STUDIA INFORMATICA 2001
Volume 22 Number 2 (44)

Grzegorz FILIPCZYK
Politechnika Śląska, Instytut Informatyki

BADANIE BEZPIECZEŃSTWA SYSTEMU KOMPUTEROWEGO METODĄ HAZOP

Streszczenie. W artykule przedstawiono założenia metody HAZOP (ang. *hazard and operability*) przeznaczonej do badania bezpieczeństwa systemów komputerowych. Za pomocą metody rozpatrywane są możliwe zagrożenia (hazardy) prawidłowego działania systemu, a także ich konsekwencje. Opisany został tryb prowadzenia analizy systemu zakładający ustaloną proceduralnie dyskusję nad poszczególnymi elementami formalnego modelu systemu. Pokazano także krótkie studium problemowe, będące częścią badań nad systemami informatycznymi jednostek samorządowych.

COMPUTER SYSTEM SECURITY ANALYSIS WITH HAZOP METHODOLOGY

Summary. In this article the HAZOP methodology for analyzing computer system security has been presented. With that methodology deviations (hazards) and their consequences from desired behavior are recognized. Flow of the control process, based on the standardized discussion over selected entities of the model, has been described. A short problem study, being a part of the researches over council computer systems, is shown as well.

1. Wprowadzenie

Bezpieczeństwo systemu komputerowego jest osiągane przez działanie różnych mechanizmów na ważne z punktu widzenia użytkownika zasoby. Jedna z definicji mówi, że system jest bezpieczny, gdy prawdopodobieństwo wystąpienia zagrożenia zdrowia człowieka lub zaistnienia szkód materialnych oraz innych jest bardzo małe. Cecha zasobu, która może doprowadzić do wystąpienia zagrożenia, nazywana jest podatnością, przy czym istnienie

takiej cechy nie stanowi o pewności wystąpienia zagrożenia, ale o jego możliwości. W omawianym dalej przykładzie dla zasobu *zbiór zakazów sądowych prowadzenia pojazdów* istnieje cecha *jawność zapisu danych w zbiorze* (inaczej: *brak zabezpieczenia kryptograficznego*) stanowiąca o możliwości nieuprawnionej modyfikacji lub usunięcia zapisu. Podatność ta może być przyczyną powstania szkody niematerialnej w postaci wydania prawa jazdy osobie nieuprawnionej. Wyszukiwanie takich sytuacji, tj. możliwości wystąpienia zdarzeń naruszenia bezpieczeństwa (hazardu), jest przedmiotem działania metody HAZOP (ang. *hazard and operability*). HAZOP nie jest ściśle formalną, matematyczną metodą oceny bezpieczeństwa. W literaturze nazywa się ją czasem półformalną inspekcją dokumentową [2].

2. Założenia metody

HAZOP jest metodą badania bezpieczeństwa powstałą w latach 60 w Wielkiej Brytanii na potrzeby przemysłu chemicznego. Łatwość zastosowania spowodowała, że przyjęła się także w innych dziedzinach, w tym w informatyce. W metodzie HAZOP zakłada się istnienie formalnej reprezentacji badanego systemu w postaci modelu zrozumiałego dla członków zespołu analitycznego. Identyfikacja możliwych hazardów polega na ich wyszukiwaniu w toku ustalonej proceduralnie dyskusji między członkami zespołu ekspertów. Dyskutowane są podatności elementów widocznych w modelu formalnym oraz związane z nimi możliwości zagrożeń, a także wydawane są zalecenia potrzebnych zmian lub dodatkowych badań. HAZOP może być stosowany na każdym z etapów w cyklu życia systemu komputerowego, zarówno do analizy projektu, jak i działającego produktu. Proces badania systemu wymaga, by powstał zespół ekspertów liczący do siedmiu osób. Każdy z członków zespołu powinien być ekspertem w jakimś obszarze dziedziny systemu (projektant, wykonawca, użytkownik, prawnik, inżynier dziedziny związanej itd.). Zespół dyskutuje nad prawdopodobnymi hazardami w trakcie spotkań prowadzonych przez tzw. lidera. Typowe badanie systemu obejmuje kilka spotkań trwających do dwóch godzin.

Podczas analizy wykorzystywane mogą być różne modele formalne, przy czym jednostkowe spotkanie w ramach badania skupiać się musi na jednym modelu. Modele formalne, zasady ich budowy i interpretacji, muszą być zrozumiałe dla członków zespołu. Przykładami możliwych narzędzi tworzenia modeli są:

- diagramy przepływu danych,
- diagramy przepływów sterowania,
- diagramy związków encji,
- diagramy przejść stanów.

