Scientific Papers of the
Institute of Electrical Power Engineering of the
Wrocław University of Technology

PRESENT PROBLEMS OF POWER SYSTEM CONTROL

No 1

Wrocław 2011

Słowa kluczowe: elektroenergetyczna automatyka zabezpieczeniowa, systemy zabezpieczeń w elektrowniach, bezpieczeństwo funkcjonalne systemów programowalnych, zastosowanie normy PN/EN/IEC 61508 i norm pochodnych

Zdzisław ŻURAKOWSKI*

BEZPIECZEŃSTWO FUNKCJONALNE UKŁADÓW ELEKTROENERGETYCZNEJ AUTOMATYKI ZABEZPIECZENIOWEJ OPARTYCH NA URZĄDZENIACH PROGRAMOWALNYCH

W związku z rosnącą liczbą urządzeń programowalnych stosowanych w układach elektroenergetycznej automatyki zabezpieczeniowej (EAZ), rosnącą złożonością systemów technicznych stosowanych w przemyśle, w tym systemów związanych z bezpieczeństwem, oraz rosnącymi wymaganiami odnośnie bezpieczeństwa, do oceny którego włączana jest również ocena niezawodności zasilania, po opublikowaniu międzynarodowej normy IEC 61508, dotyczącej bezpieczeństwa funkcjonalnego systemów programowalnych, w krajach rozwiniętych podjęte zostały prace zmierzające do zastosowania tej normy również w sektorze elektroenergetyki, w tym do układów EAZ. W referacie po krótkim rysie historycznym oraz przedstawieniu podstawowych koncepcji na których oparta jest norma IEC 61508, przedstawiono na podstawie dostępnych publikacji aktualny stan prac zmierzających do wdrożenia tej normy do układów EAZ. W zakończeniu podane są także niektóre prace związane z zastosowaniem tej normy do układów zabezpieczeń w elektrowniach konwencjonalnych.

1. WSTĘP

W literaturze wyróżnia się kilka aspektów bezpieczeństwa systemów komputerowych. Pierwsze z nich, zwane podstawowym (ang. *primary safety*), to bezpieczeństwo samego systemu komputerowego, które obejmuje możliwość porażenia prądem, spalenia się komputera lub wywołania pożaru przez sprzęt komputerowy, itp. Drugi aspekt, to bezpieczeństwo funkcjonalne (ang. *functional safety*), a trzeci wyróżniany w

* Niezależny konsultant; e-mail: zz@pvd.pl

literaturze, to bezpieczeństwo pośrednie (ang. *indirect safety*) z jakim mamy do czynienia np. w związanych z bezpieczeństwem systemach informatycznych (ang. *safety-related information systems*), odnoszące się do pośrednich konsekwencji uszkodzenia komputera lub wytworzenia błędnej informacji. Odnosi się to do szerokiego zakresu systemów, takich jak medyczne systemy zobrazowania lub systemy rejestru danych pacjenta [16].

Bezpieczeństwo funkcjonalne systemu komputerowego, lub ogólnie biorąc systemu programowalnego, polega na wykryciu potencjalnie niebezpiecznych warunków, w wyniku którego następuje uruchomienie urządzeń lub mechanizmów korygujących lub zabezpieczających, mających na celu zapobieżenie zdarzeniu zagrażającemu lub zmniejszenia skutków tego zdarzenia. Przykładem bezpieczeństwa funkcjonalnego może być włączenie systemu gaszenia po wykryciu dymu przez czujniki.

Terminem system związany z bezpieczeństwem (ang. *safety-related system*), określany jest system, który zapewnia bezpieczeństwo danego urządzenia lub obiektu przez implementację w nim funkcji bezpieczeństwa, tzn. funkcji koniecznych do osiągnięcia lub utrzymania stanu bezpiecznego. W przypadku systemów sterowania, system związany z bezpieczeństwem może być częścią systemu sterowania danym obiektem lub być oddzielnym systemem, sprzężonym z danym obiektem przez czujniki i elementy wykonawcze.

Termin system krytyczny dla bezpieczeństwa (ang. *safety-critical system*) jest zwykle używany jako synonim terminu system związany z bezpieczeństwem, chociaż w niektórych przypadkach może sugerować, że chodzi o system o wysokim stopniu krytyczności dla bezpieczeństwa.

W elektroenergetyce, w przypadku elektrowni, funkcje systemów programowalnych związane z bezpieczeństwem obejmują zarówno funkcje związane z regulacją procesów technologicznych jak i z uzupełniającymi ją zabezpieczeniami technologicznymi, stanowiącymi dodatkowe zabezpieczenie pracy zarówno danego urządzenia jak i całego procesu technologicznego. Przykładem mogą być zabezpieczenia kotłów.

Zgodnie z podanymi wyżej definicjami w EAZ przykładami systemów związanych z bezpieczeństwem funkcjonalnym mogą być wszystkie układy zabezpieczeń, których celem jest wykrycie uszkodzenia, na przykład zwarcia, a następnie wyłączenie zabezpieczanego obiektu w celu ochrony go przed zniszczeniem i ewentualnie także innymi stratami, jakie mogłyby powstać w przypadku niewyłączenia uszkodzenia. Takie podejście, od dawna stosowane na przykład w przemyśle procesowym, w EAZ dotychczas nie było stosowane. W związku z rosnącą liczbą urządzeń programowalnych stosowanych w układach EAZ, rosnącą złożonością systemów technicznych stosowanych w przemyśle, w tym systemów związanych z bezpieczeństwem, oraz rosnącymi wymaganiami odnośnie bezpieczeństwa, do oceny którego włączana jest również ocena niezawodności zasilania, po opublikowaniu międzynarodowej normy IEC 61508, dotyczącej bezpieczeństwa funkcjonalnego systemów programowalnych, w krajach rozwiniętych podjęte zostały prace zmierzające do zastosowania tej normy również w

sektorze elektroenergetyki, w tym do układów EAZ. W dalszej części, po krótkim rysie historycznym oraz przedstawieniu podstawowych koncepcji na których oparta jest norma IEC 61508, przedstawiony zostanie na podstawie dostępnych publikacji aktualny stan prac zmierzających do wdrożenia tej normy do układów EAZ. W zakończeniu podane zostaną także niektóre prace związane z zastosowaniem tej normy do układów zabezpieczeń w elektrowniach konwencjonalnych.

