Nummer 1
Mai 2013

MAHB

Major Accident Hazards Bureau
Security Technology Assessment Unit

SEVESO GEMEINSAME **INSPEKTIONS** SCHRIFTENREIHE KRITERIEN

Safety Instrumented Functions (SIF)

Diese Veröffentlichung der Europäischen Gemeinschaft zu gemeinsamen Inspektionskriterien soll den Austausch von Wissen über technische Maßnahmen und Durchsetzungspraktiken im Zusammenhang mit der Beherrschung von Störfallgefahren und der Umsetzung der Seveso-II-Richtline erleichtern. Die Kriterien wurden von Seveso-Inspektoren entwickelt, um die Verbreitung bewährter Durchsetzungs- und Risikomanagementverfahren für die Beherrschung schwerer Industrieunfälle in Europa und in anderen Teilen der Welt zu unterstützen.

In dieser Ausgabe werden eine Reihe von Aspekten angesprochen, die für eine erfolgreiche Risikominderung unter Verwendung von sicherheitstechnischen Funktionen (Safety Instrumented Functions - SIF) von entscheidender Bedeutung sind. Es wird darauf hingewiesen, dass das Dokument weder als technische Norm noch als Kurzfassung oder Ersatz für vorhandene Normen in diesem Bereich gedacht ist.

Definition

Eine „*Safety Instrumented Function*“ (SIF) ist eine Sicherheitsmaßnahme, die einen potenziell gefährlichen Zustand erkennt und automatisch eine Aktion durchführt, um den Prozess wieder in einen sicheren Zustand zu versetzen. Eine SIF wird als funktionelle Kombination eines oder mehrerer Sensoren, eines Logiksystems (*Logic Solver*) und eines oder mehrerer Aktoren implementiert. Eine SIF unterbricht in der Regel eine Ereigniskette, die mit einer Prozessstörung beginnt und zu einer potenziellen Gefährdungssituation führt. Bezogen auf eine bestimmte SIF wird diese Ereigniskette als SIF-Szenario bezeichnet (wobei es sein kann, dass die betreffende SIF nicht die einzige in diesem Szenario vorkommende Sicherheitsmaßnahme ist). Ein typisches Beispiel einer SIF ist ein Überfüllsicherungssystem bestehend aus einem oder mehreren Füllstandsdetektoren, einer speicherprogrammierbaren Steuerung (SPS) und einem oder mehreren Ventilen in der Zuleitung, die sich schließen, wenn das Flüssigkeitsniveau den Auslösepunkt erreicht. Ein weiteres Beispiel könnte ein Überdruck-Schutzsystem in einem Reaktor sein, das eine Aktion zum Abbruch der Reaktion einleitet, wenn die Temperatur im Reaktor den Auslösepunkt erreicht. Diese Aktion kann Folgendes umfassen: das Schließen eines Ventils oder das Abschalten einer Pumpe im Zulauf, das Öffnen eines Ventils in einer Notabblaseleitung oder das Öffnen eines Ventils zur Einspeisung eines Hemmers, um die Reaktion zu stoppen.

Identifikation und Dokumentation

Der Betreiber sollte alle störfallverhindernden SIFs identifizieren. Jede SIF sollte eine eindeutige Kennung tragen. Die Funktionalität jeder SIF sollte klar definiert werden, wobei insbesondere ein eindeutiger Bezug zwischen der SIF und dem SIF-Szenario, für das sie ausgelegt ist, hergestellt werden sollte. Nachstehend angesprochene konstruktive Merkmale wie Wirksamkeit, Fehlertoleranz, Reaktion auf von der SIF eingebrachte Fehler und Risiken sollten ordnungsgemäß dokumentiert werden.

Die technischen Einzelheiten der SIF-Implementierung sollten ebenfalls ordnungsgemäß dokumentiert werden, wozu auch Angaben über alle ihre Bestandteile und eine Beschreibung ihrer Funktionslogik (Auslösepunkt, Auswahllogik für Sensoren und Aktoren usw.) gehören.

Unabhängigkeit

Für jede SIF sollten Komponenten (Sensoren, Logiksysteme und Aktoren) verwendet werden, deren Versagen das SIF-Szenario nicht auslöst. In den meisten Fällen bedeutet dies, dass eine SIF aus Komponenten bestehen sollte, die nur für Sicherheitszwecke verwendet werden (und nicht zur Prozessleitung). Die gemeinsame Nutzung von Komponenten durch Prozessleitsysteme und SIFs kann dazu führen, dass die Leit- und Sicherheitsfunktionen durch einen einzigen Fehler in einer gemeinsamen Komponente gleichzeitig fortfallen.

Wenn zur Verringerung der Wahrscheinlichkeit des Auftretens eines bestimmten Szenarios mehrere unabhängige SIFs erforderlich sind, sollten dafür keine gemeinsam genutzten Sensoren oder Aktoren eingesetzt werden.

Wirksamkeit

Betreiber sollten die Wirksamkeit jeder SIF nachweisen können. Sensoren sollten an einem Standort installiert werden, an dem sie aussagekräftige und konservative Messwerte des zu überwachenden Prozessparameters liefern. Die Auslösepunkte sollten weit genug unter den zulässigen Höchstwerten ausgewählt werden, damit der Reaktionszeit der SIF und des Prozesses Rechnung getragen wird. Die Aktion der SIF sollte genügend ‚Wirkung‘ auf den Prozess ausüben, dass eine effektive Unterbrechung des SIF-Szenarios gewährleistet ist.