Dobrą cechą reprezentacji systemu jest jej hierarchiczność, pozwalająca na przekrojowe spojrzenie na badany system komputerowy. Przykładem wykorzystania hierarchiczności może być zastosowanie diagramów przepływu danych równoważonych warstwowo (w górę lub w dół). HAZOP nadaje się do prowadzenia analizy na wysokich i średnich warstwach modelu. Im większy stopień szczegółowości, tj. im niższa warstwa modelu, tym wyższe są koszty prowadzenia analizy, a zarazem mniejsza zasadność wykorzystania metody HAZOP. Standard [9] zaleca dla niższych warstw stosowanie np. metody FMEA.

Tabela 1

Słowa kluczowe w metodzie HAZOP

Słowo kluczowe	Interpretacja
No	Zamierzony cel nie jest osiągany nawet częściowo i nie dzieje się nic poza tym.
More	Wartość atrybutu jest większa od zamierzonej.
Less	Wartość atrybutu jest mniejsza od zamierzonej.
As well as	Zamierzony cel jest osiągnięty, ale poza tym występują także inne efekty.
Part of	Zamierzony cel osiągnięty jest częściowo.
Reverse	Osiągnięty został cel odwrotny do zamierzonego.
Other that	Osiągnięty został cel różniący się od zamierzonego.
Early	Zamierzony cel wystąpił wcześniej względem określonego czasu.
Late	Zamierzony cel wystąpił później względem określonego czasu.
Before	Zamierzony cel wystąpił wcześniej względem określonego zdarzenia.
After	Zamierzony cel wystąpił później względem określonego zdarzenia.

Dla każdego elementu na modelu rozpatrywane są możliwe odstępstwa od zamierzonego działania. Odstępstwa te wyrażane są przez tzw. słowa kluczowe (ang. *guide words*) odniesione do atrybutów opisujących ten element. W metodzie, w zależności od rodzaju modelu formalnego, stosuje się pełny lub okrojony zbiór słów kluczowych. Tabela 1 (za [9]) przedstawia listę wszystkich słów kluczowych oraz ich podstawową interpretację.

Interpretacja słów kluczowych nie jest ścisła w ramach metody. Dla różnych obszarów zastosowania badanych systemów, a także dla różnych reprezentacji formalnych znaczenia poszczególnych słów są inne. Powyższa tabela wymienia wszystkie możliwe słowa kluczowe oraz podaje ich podstawową interpretację. Dla modelu programu komputerowego interpretacja słowa *no* może brzmieć *brak przepływu danych lub sterowania*, a słowa *part of* – *przepływ danych lub sterowania niekompletny*. Istotne jest także, że poszczególne reprezentacje nie wykorzystują całego zbioru słów kluczowych. Podzbiór słów dla diagramów przepływu danych (ang. *DFD - data flow diagram*) jest następujący:

