Европейска комисия

Номер 1
Май 2013 г.
MAHB
Служба за опасности от големи аварии
Отдел "Оценка на технологиите за сигурност"

СЕВЕЗО ОБЩИ ИНСПЕКЦИЯ КРИТЕРИ И СЕРИЯ

Функции на измервателна система за безопасност

Тази публикация на Европейската общност относно общите критерии за инспекция има за цел да сподели знания относно техническите мерки и практиките за прилагане, свързани с контрола на големи опасности и прилагането на Директивата "Севезо II". Критериите са разработени от инспекторите на Севезо, за да подпомогнат разпространението на добри практики за прилагане и управление на риска за контрол на големи промишлени опасности в Европа и другаде.

Този конкретен брой подчертава редица проблеми, които са от решаващо значение за успешното намаляване на рисковете чрез използване на функции на измервателна система за безопасност. Имайте предвид, че този документ не е предназначен за технически стандарт, нито като обобщение или замяна на съществуващи стандарти по въпроса.

Определение

Функцията на измервателна система за безопасност (SIF) е мярка за безопасност, която усеща потенциално опасно състояние и автоматично извършва действие за връщане на процеса в безопасно състояние. SIF се реализира като функционална комбинация от един или повече сензори, логически решаващ модул и един или повече крайни елементи. SIF обикновено ще прекъсне верига от събития, започваща с нарушение на процеса и водеща до потенциално опасна ситуация. За дадена SIF тази верига от събития се нарича SIF-сценарий (въпреки че въпросната SIF може да не е единствената мярка за безопасност, включена в този сценарий). Типичен пример за SIF е защита от високо ниво, включваща един или повече детектори за ниво, програмируем логически контролер (PLC) и един или повече клапани в захранващата линия, които ще бъдат затворени, когато нивото на течността достигне точката на задействане. Друг пример може да бъде защита от високо налягане на реактор, която инициира действие за спиране на реакцията, когато температурата в реактора достигне точката на задействане. Това действие може да бъде: затваряне на клапан или спиране на помпа в захранващия тръбопровод, отваряне на клапан в тръбопровода за аварийно изхвърляне, отваряне на клапан за инжектиране на убиващ агент за спиране на реакцията.

Идентификация и документиране

Операторът трябва да идентифицира всички SIF, предотвратяващи големи аварии. Всяка SIF трябва да има уникален идентификационен код. Функционалността на всяка SIF трябва да бъде ясно описана, като се установи ясна връзка между SIF и SIF сценария, за който е проектирана. Съображенията за проектиране, които са обсъдени по-долу, като ефективност, устойчивост на грешки, реакция при отказ и рискове, въведени от SIF, трябва да бъдат надлежно документирани.

Техническите подробности за изпълнението на SIF също трябва да бъдат надлежно документирани, включително идентификация на всички нейни компоненти и описание на функционалната ѝ логика (точка на задействане, логика на гласуване за сензори и крайни елементи и т.н.).

Независимост

Всяка SIF трябва да използва компоненти (сензори, логически решаващи устройства и крайни елементи), чиято повреда няма да инициира SIF сценария. В повечето случаи това означава, че SIF трябва да има компоненти, които се използват само за целите на безопасността (а не за контрол на процеса). Споделянето на компоненти между системите за контрол на процеси и SIF може да доведе до ситуация, при която функциите за управление и безопасност се губят едновременно от една повреда в общ компонент.

Ако за даден сценарий са необходими няколко независими SIF, за да се намали вероятността от възникването му, тогава тези SIF не трябва да споделят сензори или крайни елементи.

Ефикасност

Операторите трябва да могат да демонстрират, че всяка SIF е ефективна. Сензорите трябва да бъдат инсталирани на място, където дават значителни и консервативни показания

JRC85209

Съвместен изследователски център

на параметъра на процеса, който трябва да се наблюдава. Точките на прекъсване трябва да бъдат избрани достатъчно под максимално допустимите стойности, за да се вземе предвид времето за реакция на SIF и процеса. Действието на SIF трябва да има достатъчно „въздействие“ върху процеса за ефективно прекъсване на SIF сценария.

