Programowa ocena ryzyka dla przyrządów pomiarowych w metrologii prawnej.

II. PRZEGLĄD ISTNIEJĄCYCH METOD

…. W tym kontekście, termin *ryzyko* może być traktowane jako iloczyn prawdopodobieństwa, że niezbędne wymagania nie są zgodne i wywołują konsekwencji prawne wynikające z jego naruszenia w MID. Ważne jest aby pamiętać, że straty finansowe nie muszą mieć miejsca, jednak są jedyną podstawą dla wymagań analiz ryzyka.

A. ISO/IEC 27005

Prawdopodobnie najważniejszy jest rodzina standardów ISO/IEC 27000, które odnoszą się do wszystkich aspektów systemów informatycznych zarządzania bezpieczeństwem (ISAMS). Zgodnie z ISO/IEC 27005 [3], „”ryzyko jest kombinacją konsekwencji, które mogłyby wynikać z wystąpień nieoczekiwanych zdarzeń i prawdopodobieństwa wystąpienia zdarzenia.” Zatem potrzebne są trzy różne składowe obliczeń ryzyka, mianowicie:

- lista nieoczekiwanych zdarzeń,

- konsekwencje wynikające z tych zdarzeń,

- i prawdopodobieństwo wystąpienia każdego ze zdarzeń.

W celu uzyskania wszystkich trzech składowych [3] zawiera szczegółowe informacje na temat uogólnionej procedury wyprowadzenia oceny ryzyka. Standardowe pola oceny ryzyka w łańcuchu logicznym obejmującym kontekst, oszacowanie ryzyka, poprawa ryzyka, gdzie oszacowanie ryzyka składa się z ryzyka identyfikacji, ryzyka estymacji i ryzyka obliczeń.

Podczas fazy identyfikacji ryzyka, aktywa są identyfikowane jako pierwsze. Pochodzą one z „listy składowych właściciela, lokalizacji i funkcji”, wynikają z listy zarządzanych aktywów. Następnie dla każdego możliwego aktywa, zbierane są informacje o zagrożeniu na podstawie przeglądu incydentów, właścicieli aktywów i możliwych katalogów zewnętrznych. Te zagrożenia korespondują z z „nieoczekiwanymi zdarzeniami” o których wspomniano wyżej. Następny krok składa się z identyfikacji istniejącego mechanizmu kontroli ryzyka, na przykład, określonych z dostarczonej dokumentacji. Identyfikacja ryzyka jest uzupełniana kosztami, które mogą być poniesione gdy wprowadzono jakieś zagrożenia. W tym kontekście koszty mogą być miarą szkody, którą należy zrównoważyć. Tym samym zagrożenia bez wywołania kosztów nie stanowią zagrożenia.

Następna część ISO/IEC 27005, dotyczy oszacowania ryzyka, prawdopodobnie najbardziej istotnego w kontekście tego opracowania. Standard rozważa oba jakościowe i ilościowe podejścia do obliczeń prawdopodobieństwa ryzyka, gdzie ilościowe podejście wykorzystuje skalę wartości liczbowych … z wykorzystaniem danych z różnych źródeł. Takie wartości liczbowe są warunkiem zapewnienia porównań między wynikami oceny ryzyka dla różnych produktów dostarczanych przez różnych inspektorów. Aby uzyskać aktualne prawdopodobieństwa, ISO/IEC 27005 po pierwsze przypisuje pewien wpływ lub konsekwencje do incydentu, który mógłby mieć skutki wynikające z zagrożenia w postaci kosztów. Możliwe przykłady wpływów zawierają utratę poufności pewnych aktywów jak również naruszenie integralności niektórych aktywów. W końcowym etapie szacowane jest prawdopodobieństwo z którym występuje zagrożenie. Ważnym współczynnikiem w tym kontekście jest częstotliwość występowania każdego zagrożenia w rzeczywistości i trudności w odbudowaniu strat.

## 2 Zarys projektu

### Wprowadzenie

Wraz z wprowadzeniem zmienionych dyrektyw europejskich 2014/31 / UE [1] 2014/32 / UE [2] wchodzą w życie następujące wszystkie moduły oceny:

*Na podstawie złożonej dokumentacji powinna być możliwa ocena zgodności zasadniczych wymagań przyrządów. Dokumentacja powinna zawierać odpowiednią ocenę ryzyka.*

To nowe wymaganie wynika z decyzji 768/2008/EC [3] wstecznie datowanej na 2008.