Tabela 2

Podzbiór słów kluczowych dla diagramów przepływu danych

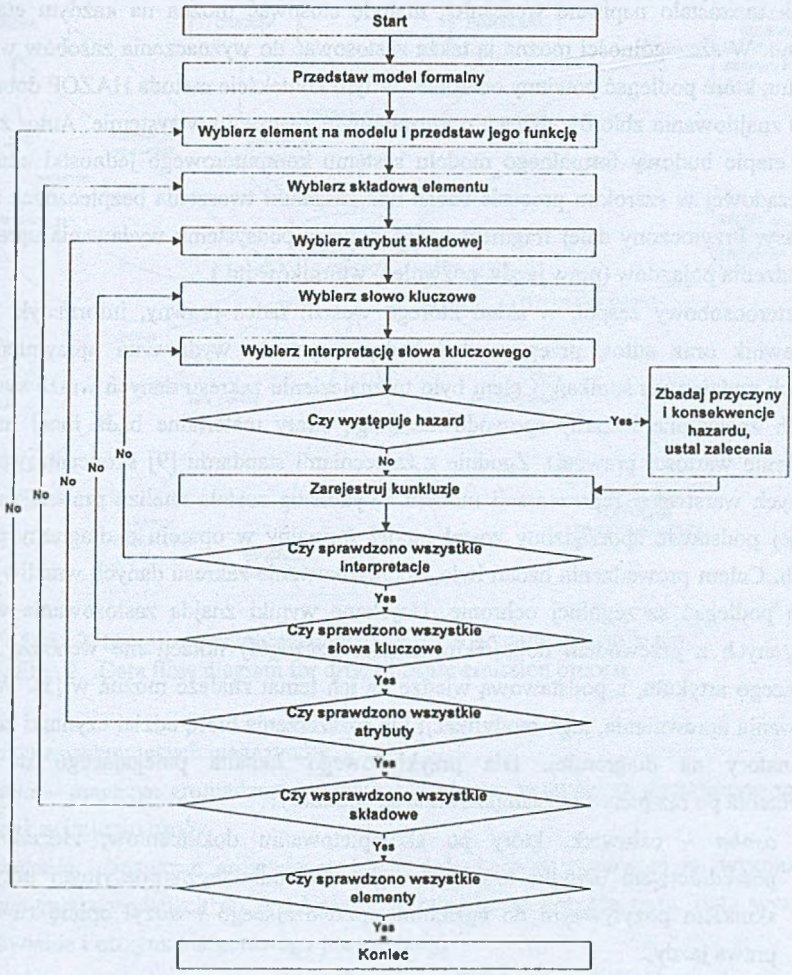
Element	Słowo kluczowe	Interpretacja
Przepływ	No	Brak przepływu.
	More	Więcej danych zostało przeniesionych, niż zamierzano.
	Part of	Przepływ niekompletny (np. w przypadku przepływu grupowego).
	Reverse	Przepływ o zmienionym kierunku[1].
	Other that	Dane w przepływie są kompletne, ale logicznie niespójne.
	Early	Przepływ występuje wcześniej, niż zamierzano.
	Late	Przepływ występuje później, niż zamierzano.
Wartość danej	More	Wartość danej za wysoka.
	Less	Wartość danej za niska.
Szybkość napływu danych	More	Szybkość napływu danych zbyt duża.
	Less	Szybkość napływu danych zbyt mała.

Zauważyć należy, że nie wszystkie słowa kluczowe są wymienione. Wobec niektórych z nich możliwa interpretacja pokrywa znaczenie innych słów, np. *more* (*więcej danych zostało przeniesionych, niż zamierzano*) zawiera w sobie logiczną interpretację słowa kluczowego *as well as*. O podanym wyżej rozumieniu słów kluczowych powiedzieć można, że jest możliwe i prawdopodobne. Nic nie stoi jednak na przeszkodzie, by, kiedy zespół uzna to za słuszne, wskazać własną interpretację – w szczególności rozszerzającą lub zawężającą zbiór słów kluczowych (rozszerzenie nie może jednak wykraczać poza zbiór podany w tabeli 1). Proponowane zbiory słów kluczowych dla innych niż DFD reprezentacji systemu podane są np. w [9].

„Przyłożenie" słowa kluczowego do wybranego elementu w modelu ma w konsekwencji dać odpowiedź na pytania: „jakie są możliwe przyczyny występujących wówczas hazardów" i „jakie są konsekwencje tych hazardów". Przykład: słowo *more* zastosowane do elementu *wartość danej x* generuje pytania: „jakie są możliwe przyczyny osiągnięcia przez daną *x* wartości przekraczającej dopuszczalny kres górny" oraz „jakie mogą być konsekwencje przekroczenia przez daną *x* wartości kresu górnego". W toku badań wybór elementu i zadanie powyższych pytań należy do zakresu pracy lidera zespołu. Rozpoczęta w ten sposób dyskusja nad obranym aspektem systemu zostaje protokołowana przez tzw. recordera. Ostateczne konkluzje zapisywane są do arkusza badań (tabela 3). Zapis przykładowej dyskusji podany

[1] Sytuacja taka w klasycznym diagramie przepływu jest niemożliwa. Na potrzeby metody przypadek taki jest jednak czasem rozpatrywany.

jest np. w [8]. Całkowity przebieg procesu badawczego dla dowolnego systemu (niekoniecznie informatycznego) przedstawiony jest na rys 1.