2. RYS HISTORYCZNY

Z informacji zawartych w publikacjach można wywnioskować, że kształtowanie się świadomości w przemyśle, świadomości społecznej, uregulowań prawnych i koncepcji na których oparta jest międzynarodowa norma IEC 61508 zaczęło się w latach 1970.

We wstępie do poradnika stosowania normy IEC 61508 autorzy piszą, że na początku lat 1970. w przemyśle procesowym zaczęto uświadamiać sobie, że w przypadku większych zakładów, posiadających duże ilości materiałów niebezpiecznych praktyka uczenia się na błędach (jeśli rzeczywiście ma miejsce) nie jest dłużej do zaakceptowania. Z własnej inicjatywy opracowano metody identyfikacji zagrożeń i ilościowego określania konsekwencji awarii w przeważającym stopniu jako pomoc w procesie podejmowania decyzji, związanych z rozbudową lub zmianami wprowadzanymi do zakładów. Zewnętrzne naciski przyszły później [15].

W sobotę 1 czerwca 1974 roku zakłady chemiczne we Flixborough w Wielkiej Brytanii zostały całkowicie zniszczone w wyniku eksplozji. 28 osób pracujących w tym czasie w zakładach zostało zabitych, a 36 innych odniosło rany. Na zewnętrz zakładów miały miejsce rozległe szkody i zniszczenia. Odnotowano 53 rannych, setki innych, którzy odnieśli relatywnie mniejsze zranienia nie zostało odnotowanych. 1821 domów i 167 sklepów i fabryk doznało większych lub mniejszych zniszczeń. Katastrofa we Flixborough 1974 roku skoncentrowała w Wielkiej Brytanii uwagę społeczeństwa i mediów na tych dziedzinach przemysłu, które mogły stwarzać takie zagrożenie. Istnieje w publikacjach zgodna opinia, że ta katastrofa oraz powtarzająca się po niej cała seria następujących prawie rok po roku kolejnych katastrof [7], miały w jakimś stopniu przełomowe znaczenie dla postrzegania tego typu zagrożeń jakie stwarza przemysł.

W następstwie katastrofy we Flixborough podjęto szereg działań, które w roku 1984 doprowadziły do regulacji CIMACH (Control of Industrial Major Accident Hazards), a w roku 1990 do jej poprawionej wersji w postaci COMACH (Control of Major Accident Hazards).

Ocena zagrożeń w przemyśle procesowym i w innych sektorach stała się powszechna w latach 80-tych dwudziestego wieku, ale formalne wytyczne i normy były

rzadkie i fragmentaryczne i nie dotyczyły całości zagadnień. Prowadzono wówczas prace nad opracowaniem norm w dziedzinie tworzenia oprogramowania dla systemów związanych z bezpieczeństwem i opublikowano pierwsze normy krajowe w tej dziedzinie, miedzy innymi przez TUV w Niemczech i Health and Safety Executive w Wielkiej Brytanii. W wyniku tych prac oraz presji przemysłu na opracowanie wspólnej normy międzynarodowej w tej dziedzinie, w roku 1995 opublikowany został projekt normy IEC 1508, a w latach 1998 – 2000 projekt ten opublikowany został jako międzynarodowa norma IEC 61508 [11].

Norma ta bardzo szybko znalazła powszechne uznanie jako podstawowa norma międzynarodowa w dziedzinie bezpieczeństwa funkcjonalnego systemów programowalnych, umożliwiająca coraz powszechniejsze stosowanie tych systemów w zastosowaniach związanych z bezpieczeństwem. Przed powstaniem tej normy używanie systemów programowalnych do zastosowań związanych z bezpieczeństwem natrafiało na opory, wynikające z braku zaufania do tych systemów, spowodowanego trudnościami ich oceny. W oparciu o tę normę publikowana jest coraz większa liczba norm dotyczących bezpieczeństwa funkcjonalnego w takich zastosowaniach, jak przemysł chemiczny, aparatura medyczna czy transport [1]. Opublikowana została również jako norma europejska EN i polska PN [11].

Z literatury wynika, że jej szybkie i powszechne wdrażanie wiąże się także z coraz bardziej rygorystycznymi wymaganiami rynkowymi dla systemów związanych z bezpieczeństwem. Obejmują one wykazanie z wykorzystaniem międzynarodowych norm, że wymagane bezpieczeństwo funkcjonalne zostało osiągnięte oraz spełnione zostały istniejące uregulowania prawne.

3. PODSTAWOWE KONCEPCJE NA KTÓRYCH OPARTA JEST NORMA IEC 61508

Maszyny, instalacje procesowe i inne urządzenia mogą w przypadku wadliwego działania stwarzać ryzyko dla ludzi i środowiska, związane z takimi zdarzeniami, jak pożary, eksplozje, nadmierne dawki promieniowania, niespodziewane powtórzenie suwu maszyny, itp. Wymienione wadliwe działania mogą powstać z powodu:

- defektów fizycznych w urządzeniu, spowodowanych na przykład przypadkowymi uszkodzeniami sprzętu;
- defektów w oprogramowaniu spowodowanych błędami ludzkimi popełnionymi w specyfikacji i projekcie systemu, które w przypadku określonych kombinacji sygnałów wejściowych mogą ujawnić się w postaci błędu w działaniu;
- warunków środowiskowych, takich jak zakłócenia elektromagnetyczne, temperatura, zjawiska mechaniczne;

- zakłóceń w napięciu zasilającym (zanik lub obniżenie napięcia, powrót napięcia po zaniku), itp.

Omawiana norma została opracowana w celu zapewnienia możliwości bezpiecznego zautomatyzowania instalacji przemysłowych i urządzeń z użyciem systemów programowalnych, które mają wiele korzystnych cech. Norma zawiera szczegółowe wytyczne umożliwiające realizację i ocenę systemu związanego z bezpieczeństwem, który ma zredukować ryzyko uszkodzeń do minimalnego akceptowalnego poziomu, zgodnie z zasadą ALARP, wymagającą żeby każde ryzyko zostało zmniejszone w takim stopniu, w jakim to jest racjonalnie uzasadnione (ang. *As Low As Reasonably Practicable*) [2].