Obie zmienione dyrektywy powinny być przetłumaczone na język prawodawstwa do kwietnia 2016. W Niemczech przykładowo Akt pomiaru i weryfikacji (MessEG) przewiduje analizy i ocenę wszystkich przyrządów pomiarowych podlegających prawnej kontroli (patrz odpowiednia regulacja (MessEV [4]). Według opinii wewnętrznego rynku Europejskiego wykonanie zgodności oceny w jednym kraju powinno być uznawane we wszystkich innych krajach. Warunkiem przyjęcia tego jest akceptacja oczywiście zharmonizowanych procedur przez wszystkie jednostki notyfikujące. Od czasu gdy technologia informacyjna (information and communication technology (ICT)) jest coraz częściej integralną częścią wielu przyrządów pomiarowych zagrożenia i w konsekwencji ryzyka związane z ITC zaczynają być coraz bardziej ważne.

W kontekście nowego podejścia [5] producenci podlegają wymogom, ale nie ma jawnych normalnie dostępnych instrumentów technicznych. Tym samym producenci nie mogą być zmuszani do postępowania zgodnie z jednolitą procedurą oceny ryzyka. Z perspektywy jednostki notyfikującej, jakkolwiek standardowe procedury byłyby bardzo pomocne podczas porównywania wyników ocen pomiędzy innymi jednostkami notyfikującymi. Dodatkowo, scenariusze ataku opisane przez różnych producentów podlegałyby porównaniu lub nawet zmianie na podstawie jednolitej procedurze.

Tak więc podstawowym celem ewidencji mogłoby być stworzenie możliwości do przedstawienia różnic w dokumentacji oceny ryzyka dostarczonej przez producenta. Jeśli producent korzysta z procedury oceny ryzyka podobnej do tej, która jest stosowana przez jednostki notyfikujące, proces badania i identyfikacji może być znacznie przyśpieszony. Jeśli stosowane są międzynarodowe i ustalone procedury, to zakłada się, że będą one łatwiej akceptowane przez wszystkie zaangażowane strony.

Innym ważnym aspektem procedury będzie opracowanie i wywoływanie czynnika akceptacji przez przemysł nowych technologii i innowacji. Jeśli przyjęcie procedur dla nowych technologii będzie stosunkowo łatwe, to akceptacja ich byłaby by podobnie łatwa. Wirtualna baza wiedzy dotycząca oceny ryzyka i powtarzających się scenariuszy ataku mogłaby ułatwić przyjęcie nowych procedur.

Zgodnie z rozporządzeniem 765/2008 [5], organy nadzoru rynku również wykonują odpowiednie procedury oceny ryzyka. Jednakże, ze względu na różne perspektywy nadzoru rynku i notyfikowana, odpowiednie oceny ryzyka są również inne. Nadzór rynku, z jednej strony, ocenia zagrożenia pochodzące z przyrząd pomiarowy, który nie jest zgodny z zasadniczymi wymaganiami (pre / post-rynkowymi).

Przyrządy pomiarowe, które wykazały nieprawidłowości są rejestrowane w krajowych i Europejskich bazach danych. Włączenie przedmiotowej wiedzy nabytej przez organ nadzoru rynku ma na celu dalszą poprawę oceny ryzyka poprzez zamknięcie pętli sterowania.

Ocena istniejących krajowych i międzynarodowych baz wiedzy, które monitorują  
nieprawidłowości przyrządów pomiarowych na rynku (np. obsługiwanych internet -  
system informacji i komunikacji dla paneuropejskiego nadzoru rynku (ICSMC)) będzie również częścią projektu. Celem tej oceny będzie rozszerzenie bazy danych, aby oznaczyć incydenty związane z IT i je ocenić.

Wyniki projektu dostarcza się do Europejskiego i krajowego ciała (WELMEC, OIML) aby osiągnąć zharmonizowany lub ustandaryzowany poziom w Europie. Będą zbierane Listy wsparcia z OIML oraz WELMEC.

Niemcy, reprezentowane przez PTB, przewodniczą Grupie Roboczej "Oprogramowanie" WELMEC, która obecnie składa się z 19 przedstawicieli państw członkowskich UE, członków i stowarzyszeń dużych producentów. Grupa robocza zajmuje się i dąży do harmonizacji procedur w połączeniu z wszystkimi zagadnieniami związanymi z ICT, którymi są również zainteresowane branże przyrządów pomiarowych lub, jednostki notyfikujące, które uznają spełnienie wymagania za kwestię zasadniczą.