Rys. 1. Przebieg badania w metodzie HAZOP
Fig. 1. Flow of analysis in HAZOP

Podczas prowadzonych badań wykrywane są możliwe zagrożenia (hazardy) i ich przyczyny. Zespół może także wskazywać możliwe drogi osiągnięcia odpowiedniego stopnia bezpieczeństwa minimalizującego wskazane ryzyko. Nie jest jednak celem analizy HAZOP dokonywanie zmian w projekcie bądź działającym systemie. Z tego punktu widzenia HAZOP powinien być traktowany jako uzupełnienie innych form badania i osiągania bezpieczeństwa systemów.

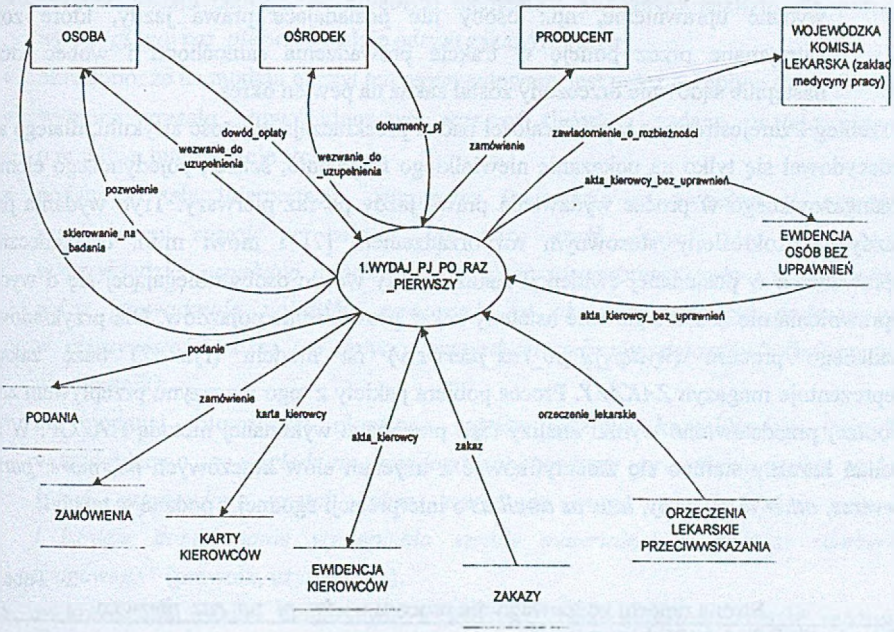
3. Przykład zastosowania

Jak to zostało napisane wcześniej, metodę stosować można na każdym etapie życia systemu. W szczególności można ją także zastosować do wyznaczenia zasobów wrażliwych systemu, które podlegać powinny ochronie. W tym kontekście metoda HAZOP dobrze nadaje się do znajdowania zbiorów danych o szczególnym znaczeniu w systemie. Autor zastosował ją na etapie budowy formalnego modelu systemu komputerowego jednostki administracji samorządowej w szerokim procesie badań nad zasadami tworzenia bezpiecznych systemów tej klasy. Przytoczony dalej fragment badań dotyczy podsystemu wydawania uprawnień do prowadzenia pojazdów (praw jazdy, pozwoleń, wtórników itd.).

Czteroosobowy zespół, w skład którego weszli: radca prawny, informatyk, urzędnik-użytkownik oraz autor, przeprowadził badanie systemu wydawania uprawnień w toku czterech godzinnych spotkań. Celem było tu znalezienie zakresu danych wrażliwych, wobec których znalezione hazardy spowodować mogą straty materialne bądź innej natury (np. naruszenie wartości prawnej). Zgodnie z zaleceniami standardu [9] skoncentrowano się na wyższych warstwach reprezentacji modelu. Wykonana została analiza prawna zagadnienia i na jej podstawie sporządzony został model formalny w oparciu o diagramy przepływu danych. Celem prowadzenia badań było zidentyfikowanie zakresu danych wrażliwych, które muszą podlegać szczególnej ochronie. Uzyskane wyniki znajdą zastosowanie w pracach zawiązanych z przewodem doktorskim autora. Szczegóły notacji nie wchodzą w zakres niniejszego artykułu, a podstawową wiedzę na ich temat znaleźć można w [3]. W procesie wydawania uprawnienia, jego modyfikacji lub rozszerzenia biorą udział czynniki zewnętrzne (terminatory na diagramie). Dla przykładowego zadania polegającego na wydaniu uprawnienia po raz pierwszy zaangażowane są podmioty:

- *osoba* – człowiek, który po skompletowaniu dokumentów, złożeniu ich za pośrednictwem ośrodka szkoleniowego w ośrodku egzaminacyjnym przystąpił ze skutkiem pozytywnym do egzaminu sprawdzającego i złożył opłatę za dokument prawa jazdy,
- *ośrodek* – ośrodek egzaminacyjny, który zebrał wymagane prawem dokumenty od osoby, stwierdził zdanie przez nią egzaminu i stosowne akta tej osoby (podanie, wniosek z adnotacją egzaminatora, orzeczenie lekarskie, fotografia itd.) przesłał do organu wydającego uprawnienie,
- *producent* – uprawniony podmiot wykonujący dokument uprawnienia (prawo jazdy) na zamówienie *osoby* złożone w jej imieniu przez organ wydający (prezydent miasta),
- *wojewódzka komisja lekarska* – ośrodek wykonywania i dokumentacji badań lekarskich, podmiot, który zawiadamiany jest o ewentualnych rozbieżnościach

między zapisami orzeczeń lekarskich przesyłanymi przez ośrodek a posiadanymi w ewidencji własnej organu.



Rys. 2. Diagram przypływu danych procesu wydania prawa jazdy
Fig. 2. Data flow diagram for driver license emission process

Proces korzysta z następujących magazynów:

- *podania* – magazyn gromadzący podania o wydanie uprawnienia dostarczane przez *ośrodek* w imieniu *osoby*,
- *zamówienia* – magazyn gromadzący kopie dokumentów zamówień na wykonanie uprawnienia wysyłanych do *producenta*, informacje te dotyczą m.in. daty wysyłki zamówienia i otrzymania gotowego prawa jazdy,
- *karty kierowców* – magazyn przechowujący dokumenty, których wzór określa rozporządzenie, są tu informacje o zakresie posiadanych uprawnień, zmianach w tych uprawnieniach, zatrzymaniach itp.,
- *ewidencja kierowców* – magazyn danych osobowych kierowców,
- *zakazy* – magazyn dokumentów sądowych lub podobnych (np. wyroków) orzekających o zakazach prowadzenia pojazdów, cofnięciu uprawnień itp.,
- *orzeczenia lekarskie przeciwwskazania*, magazyn orzeczeń lekarskich otrzymanych z *wojewódzkiej komisji lekarskiej*, na podstawie których nie można wydać określonego w orzeczeniu uprawnienia *osobie*, której orzeczenie dotyczy,

- *ewidencja osób bez uprawnień* – magazyn danych osobowych osób, nie-kierowców, wobec których ustalone zostały zakazy i którym na ich podstawie nie może zostać wydane uprawnienie, np.: osoby nie posiadające prawa jazdy, które zostały zatrzymane przez policję w trakcie prowadzenia samochodu i wobec których następnie sądownie orzeczony został zakaz na pewien okres.

Przebieg i zarejestrowane wyniki całości badań przekraczają objętość artykułu, dlatego autor zdecydował się tylko na pokazanie niewielkiego fragmentu, ściślej, pojedynczego elementu zaangażowanego w proces wydawania prawa jazdy po raz pierwszy. Tryb wydania prawa jazdy jest określony stosownym rozporządzeniem [7] i mówi m.in. o konieczności sprawdzenia w posiadanej ewidencji zakazów, czy wobec osoby ubiegającej się o wydanie uprawnienia nie został sądownie ustalony zakaz prowadzenia pojazdów. Dla przykładowego badanego procesu (*wydaj_pj_po_raz_pierwszy*) na modelu (rys. 2) bazę zakazów reprezentuje magazyn *ZAKAZY*. Proces pobiera pakiety z tego magazynu przepływem *zakaz*. Poniżej przedstawiono wyniki analizy tego przepływu wykonanej metodą HAZOP. W toku badań hazardy starano się zidentyfikować z użyciem słów kluczowych *no, more, part of, reverse, other than, early, late, as awell as* o interpretacji zgodnej z podaną w tabeli 2.