Zgodnie z definicją podaną we wstępie, w normie IEC 61508 termin urządzenia programowalne jest ogólnym określeniem wszystkich urządzeń elektronicznych opartych na oprogramowaniu, takich jak układy komputerowe, sterowniki programowalne, mikrosterowniki, programowalne układy logiczne (PLC). Przez systemy związane z bezpieczeństwem funkcjonalnym podstawowo przyjęto w tej normie układy, których błąd w działaniu spowodować może zranienie lub śmierć osób, ale rozszerza się je również na układy, które w przypadku błędu w działaniu mogą spowodować duże szkody dla środowiska lub duże straty materialne.

Norma IEC 61508 oparta jest na analizie zagrożeń i ryzyka wykonywanej we wstępnej fazie projektu danego systemu. Analiza obejmuje projektowany system wraz obiektem dla którego ma realizować funkcję związana z bezpieczeństwem oraz całym otoczeniem systemu i obiektu, z którym dany obiekt i projektowany system będą wchodzić w interakcję. Ryzyko określa się zwykle jako iloczyn straty powstałej w przypadku zaistnienia danego zagrożenia i przewidywanej częstotliwości występowania tego zagrożenia.

Głównymi narzędziami, służącymi do zrealizowania celu normy są:

- całkowity cykl życia bezpieczeństwa (ang. *overall safety lifecycle*) systemu związanego z bezpieczeństwem;
- nienaruszalność bezpieczeństwa danej funkcji związanej z bezpieczeństwem określana skrótem SIL, od nazwy w języku angielskim *Safety Integrity Level*, podzielona na cztery kategorie, przy czym SIL 1 oznacza najniższy poziom nienaruszalności, a SIL 4 – najwyższy.

Przyjęty całkowity cykl życia bezpieczeństwa definiuje wymagania dla wszystkich etapów życia danego systemu, od etapu tworzenia koncepcji systemu poprzez analizę zagrożeń i ryzyka, określenie wymagań związanych z zapewnieniem bezpieczeństwa, realizację systemu, walidację bezpieczeństwa, przekazanie do eksploatacji oraz eksploatację, konserwację i naprawy aż do wyłączenia z ruchu lub likwidacji. Cykl ten narzuca podział etapu realizacji systemu na poszczególne fazy, organizuje te fazy w proces oraz włącza w proces wytwarzania czynności oceny jakości realizacji systemu w dogodnych punktach tego procesu. Dokumenty z czynności oceny są podstawą do

oceny jakości całego procesu oraz służą jako dowód w procesie oceny uzyskanego poziomu bezpieczeństwa systemu, dokonywanej w procesie certyfikacji.

Celem analizy zagrożeń i ryzyka jest przeanalizowanie wszystkich możliwych do wystąpienia sytuacji zagrażających, jakie mogłyby wystąpić w przypadku błędu w funkcjonowaniu systemu lub w przypadku innych możliwych do przewidzenia okoliczności związanych z danym obiektem lub z otoczeniem systemu i obiektu. Jeśli z analizy wynika, że sytuacje zagrażające nie mogą wystąpić, lub że prawdopodobieństwo ich wystąpienia lub skutki w przypadku wystąpienia są do zaakceptowania, to system taki uważa się za system nie związany z bezpieczeństwem funkcjonalnym i norma IEC 61508 nie ma w tym przypadku zastosowania.

Jeśli analiza wykaże, że zagrożenia o potencjalnych skutkach nie do zaakceptowania mogą wystąpić, to dalszy projekt systemu powinien być wykonywany jak dla systemów związanych z bezpieczeństwem na podstawie normy IEC 61508 lub norm sektorowych opartych na tej normie. W tym przypadku w trakcie analizy zagrożeń i ryzyka tworzona jest specyfikacja wymagań bezpieczeństwa funkcjonalnego definiująca:

- czynności, jakie poszczególne funkcje związane z bezpieczeństwem, tzw. funkcje bezpieczeństwa, mają wykonać w przypadku wystąpienia zagrożenia.
- wymagany poziom nienaruszalności bezpieczeństwa SIL dla każdej funkcji bezpieczeństwa.

Przypisanie danej funkcji bezpieczeństwa jednego z czterech poziomów bezpieczeństwa, określa wymaganą niezawodność z jaką dana funkcja powinna być realizowana, aby zidentyfikowane ryzyko zostało zmniejszone do poziomu akceptowalnego zgodnie z zasadą ALARP. Wysoki poziom SIL oznacza mniejsze prawdopodobieństwo wystąpienia uszkodzeń (niezadziałania) funkcji bezpieczeństwa, przy czym SIL określa tylko prawdopodobieństwo uszkodzeń niebezpiecznych, wymaganych do realizacji funkcji bezpieczeństwa. Odróżnia to SIL od niezawodności, która dotyczy wszystkich uszkodzeń, bezpiecznych i niebezpiecznych.

Na wymaganą wartość prawdopodobieństwa uszkodzeń niebezpiecznych danej funkcji bezpieczeństwa składają się dwa rodzaje uszkodzeń: uszkodzenia przypadkowe sprzętu (ang. *random hardware failure*) i uszkodzenia systematyczne (ang. *systematic failure*). Dlatego zapewnienie wymaganej docelowej miary uszkodzeń funkcji bezpieczeństwa wymaga dwóch rodzajów podejść w procesie tworzenia systemu, uwzględniających dwa różne rodzaje uszkodzeń.

Uszkodzenia przypadkowe spowodowane są degradacją sprzętu i liczbowa wartość prawdopodobieństwa ich wystąpienia może być ustalona przez porównanie wartości liczbowej prognozowanej częstotliwość uszkodzeń sprzętu z wartością docelowej miary uszkodzeń, odpowiadającą przyjętemu poziomowi SIL. Jeśli częstotliwość ta jest niewystarczająca, to dokonujemy zmian, polegających na przykład na przyjęciu innego sprzętu lub zastosowaniu redundancji.