Толерантност към грешки

Операторът трябва да може да обоснове толерантността към грешки (0, 1, 2, ...) за сензорите, логическото решаване и крайните елементи. Толерантност на грешки 1 за сензорите означава, че 2 сензора се използват за задействане на SIF, така че ако единият сензор се повреди, другият сензор все още може да задейства SIF. По същия начин толерантност на грешки 1 за крайните елементи означава, че са инсталирани 2 излишни крайни елемента. Необходимостта от толерантност към грешки зависи от вероятността и последствията от SIF-сценария и съществуването на други мерки за безопасност (напр. предпазни клапани), които могат да прекъснат SIF-сценария. Операторите могат да се позовават на стандарта IEC61511 (Функционална безопасност - Системи с инструменти за безопасност за сектора на преработващата промишленост), който установява връзка между толерантността към грешки и нивото на пълнота на безопасността 1[I] (SIL) на SIF. Като алтернатива операторите могат да разработят типови архитектури за SIF и да ги свържат с оценка на SIF сценария.

Отговор на неуспех

За всеки SIF операторът трябва да определи и документира отговора на SIF на сигнал извън обхвата (идващ от сензорите, показващ неизправност на сензора). Трябва да се обмисли прилагането на онлайн диагностика чрез сравняване на показанията от различни сензори. Отговорът на алармите за отклонение трябва да бъде документиран. Необходимото състояние на отказ на крайните елементи (напр. за клапан: отворен, затворен, последно положение) трябва да бъде определено, обосновано и документирано.

Рискове, въведени от SIF

Когато SIF е активиран, той извършва автоматично едно или повече действия (напр. затваряне или отваряне на клапани, стартиране или спиране на двигатели и др.). Тези действия имат за цел да спрат SIF сценария, но понякога могат да създадат (нова) опасна ситуация. Например, затварянето на клапан може да причини флуиден чук или блокираща помпа. Рисковете от действието(ята) на SIF трябва да са идентифицирани и трябва да се предприемат допълнителни мерки за управление на тези рискове.

Въвеждане в експлоатация

Преди да се пусне в експлоатация новоинсталирана SIF, трябва да се тества пълната функционалност на SIF. Този тест трябва да потвърди правилното функциониране на всички компоненти и правилното изпълнение на пълната функционална логика. След модификации, ремонт или поддръжка, онези части от SIF, които са били засегнати, трябва да бъдат тествани. Всички резултати от тестове трябва да бъдат надлежно документирани, за да демонстрират обхвата и качеството на тестването.

Периодично тестване

Всяка SIF трябва да се тества редовно. Тестът трябва да обхваща пълната „верига“ от компоненти: от сензора(ите) до логическия решаващ модул и от логическия решаващ елемент до крайния(те) елемент(и). Тестът на SIF трябва да бъде описан в инструкция. Резултатите от теста трябва да бъдат надлежно документирани и да имат достатъчно подробности, за да демонстрират качество и пълнота на теста. Операторите трябва да могат да обосноват тестовия интервал. Това може да стане чрез извършване на изчисления за надеждност или чрез позоваване на доказани практики.

Деактивиране

Операторите трябва да ограничават и контролират достъпа до логическия софтуер, използван от SIF, за да избегнат неконтролирани промени в настройките или временно деактивиране (байпас). Временното деактивиране трябва да изисква официално разрешение от висшето ръководство. Трябва да се обмислят, документират и приложат алтернативни мерки преди деактивирането на SIF. Персоналът, обслужващ процесната инсталация, трябва да има по всяко време преглед на всички деактивирани SIF. Операторите трябва да разполагат със система, която да гарантира отвореното положение на всички клапани, изолиращи сензорите от процеса.

Управление на промяната

Постоянните и временните промени в SIF следва да попадат в обхвата на процедурата за управление на промените. Операторът трябва да оцени дали модификациите оказват влияние върху надеждността на SIF, нейната ефективност и върху рисковете, въведени от SIF. След промяна всички документи, описващи SIF и инструкциите за теста, трябва да бъдат прегледани и актуализирани.

Данни за контакт:

Този бюлетин е продукт на Техническата работна група на ЕС за инспекциите по Севезо. За повече информация, свързана с този бюлетин или други продукти и дейности на Техническата работна група, моля, свържете се с:

Maureen.Wood@jrc.ec.europa.eu
Отдел за оценка на технологиите за сигурност
Служба за опасности от големи аварии

[I] IEC61511 определя 4 отделни нива на интегритет на безопасност. Всяко ниво съответства на диапазон от честота на неуспех. Колкото по-висок е SIL, толкова по-нисък е процентът на отказ.