Wreszcie, opracowanie zharmonizowanej oceny ryzyka przez WELMEC zostanie przedłożone OIML. Komisja Europejska na ogół przyjmuje dokumenty OIML jako zharmonizowane standardy normatywne. Niemcy, reprezentowane przez PTB, przewodniczą podkomisji "Oprogramowanie w systemach pomiarowych".

W chwili przyjęcia odpowiednich środków bezpieczeństwa może być również interesujący dla szerszej społeczności, wyjściowy projekt może być również złożony do innych europejskich organów normalizacyjnych takich jak ETSI i CEN / CENELEC.

### 3.2 Pakiety robocze

Poniższy rozdział zawiera krótki opis każdego z planowanych pakietu prac. Więcej informacji i szczegółowy planu można znaleźć w sekcji 4.

#### 3.2.1 WP1: Wyprowadzenie wymagań dla metody oceny ryzyka

Pierwszy etap tego pakietu składać się będzie z opracowania kwestionariusza dotyczącego pożądanych cech metody oceny ryzyka. Kwestionariusz ten następnie będzie rozdzielony wśród zaangażowanych jednostek notyfikacyjnych, a wyniki zostaną zebrane i ocenione. Na podstawie wyników badań, zostaną wyprowadzone i zdefiniowane metody oceny.

Lista zostanie rozwinięta o pewne cechy wspólne jak wszystkie/ pewne metody oceny ryzyka takie jak:

* Wymagane dane wejściowe
* Dane wyjściowe
* Zdolność wyprowadzenia nowego wektora ataku
* Złożoność metody w odniesieniu do wymaganych możliwości obliczeniowych, wyposażenia itp.

W tym samym czasie rozpoczęta będzie podobna działalność badawcza polegającą na zbieraniu danych na temat metod, które są wykorzystywane do identyfikacji, śledzenie i aktualizacji kierunków ataku. Ponadto, wszyscy partnerzy projektu będą wspólnie rozwijać abstrakcyjną koncepcję urządzenia pomiarowego z funkcjami powszechnie stosowanymi w tym obszarze.

Końcowym krokiem tego pakietu będzie zebrane metod, które będą porównane na podstawie wspomnianego abstrakcyjnego przyrządu pomiarowego.

#### 3.2.3 WP3: Wybór lub definicja odpowiednich metod

Z pomocą wyników wymagań z WP2, zebrane będą metody oceny ryzyka będą mogły być rozwijane. W tym czasie sprawdzane będą w celu rozwinięcia lub uzupełnienia, standardy branżowe. Z pomocą wyników tej działalności, jedna (ewentualnie większa ilość) metod wybranych zostanie jako badania kluczowe obiektu w dalszej części projektu.

#### 3.2.4 WP4: Ocena wybranej metody

Po zdefiniowaniu wspólnych metod oceny ryzyka podlegających badaniu, będzie użyty do wybranej metody abstrakcyjny przyrząd pomiarowy z WP1.

W tym samym czasie badane będą możliwości włączenia baz wiedzy nadzoru rynku (takich jak ICSMC i SAM). Z pomocą wyników wspomnianych badań założone zostanie wirtualne centrum powiadamiania o incydentach związanych z software’m. Włączając w to produkcję przewodników dokumentujących incydenty związane z software’m dla organów nadzoru rynku.

Poprzez wykorzystanie procedury pozostaną jeszcze do zdefiniowania dane pozyskane przez wirtualne centrum powiadamiania dla utrzymania bieżącej bazy danych.

#### 3.2.5 WP5: Testy w terenie

#### 3.2.6 WP6: Określenie konsekwencji

#### D.Luśtyk - potencjalne zaangażowanie

Nawiązując do naszej rozmowy, po wcześniejszych konsultacjach z osobą / osobami zainteresowanymi uczestnictwem w projekcie, posiadających wiedzę nt. potencjalnych zagrożeń dotyczących przyrządów pomiarowych, dla wypracowania uogólnionej koncepcji matematycznego ujęcia zagadnień oceny ryzyka i abstrakcyjnego przyrządu pomiarowego, proponuję swój udział w:

* opracowaniu ww. zagadnień z wykorzystaniem: logiki rozmytej, diagramów decyzyjnych, analizy składowych głównych, sztucznych sieci neuronowych lub innych propozycji,
* napisaniu programów, przeprowadzeniu testów, ich wdrożeniu.

Wsparcie zainteresowanych uczestników projektu (w szczególności znających zagadnienia zagrożeń i ich szacowania w przyrządach pomiarowych) pomogłoby wypracować idee rozwiązania, która z jednej strony miałaby związek z praktyką, a z drugiej pozwoliłaby na jej implementację informatyczną.