Uszkodzenia systematyczne spowodowane są błędami w projektowaniu, nie mają charakteru przypadkowego i tym samym nie podlegają analizie statystycznej i nie jest możliwe określenie ilościowe prawdopodobieństwa ich wystąpienia. Przyczynami niebezpiecznych uszkodzeń systematycznych funkcji bezpieczeństwa mogą być:

- nieprawidłowa specyfikacją sprzętu lub oprogramowania;
- przeoczenia lub pominięcia w specyfikacji wymagań bezpieczeństwa (na przykład pominiecie niezbędnych funkcji bezpieczeństwa);
- systematyczne mechanizmy błędów w sprzęcie;
- błędy w oprogramowaniu;
- błędy ludzkie;
- zakłócenia elektromagnetyczne;
- konserwacja lub modyfikacja.

Określenie obu powyższych rodzajów nieprawidłowości w działaniu urządzeń programowalnych jako „uszkodzenia", użyte zostało za polską wersją normy IEC 61508, w której użyte one zostały jako odpowiedniki angielskich terminów *random failure* i *systematic failure*, mimo że nieprawidłowe działanie spowodowane na przykład błędem w oprogramowaniu nie ujawnia się zwykle jako uszkodzenie systemu programowalnego, a jako jego błędne działanie.

Zapewnienie wymaganej częstotliwości występowania uszkodzeń systematycznych odpowiadającej przyjętemu poziomowi SIL, uzyskuje się przez zastosowanie zalecanych w normie metod i środków dla danego SIL, uznanych na podstawie aktualnej wiedzy i doświadczenia za odpowiednie do osiągnięcia danego poziomu częstotliwości występowania uszkodzeń systematycznych. Poziom SIL spełnia w normie rolę parametru, określającego jakie środki i z jakim rygorem należy zastosować w procesie tworzenia systemu, aby uzyskać wymaganą częstotliwości występowania uszkodzeń systematycznych. Jest to główna rola SIL w omawianej normie.

Podawana w części pierwszej normy wymagana liczbowa wartość prawdopodobieństwa uszkodzeń niebezpiecznych funkcji bezpieczeństwa dla danego poziomu SIL odnosi się tylko do uszkodzeń przypadkowych sprzętu. Wymagana niezawodność uszkodzeń systematycznych ustalana jest jakościowo, przez zastosowanie technik i środków narzucanych przez przyjęty poziom SIL.

Przyjęcie poziomu SIL jako parametru do uzyskania wymaganego poziomu występowania uszkodzeń systematycznych jest procedurą uproszczoną, wynikająca z aktualnych możliwości techniki w tym zakresie. Szereg czynników wpływa na nienaruszalność bezpieczeństwa oprogramowania i nie jest możliwe podanie dokładnego algorytmu doboru technik i innych środków. W każdym konkretnym przypadku techniki oprogramowania powinny być rozważnie dobrane z uwzględnieniem takich czynników, jak [5]:

- kompetencje i doświadczenie wykonawcy oprogramowania w stosowaniu technik;

- zaznajomienie wykonawcy oprogramowania z aplikacją i przewidywane trudności;
- rozmiar i złożoność aplikacji;
- rekomendacje i rozwiązania dobrej praktyki istniejące w danym sektorze przemysłu;
- opublikowane krajowe i międzynarodowe normy.

4. ZASTOSOWANIE NORMY IEC 61508 DO UKŁADÓW ELEKTROENERGETYCZNEJ AUTOMATYKI ZABEZPIECZENIOWEJ

Jako przykład pojawiającego się w literaturze podejścia do układów EAZ, jak do systemów związanych z bezpieczeństwem funkcjonalnym zgodnie z normą IEC 61508, może być opis przekaźnika przeznaczonego do zabezpieczeń linii średnich napięć, opracowanego w firmie Schneider Electric [9]. W podsumowaniu referatu autorzy piszą, że jak każdy system związany z bezpieczeństwem, przekaźniki do zabezpieczeń linii średnich napięć muszą spełniać wymagania SIL zdefiniowane w normie IEC 61508. Funkcją bezpieczeństwa części programowej przekaźnika jest wykrycie powstałego uszkodzenia w sieci, a następnie wysłanie do wyłączników sygnału wyłączenia, w celu izolowania dotkniętej uszkodzeniem części sieci. Wykrycie i izolacja uszkodzeń musi nastąpić w czasie podanym w normie IEC 60255. Jako typowe stany towarzyszące uszkodzeniom autorzy wymieniają przeciążenia, zwarcia, uszkodzenia izolacji, itp. Referat opisuje opracowane w Schneider Electric podejście do konstrukcji oprogramowania, umożliwiające zbudowanie przekaźnika o deterministycznej stałej zwłoce czasowej. W przeprowadzonych testach uzyskano formalne potwierdzenie, że czas zwłoki od powstania uszkodzenia do wykrycia go przez algorytmy zabezpieczeniowe przekaźnika ma stałą wartości $t_{\text{detection}}$ = 26,664 ms. Autorzy podają, że zagwarantowanie stałego czasu działania umożliwia poprawienie selektywności zabezpieczeń i wymagane jest także do zagwarantowania przekaźnikowi poziomu nienaruszalności bezpieczeństwa SIL 2.

W publikacjach takie podejście, jak opisywane w referacie [9], spotyka się jednak rzadko. Norma IEC 61508 i normy pochodne, jak norma IEC 61511, przeznaczona dla przemysłu procesowego [12], w pierwszej kolejności wdrażane były do systemów programowalnych związanych z bezpieczeństwem w takich sektorach, jak przemysł procesowy, petrochemiczny, aparatura medyczna, systemy bezpieczeństwa maszyn, gdzie w grę wchodziło bezpieczeństwo pracowników i innych osób oraz gdzie w związku z tym obowiązują wymagania prawne krajowe i Unii Europejskiej. W elektroenergetyce w odniesieniu do EAZ takich wymagań prawnych nie ma i normy te nie były stosowane w tym sektorze i nawet nie były znane, poza elektrowniami jądrowymi, gdzie normy na układy zabezpieczeń oparte na systemach programowalnych sto-

sowane są od dawna, a w ostatnich latach wydana została oparta na IEC 61508 norma IEC 61513 [8].

