products and activities of the Technical Working Group, please contact:

Maureen.Wood@jrc.ec.europa.eu
Security Technology Assessment Unit
Major Accident Hazards Bureau
European Commission
Joint Research Centre
Institute for the Protection and Security of the Citizen
Via E. Fermi, 2749
21027 Ispra (VA) Italy

http://mahb.jrc.ec.europa.eu

Joint Research Centre