Joint Research Centre

Fehlertoleranz

Ein Betreiber sollte die Fehlertoleranz (0, 1, 2 ...) für die Sensoren, das Logiksystem und die Aktoren begründen können Eine Fehlertoleranz von 1 für die Sensoren bedeutet, dass 2 Sensoren zur Auslösung der SIF eingesetzt werden, damit beim Ausfall des eines Sensors immer noch der andere die SIF auslösen kann. Ähnlich bedeutet eine Fehlertoleranz von 1 bei den Aktoren, dass 2 redundante Aktoren installiert sind. Die Fehlertoleranzanforderungen richten sich nach der Wahrscheinlichkeit und den Folgen des SIF-Szenarios und dem Vorhandensein anderer Sicherheitsmaßnahmen (z. B. Sicherheitsventile), die das SIF-Szenario unterbrechen können. Betreiber können sich auf die Norm IEC61511 (Funktionale Sicherheit - Sicherheitstechnische Systeme für die Prozessindustrie) berufen, die eine Beziehung zwischen der Fehlertoleranz und dem Sicherheitsintegritätslevel (SIL) 1[1] einer SIF herstellt. Alternativ können Betreiber spezifische Architekturen für SIFs erarbeiten und sie mit einer Bewertung des SIF-Szenarios verbinden.

Ausfallreaktion

Für jede SIF sollte der Betreiber die Reaktion dieser SIF auf ein „out of range" Signal (das von den Sensoren kommt und ein Sensorversagen anzeigt) bestimmen und dokumentieren. Die Durchführung einer Online-Diagnose durch Vergleichen der Anzeigen verschiedener Sensoren sollte in Betracht gezogen werden. Die Reaktion auf Abweichungsalarme sollte dokumentiert werden. Der erforderliche Ausfallzustand der Aktoren (z. B. bei einem Ventil: offen, geschlossen, letzte Position) sollte bestimmt, begründet und dokumentiert werden.

Von der SIF hervorgerufene Risiken

Wird eine SIF aktiviert, führt sie automatisch eine oder mehrere Aktionen durch (z. B. Schließen oder Öffnen von Ventilen, An- oder Abschalten von Motoren usw.). Diese Aktionen sollen an sich das SIF-Szenario stoppen, doch sie können in manchen Fällen eine (neue) Gefahrenlage schaffen. Beispielsweise kann das Schließen eines Ventils zu Druckschlägen oder Nullförderung (Pumpe) führen. Die Risiken der Aktion(en) einer SIF sollten bestimmt worden sein, und es sollten zusätzliche Maßnahmen zur Beherrschung dieser Risiken ergriffen werden.

Inbetriebnahme

Vor der Inbetriebnahme einer neu installierten SIF sollte ihre gesamte Funktionalität überprüft werden. Diese Überprüfung sollte das ordnungsgemäße Funktionieren aller Komponenten und die ordnungsgemäße Implementierung der gesamten Funktionslogik bestätigen. Nach Änderungs-, Reparatur- oder Wartungsmaßnahmen sollten die davon betroffenen Teile der SIF überprüft werden. Zum Nachweis des Umfangs und der Qualität der Überprüfung sollten alle Prüfergebnisse ordnungsgemäß dokumentiert werden.

[1] IEC61511 gibt 4 getrennte Sicherheitsintegritätslevel vor. Jeder Level entspricht einem Ausfallratenbereich. Je höher der SIL, desto niedriger die Ausfallrate.

Regelmäßige Überprüfung

Jede SIF sollte regelmäßig überprüft werden. Die gesamte ‚Kette' der Komponenten - von Sensor(en) zu Logiksystem und von Logiksystem zu Aktor(en) - sollte darin einbezogen werden. Die Überprüfung einer SIF sollte in einer Anweisung beschrieben werden. Die Prüfergebnisse sollten ordnungsgemäß dokumentiert werden und so detailliert sein, dass sie als Beleg für die Qualität und die Vollständigkeit der Überprüfung dienen. Die Betreiber sollten das Prüfintervall begründen können. Dies kann durch Zuverlässigkeitsberechnungen oder durch Verweis auf bewährte Praktiken geschehen.

Deaktivierung

Zur Vermeidung unkontrollierter Änderungen der Einstellungen oder einer vorübergehenden Deaktivierung (Überbrückung) sollten Betreiber den Zugang zu dem von der SIF verwendeten Logiksystem einschränken und kontrollieren. Für eine vorübergehende Deaktivierung sollte eine förmliche Genehmigung durch das Linienmanagement erforderlich sein. Alternativmaßnahmen sollten vor der Deaktivierung der SIF sondiert, dokumentiert und umgesetzt werden. Das Betriebspersonal einer Prozessanlage sollte sich jederzeit einen Überblick über alle deaktivierten SIFs verschaffen können. Betreiber sollten über ein System verfügen, das sicherstellt, dass alle Ventile, die die Sensoren vom Prozess trennen, in Offenposition stehen.

Änderungsmanagement

Dauerhafte oder vorübergehende Änderungen einer SIF sollten Gegenstand eines Änderungsmanagementverfahrens sein. Der Betreiber sollte prüfen, ob die Änderungen Auswirkungen auf die Zuverlässigkeit der SIF, ihre Wirksamkeit und auf die von der SIF eingebrachten Risiken haben. Nach erfolgter Änderung sollten alle Dokumente, in denen die SIF und die Prüfanweisungen beschrieben sind, überarbeitet und aktualisiert werden.

Kontakt

Dieses Bulletin wurde von der EU Technical Working Group on Seveso Inspections erarbeitet. Weitere Informationen zu diesem Merkblatt oder zu anderen Produkten und Aktivitäten der Technical Working Group sind erhältlich unter:

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

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

Joint Research Centre