4.1 ZASTOSOWANIE NORMY IEC 61508 I NORM POCHODNYCH DO EAZ W SYSTEMACH ZASILANIA I SIECIACH WEWENĘTRZNYCH ZAKŁADÓW PRZEMYSLOWYCH

Układy realizujące funkcje związane z bezpieczeństwem składają się z takich elementów jak czujniki, urządzenia programowalne, systemy komunikacyjne, elementy wykonawcze oraz zasilanie. Dla zapewnienia danej funkcji bezpieczeństwa wymaganego poziomu SIL, wszystkie urządzenie i podsystemy, tworzące układ realizujący tę funkcję, muszą posiadać zdolność wypełniania swojej funkcji do poziomu SIL, który w odniesieniu do takich elementów jak czujniki i urządzenia programowalne, podawany jest w danych katalogowych tych elementów. Podobne wymagania odnośnie wymaganego poziomu SIL odnoszą się do zasilania. Zarówno do układów UPS, zasilających urządzenia i podsystemy realizujące daną funkcję bezpieczeństwa, jak i do całego systemu zasilania danego zakładu czy procesu technologicznego w energię elektryczną, od którego zależeć może funkcjonowanie układów i urządzeń, na przykład napędów elektrycznych, dla których układy UPS są niewystarczające. Zapewnienie systemom zasilania odpowiedniego poziomu SIL wymaga aby odpowiedni poziom SIL posiadały również przekaźniki do zabezpieczeń, stosowanych w tych systemach zasilania. Z publikacji wynika, że rozwiązania takie zaczynają być stosowane w takich sektorach, jak petrochemia, przemysł procesowy czy transport miejski, co jak się wydaje spowodowane jest coraz bardziej rygorystycznym egzekwowaniem uregulowań prawnych dotyczących bezpieczeństwa w tych sektorach, które powoduje objęcie wymaganiami tych uregulowań także systemów zasilania zakładów w tych sektorach. Przykładem może być przekaźnik zabezpieczeniowy SEPCOS-PRO firmy Sécheron, posiadający certyfikat SIL 2, przeznaczony do stosowania w stacjach zasilających transportu publicznego, jak metro, linie trolejbusowe i pociągi podmiejskie [14] oraz wytyczne projektowania układów EAZ dla systemów zasilania zakładów petrochemicznych z uwzględnieniem wymaganego poziomu SIL [6].

We wstępie do opublikowanych przez Instytut Energetyki w Londynie wytycznych [6] podano, że powodem opracowania zawartej w tej publikacji metodologii opartej na ryzyku i normach IEC 61508/IEC 61511 jest rosnące zastosowanie mikroprocesorów i urządzeń programowalnych w EAZ oraz wymagana w Wielkiej Brytanii ocena ryzyka w tym sektorze przez uregulowania prawne takie jak Control of Major Hazard Regulations (COMAH), która powinna zawierać ocenę nienaruszalności zasilania i scenariusze wyłączania instalacji.

Publikacja dostarcza wytycznych i danych liczbowych do stosowania opartej na normach IEC 61508/IEC 16511 metodologii oceny wymaganego poziomu nienaruszalności bezpieczeństwa SIL oraz alokacji SIL do urządzeń i układów zabezpieczeń zasilania elektrycznego, łącznie z silnikami i innymi urządzeniami mechanicznymi,

związanymi z daną instalacją. W oparciu o te wytyczne, projektujący układy EAZ powinni sprawdzać przyjmowane schematy, szczególnie różniące się od stosowanych poprzednio, między innymi także w celu upewnienia się czy przyjmowany poziom SIL nie jest wyższy od wymaganego dla danego zastosowania. Wytyczne podają, że w zastosowaniach objętych wytycznymi, wymagany poziom SIL nie jest zwykle wyższy niz SIL1. Podają także, że postępując zgodnie ze stosowanymi poprzednio dobrymi praktykami w projektowaniu urządzeń i układów zabezpieczeń, łącznie z odpowiednim testowaniem, procedurami kontroli i obsługi w celu zapewnienia niskiego poziomu uszkodzeń, w większości przypadków powinno się osiągnąć taki poziom SIL [6], [4].

4.2 ZASTOSOWANIE NORMY IEC 61508 DO UKŁADÓW EAZ W SIECIACH PRZESYŁOWYCH I ROZDZIELCZYCH ELEKTROENERGETYKI

Z dostępnych publikacji wynika, że wdrożenie normy IEC 61508 w sektorze elektroenergetyki jest na etapie początkowym szczególnie, jeśli idzie o układy EAZ w sieciach przesyłowych i rozdzielczych. Z publikacji wywnioskować można, że najbardziej zaawansowana w tym zakresie jest elektroenergetyka brytyjska, co wiązać należy zapewne z dużą rolą, jaką w Wielkiej Brytanii w zapewnieniu bezpieczeństwa w przemyśle odgrywa organizacja Health and Safety Executive (HSE), będąca niezależną rządową organizacją sprawującą w interesie publicznym nadzór nad ochroną przed zagrożeniami dla życia i zdrowia w obiektach przemysłowych, w tym w instalacjach nuklearnych, kopalniach, w systemach dostawy gazu i elektryczności, oraz w sąsiedztwie tych obiektów. HSE sprawowała również jedną z wiodących ról w opracowaniu normy IEC 61508 i posiada duże doświadczenie w zagadnieniach związanych z zastosowaniem tej normy w różnych sektorach przemysłu.

Publikacja [13] jest podsumowaniem wyników przeglądu dokonanego w sektorze przesyłu i rozdziału w Wielkiej Brytanii przez HSE wspólnie z tymi sektorami. Przegląd ten miał na celu ocenę zakresu zastosowania elektroniki programowalnej w układach EAZ związanych z bezpieczeństwem funkcjonalnym oraz ocenę czy odpowiednie techniki i środki były użyte w projektowaniu, weryfikacji i eksploatacji tych układów. Zastosowane podejście polegało na dokonaniu oceny pewnej liczby układów czy są one związane z bezpieczeństwem, a następnie na ustaleniu jaka praktyka stosowana była w projektowaniu, weryfikacji i eksploatacji tych układów. Punktem odniesienia przy ocenie stosowanej praktyki była norma IEC 61508, która jest także normą Europejską EN i Brytyjską BS.

Analizowane układy obejmowały:

- układy zabezpieczeń;
- urządzenia łączeniowe z programowalnym interfejsem;
- zdalne układy sterowania i monitorowania;

– układy automatycznej restytucji zasilania.

Ustalono, że układy zabezpieczeń, układy automatycznej restytucji zasilania oraz programowalny interfejs urządzeń łączeniowych są związane z bezpieczeństwem z różnym poziomem ryzyka. Ponadto ustalono, że systemy SCADA, zależnie od realizowanych funkcji, mogą być związane z bezpieczeństwem. Ustalenia te były punktem wyjścia do dalszych prac.

Autorzy stwierdzają, że mimo coraz powszechniejszego stosowania urządzeń programowalnych w EAZ aktualnie stosowana praktyka przy projektowaniu, badaniu i eksploatacji tych urządzeń jest wciąż oparta na doświadczeniu, wynikającym z wieloletniego stosowania urządzeń elektromechanicznych. O ile schematy funkcjonalne stosowane przy zastosowaniu urządzeń elektromechanicznych są dalej ważne, o tyle zastosowanie w tych układach urządzeń programowalnych wymaga innego podejścia do weryfikacji działania tych układów. Wynika to z różnic między układami wykorzystującymi urządzenia elektromechaniczne, a odpowiadającymi im układami opartymi na urządzeniach programowalnych.

Urządzenia elektromechaniczne mają bardzo ograniczoną funkcjonalność. Ich zachowanie jest stosunkowo proste, łatwo zrozumiale i łatwe do sprawdzenia. Nienaruszalność bezpieczeństwa zapewniana przez te urządzenia, określana jest przez ich niezawodność i może być stosunkowo łatwo i pewnie oceniona przez testowanie typu. Uszkodzenia sprzętu mają charakter przypadkowy, wynikający między innymi ze zużycia sprzętu, dlatego przez zastosowanie redundancji takim samym lub podobny urządzeniem można łatwo poprawić niezawodność układu. Redundancja i prostota, umożliwiająca łatwe sprawdzenie wszystkich funkcji, daje de facto poczucie rozwiązania deterministycznego. Dlatego tradycyjne układy nie wymagają podejścia opartego na ocenie ryzyka i taka ocena nie jest stosowana.

Prawdopodobnie między innymi z tego względu autorzy stwierdzają, że norma IEC 61508 jest słabo rozumiana w sektorze przesyłu i rozdziału oraz wciąż jest trochę dyskusji na temat jej przydatności w tym sektorze. Z dyskusji, jakie miały miejsce w początkowym okresie wdrażania normy także w innych sektorach, można wywnioskować, że pewną trudność w zrozumieniu normy i pewną nieprzystawalność tej normy do tradycyjnie stosowanych metod oceny urządzeń może sprawiać także fakt, że jest to norma na proces, a nie na produkt.

Urządzenia programowalne realizują wiele funkcji w jednym urządzeniu. Mają inną charakterystykę błędów w działaniu, przy czym nad błędami spowodowanymi uszkodzeniami przypadkowymi sprzętu przeważają uszkodzenia systematyczne. Uszkodzenia systematyczne odnoszą się szczególnie do błędów w oprogramowaniu i prawdopodobieństwo tego rodzaju uszkodzeń rośnie, wraz ze wzrostem złożoności i ilości funkcji zaimplementowanych w jednym urządzeniu. Dlatego projektując układ redundancyjny trzeba uwzględnić możliwość wystąpienia niewłaściwego działania, spowodowanego takim samym błędem w oprogramowaniu urządzenia wykorzystanego do redundancji. Oznacza to, że w przypadku projektowania redundancji w oparciu

o urządzenia programowalne większą uwagę należy poświęcić zróżnicowaniu rozwiązania w urządzeniu redundancyjnym.

W przypadku oprogramowania testowanie też jest niezbędne do zapewnienia niezawodności i jest niezawodnym sposobem zapewnienia niezawodności działania w warunkach określonych w testowaniu, ale jest bardzo niewystarczające do oceny, czy dany układ może niewłaściwie zadziałać w innych, pozornie nieszkodliwych warunkach.

Ze względu na złożoność układów opartych na urządzeniach programowalnych, takie aspekty jak istniejące kompetencje i szkolenia wszystkich zaangażowanych w projektowanie, wprowadzanie do eksploatacji i eksploatację tych układów nabierają coraz większego znaczenia.

W wyniku przeglądu dokonanego przez HSE wspólnie z firmami sektora przesyłu i rozdziału firmy tych sektorów zaakceptowały, że wprowadzenie urządzeń i systemów programowalnych do sektora przesyłu i rozdziału wymaga uwzględnienia normy IEC 61508 i podjęły się opracowania poprzez Energy Networks Association (ENA) zwartych wytycznych do stosowania IEC 61508 tych sektorach. Odbiorcami tych wytycznych mają być przedsiębiorstwa energetyczne, a poprzez ich związki kontraktowe stosowanie opracowanych wytycznych zostanie rozszerzone na inne strony. Dokument ten ma promować wspólne podejście do dobrej praktyki w zakresie stosowania normy IEC 61508 i dążyć do przezwyciężenia jej złożoności.

Opracowywane wytyczne podzielono na dwie odrębne części. Pierwsza, która w trakcie pisania omawianej publikacji, była na etapie końcowym, dotyczy zasadniczego pytania czy dany system lub urządzenie wykonuje funkcję związaną z bezpieczeństwem, i jeśli tak, to jaki poziom SIL jest właściwy. Jest to bardzo ważna część wytycznych, ponieważ użytkownik lub jego pośrednik musi być w stanie dokonać opartej na ocenie ryzyka, oceny krytyczności funkcji spełnianej przez dane urządzenie lub system, który użytkownik zamierza zastosować.

Druga część wytycznych dotyczy metod zapewnienia i utrzymania wymaganego poziomu bezpieczeństwa przez cały czas życia danego układu w oparciu o tzw. cykl życia bezpieczeństwa. Odpowiedzialność za cykl życia bezpieczeństwa danego układu podzielona została pomiędzy wytwórców urządzeń i podsystemów, integratorów systemów oraz użytkowników. Zgodnie z wytycznymi:

- Wytwórcy urządzeń i podsystemów odpowiedzialni są za projektowanie i weryfikację zdolności danego urządzenia lub podsystemu do wypełniania swojej funkcji do określonego poziomu SIL (ang. SIL capability).
- Integratorzy systemów odpowiedzialni są za projektowanie i weryfikację systemów, złożonych z urządzeń i podsystemów o określonym SIL, spełniających funkcje bezpieczeństwa zgodnie z wymaganym poziomem SIL.
- Użytkownicy (przedsiębiorstwa przesyłu i rozdziału) odpowiedzialni są za specyfikację właściwego poziomu SIL dla danej funkcji bezpieczeństwa i upewnie-

nie się, że systemy zastosowane w ich sieciach zostały właściwie zaprojektowane i zweryfikowane dla wyspecyfikowanego poziomu SIL oraz za właściwą ich obsługę i konserwację. Ponoszą również odpowiedzialność za zapewnienie ciągłej kontroli nad zarządzaniem tymi systemami, obejmującym takie zagadnienia jak aktualizacja oprogramowania, zmiany nastawień, zabezpieczanie haseł, zmiana konfiguracji, itp. Odpowiedzialni są również za zarządzanie końcem pracy tych systemów, gdy malejąca niezawodność może zmniejszyć początkową wartość SIL.

W publikacji podano, że powyższy zakres odpowiedzialności w swojej podstawowej postaci nie różni się tak bardzo od stanu aktualnie oczekiwanego w przedsiębiorstwach, w których narzędzia i procedury procesu zarządzania są skutecznie stosowane. Jest jednak oczywiste, że w przypadku systemów programowalnych w podanych zakresach odpowiedzialności poszczególnych stron większy nacisk oprócz testowania powinien być położony także na zarządzanie. Efektywne zarządzanie cyklem życia systemów programowalnych wymaga coraz bliższej współpracy między wszystkimi stronami dla zapewnienia, że stosowane u nich procesy zarządzania opracowane zostały pod kątem potrzeb urządzeń programowalnych i są ze sobą spójne.

W końcowej części publikacji ponownie zawarte jest stwierdzenie, że zastosowanie układów programowalnych w EAZ jest obecnie w bardzo dużym stopniu oparte na poprzednio stosowanej, sprawdzonej przez wiele lat praktyce, jaka ukształtowała się przy zastosowaniu układów elektromechanicznych. O ile jednak praktyka ta pozostaje właściwa w odniesieniu do funkcjonalności układów programowalnych o tyle nie jest efektywna, jeśli idzie o zapewnienie odpowiedniego poziomu nienaruszalności bezpieczeństwa. Dlatego zaproponowano żeby dokonać przeglądu istniejących procedur w zakresie EAZ i żeby to poprawione podejście było oparte na obecnych normach dla systemów związanych z bezpieczeństwem, a w szczególności na normie IEC 61508. Uwzględnienie tych norm nieuchronnie wpłynie na sposób, w jaki urządzenia będą projektowane, wytwarzane, weryfikowane, konserwowane i eksploatowane. Jednak zmiany powinny w większości zmierzać raczej do korekt lub ponownego przeanalizowania stosowanych obecnie procesów niż prowadzić do całkowitych zmian.

W podsumowaniu omawianej publikacji zawarte jest stwierdzenie, że elektroenergetyka brytyjska w oparciu o wytyczne HSE opracowuje aktualnie wytyczne zastosowania zasad normy IEC 61508 do zabezpieczeń w sektorze przesyłu i rozdziału. Jednak ze względu na międzynarodowy charakter działalności w tych sektorach oraz międzynarodowy charakter normy IEC 61508 ważne jest żeby zagadnienie to przedyskutowane było na poziomie międzynarodowym w celu osiągnięcia wspólnych uzgodnień. Następnie przeanalizowane muszą być zależności miedzy IEC 61508 a innymi normami IEC/CENELEC i normami innych organizacji na produkt lub system w dziedzinie przesyłu i rozdziału. Ma to na celu uzyskanie wspólnego rozumienia wpływu normy IEC 61508 na sektor przesyłu i rozdziału w najlepszym interesie

wszystkich zainteresowanych stron i intencją zarówno HSE jak i energetyki brytyjskiej jest dążyć do takiego celu.

5. NIEKTÓRE PRACE ZWIĄZANE Z ZASTOSOWANIEM NORMY IEC 61508 DO UKŁADÓW ZABEZPIECZEŃ W ELEKTROWNIACH KONWENCJONALNYCH

Prace związane z wdrożeniem w sektorze elektroenergetyki w Wielkiej Brytanii metody projektowania układów automatyki i zabezpieczeń opartej na ocenie zagrożeń i ryzyka z wykorzystaniem normy IEC 61508 i norm pochodnych prowadzone są również w odniesieniu do elektrowni konwencjonalnych sektora wytwórczego. Prace przedstawione w opublikowanych informacjach obejmowały zastosowanie podejścia opartego na normie IEC 61508 zarówno w nowych układach zabezpieczeń, jak i do oceny poziomu bezpieczeństwa w układach istniejących, powstałych nieraz na długo przed powstaniem normy IEC 61508, w latach 1960., 1970. i w połowie lat 1990., kiedy podejście oparte na ocenie ryzyka, na którym oparta jest norma IEC 61508, nie było stosowane w sektorze elektroenergetyki. Zakres dokonanej oceny obejmował układy zabezpieczeń kotłów, turbin, itp. we wszystkich tradycyjnych elektrowniach sektora wytwórczego: węglowych, olejowych, gazowych i wodnych, łącznie z kogeneracją [18], [17], [10].

Publikacja [18] opisuje pierwsze kroki związane z wprowadzeniem normy IEC 61508, jakie wkrótce po wprowadzeniu tej normy podjął RWE npower w odniesieniu do swoich elektrowni węglowych i olejowych. Zawiera również opis zrealizowanego studium przypadku, które służyło do zademonstrowania sposobu zastosowania opracowanego w RWE npower diagramu sekwencji technik bezpieczeństwa, jako podejścia do tworzenia w elektrowniach systemów związanych z bezpieczeństwem zgodnie z IEC 61508. W podsumowaniu publikacja stwierdza, że RWE npower ocenia ogólne podejście zawarte w normie IEC 61508 jako doskonałe podejście do budowy systemów związanych z bezpieczeństwem.

6. PODSUMOWANIE

Omówione wyżej z braku miejsca bardzo pobieżnie publikacje [6], [13] i [18] oraz prezentacje [4], [17], [10], zawierają opis ważnego doświadczenia z praktycznych prac, związanych z wprowadzaniem nowego podejścia do projektowania i eksploatacji układów EAZ i układów zabezpieczeń w elektrowniach, coraz powszechniej opartych na urządzeniach programowalnych, które powoli wypierają tradycyjne układy elektromechaniczne.

Wytwórca systemu czy urządzenia programowalnego może podać, że przetestował oprogramowanie tak dokładnie jak to jest możliwe. Jest to jednak subiektywna ocena wytwórcy, oparta na kwalifikacjach i możliwościach, jakimi dysponuje. I nie chodzi tylko o to, że może to być za mało dokładne testowanie, ale także o to, że może być zbyt dokładne, z czym wiążą się duże niepotrzebne koszty, jak i o znaczenie prawne takiej deklaracji na wypadek nieszczęśliwego zdarzenia. Potwierdzenie wymaganego poziomu nienaruszalności bezpieczeństwa systemu, w tym oprogramowania, zgodnie z powszechnie zaakceptowaną normą międzynarodową, daje wszystkim, wytwórcom, klientom i organom nadzoru, poczucie należytej staranności w dążeniu do zapewnienia bezpieczeństwa.

Z publikacji wynika, że w przemyśle, gdy rozważane jest zastosowanie normy IEC 61508 w miejsce istniejących metod zapewnienia odpowiedniego poziomu bezpieczeństwa powszechne jest narzekanie, że procedury wymagane przez tę normę są zbyt rozbudowane i znacznie podniosą koszty urządzeń i systemów. W prezentacji [3] podano, że w przemyśle maszynowym zastosowanie podejścia opartego na ocenie ryzyka, na którym oparta jest norma IEC 61508 i normy pochodne, wciąż uważane jest za zbyt wielkie obciążenie i aby być po bezpiecznej stronie wymaga się najwyższego poziomu SIL 4, który w praktyce wymagany jest rzadko. Z publikacji wynika, że nienaruszalność bezpieczeństwa wymagana dla EAZ jest zwykle SIL1, a najwyżej SIL2, natomiast dla systemów zabezpieczeń w elektrowniach SIL2 lub SIL3. Miedzy nienaruszalnością SIL1 i SIL2 a SIL3 i SIL4 jest skokowa zmiana wymagań odnośnie stosowanych procedur i tym samym kosztów.

LITERATURA

[1] ACOS references to IEC 61508 series in other standards, dokument 65A/571/INF, 02-19-2010 (http://www.iec.ch/functionalsafety/pdf/65A_571e_INF.pdf).

[2] *ALARP "at a glance"* http://www.hse.gov.uk/risk/theory/alarpglance.htm.

[3] FALLER R., *Evolution of European Safety Standards*, Exida, 2002 (http://www.exida.com/articles/Rockwell.pdf).

[4] FREEMAN P., *SIL evaluation: Practical Experience of Developing IP Gaidance on Assesssing the Safety Integrity of Electrical Supply Protection*, The IET Seminar on SIL Determination: Principles and Practical Experience, London, 28 March 2007.

[5] *Frequently Asked Questions*, IEC Safety Zone, http://www.iec.ch/functionalsafety.

[6] *Guidance on assessing the safety integrity of electrical supply protection*, The Energy Institute, London, 2006.

[7] *HSE accident reports* http://www.icheme.org/resources/safety_centre/publications/hse_accident_reports.aspx

[8] IEC 61513: *Nuclear power plants – Instrumentation and control for systems important to safety – General requirements for systems*.

[9] JAN M., DAVID V., LALANDE J., PITEL M., *Usage of the safety-oriented real-time OASIS approach to build determiniostic protection relays*, International Symposium on Industrial Embedded Systems, IEEE, 2010.

[10] McCOLLUM D., *Legacy Systems Issues*, The IEE Seminar on SIL Determination: Principles and Practical Experience, 2006.
[11] PN/EN/IEC 61508: *Bezpieczeństwo funkcjonalne elektrycznych/elektronicznych/ programowalnych elektronicznych systemów związanych z bezpieczeństwem*. Część 1: *Wymagania ogólne*, Część 2: *Wymagania dotyczące elektrycznych/elektronicznych /programowalnych elektronicznych systemów związanych z bezpieczeństwem,* Część 3: *Wymagania dotyczące oprogramowania,* Część 4: *Definicje i skrótowce*, Część 5: *Przykłady metod określania poziomów nienaruszalności bezpieczeństwa*, Część 6: *Wytyczne do stosowania IEC 61508-2 i IEC 61508-3*, Część 7: *Przegląd technik i miar*.
[12] PN/EN/IEC 61511: *Bezpieczeństwo funkcjonalne - Systemy Automatyki Zabezpieczeniowej dla Przemysłu Procesowego*, cz. 1-3.
[13] PUREWAL S., WALDRON M.A., *Functional safety in application of programmable devices in power system protection and automation*, Eighth IEE International Conference on Developments in Power System Protection, 2004.
[14] *SEPCOS-PRO*, przekaźnik firmy Secheron, http://www.secheron.com/uk/products-services/gamm24-sepcos-pro-protection-relay.html.
[15] SMITH D.J., SIMPSON K.G.L., *Functional Safety-A Straightforward Guide to Applying IEC 61508 and Related Standards*, 2nd Edition, Elsevier, 2004.
[16] STOREY N., *Safety-Critical Computer Systems*, Addison-Wesley Longman 1996, 2-8.
[17] WYMAN P.,M., *The Approach to legacy systems within the non-nuclear power station sector*, 4th IET Seminar on SIL Determination – Minimising the Risk in Your Systems, 5th December 2008.
[18] WYMAN P.M., *A Case Study of The Application of BS:EN 61508 in Electrical Power Generation*, 2nd Institution of Engineering and Technology International Conference on System Safety, 2007.

FUNCTIONAL SAFETY OF RELAY PROTECTION SYSTEMS BASED ON PROGRAMMABLE DEVICES

In connection with the growing number of programmable devices used in relay protection systems, the growing complexity of technical systems used in industry, including safety-related systems, and increasing demands for safety, that requires also consideration of the reliability of power supply, after publication of the international standard IEC 61508 in developed countries works were undertaken connected with application this standard also in the electric power industry, including to power systems relay protection. The paper presents a brief historical overview, the basic concept on which the IEC 61508 standard is based and the status of current work to implement this standard for power systems relay protection. At the end are given also some works related to the use of this standard for protection systems in conventional power plants.