Tabela 3

Strona raportu końcowego dla procesu *wydaj_pj_po_raz_pierwszy*

Table 4 HAZOP Study for **Wydaj uprawnienie**

HAZOP: Procedura wydania pierwszego prawa jazdy Description:
Diagram: 01. Wydaj_pj_po_raz_pierwszy
Date:
Leader: Grzegorz Filipczyk
Recorder:
Team Members: Andrzej Oświęcimski, Dorota Malejka, Mariusz Brewko

HAZOP ITEM	INTERCONNECTION	ATTRIBUTE	GUIDE WORD	CAUSE	CONSEQUENCE/ IMPLICATION	INDICATION/ PROTECTION	QUESTION/ RECOMENDATION	ANSWERS/ COMMENT
9	zakaz	data flow	no	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
10	zakaz	data flow	more	[illegible]	[illegible]	[illegible]		
11	zakaz	data flow	part of	[illegible]	[illegible]	[illegible]	[illegible]	
12	zakaz	data flow	reverse	nie występuje				
13	zakaz	data flow	other than	[illegible]	[illegible]			
14	zakaz	data flow	early	[illegible]	[illegible]	[illegible]	[illegible]	
15	zakaz	data flow	late	[illegible]	[illegible]	[illegible]	[illegible]	
16	zakaz	data flow	as well as	[illegible]	[illegible]	[illegible]	[illegible]	

Tabela 3 stanowi część raportu końcowego wyników badań. Przebieg identyfikacji hazardu za pomocą np. słowa *part of* był następujący:

- podjęta została decyzja, że kolejnym elementem poddanym analizie dla procesu *wydaj_pj_po_raz_pierwszy* będzie odczyt zakazów (lider),
- określono, że na modelu odczyt ten reprezentowany jest przez przepływ *zakaz* (lider),
- wybrane zostało słowo kluczowe *part of* (lider) i zadane zostało pytanie o możliwe interpretacje słowa,
- podana została interpretacja *„otrzymane informacje są niepełne, tj. przepływ zrealizowany zostaje w całości, ale tylko część danych jest prawdziwa"*, w przykładzie *„uzyskano informacje, że wobec sprawdzanej osoby ustalony został zakaz prowadzenia pojazdów szynowych na okres 6 miesięcy, podczas gdy w rzeczywistości zakaz ten dotyczył wszystkich rodzajów pojazdów"* (informatyk, użytkownik),
- dla podanej interpretacji określone zostały możliwe konsekwencje (szkody) w stwierdzeniu *„ze względu na prawdopodobne wydanie uprawnienia osobie, wobec której ustanowiony został zakaz, naruszone mogą zostać dobra prawne i istnieje domniemanie wystąpienia szkody materialnej w postaci zdarzenia drogowego"* (prawnik, użytkownik),
- w kontekście ustaleń dotyczących możliwych szkód określona zostaje możliwa przyczyna *„nieuprawniona modyfikacja danych w bazie"* (informatyk, lider) oraz zadane pytanie o możliwość obrony (lider),
- jako możliwą obronę wskazany zostaje mechanizm kont dostępu, a także implementacja podpisu cyfrowego jako środka pozwalającego na wykrywanie nieuprawnionych modyfikacji (informatyk, lider),
- całość przeprowadzonej dyskusji zostaje zaprotokołowana, a jej konkluzje zapisane formalnie w sposób przedstawiony wyżej.

Przedstawiono tu ideę metody. W opisanym przykładzie występują wszystkie etapy przewidziane metodą poza prezentacją reguł modelu. Doświadczenie przeprowadzonego badania wskazuje, że rozumienie modelu jest największym problemem dla członków zespołu. Dużo uwagi należy też poświęcić poprawnej identyfikacji szkód. Dobrany zespół okazał się za mały (cztery osoby), a w toku dyskusji dała się zauważyć swoista opozycja *lider, informatyk – prawnik, użytkownik* wynikająca z braku wiedzy o „opozycyjnych" dziedzinach.

4. Podsumowanie

W odniesieniu do przedstawionej metody, w kontekście przeprowadzonych badań, wyciągnąć można kilka ważnych wniosków. Po pierwsze, wyniki badań są tak dobre, jak dobry jest zespół ekspertów. Domniemywać można, że metoda ta powinna być stosowana przez specjalizowane podmioty audytorskie w porozumieniu z użytkownikami systemu. Drugim ważnym wnioskiem jest stwierdzenie faktu, że nie ma gwarancji, że wszystkie hazardy zostaną wykryte. Nie wiadomo bowiem, czy znalezione zostały wszystkie możliwe interpretacje słów kluczowych w kontekście badanych atrybutów. Pomocne tu są różne reprezentacje formalne - różne spojrzenia na badany system. Poddając inspekcji różne modele zwiększa się możliwości metody. Trzecie spostrzeżenie, zgodne z sugestiami standardu [9], wskazuje na potrzebę stosowania także innych metod badania bezpieczeństwa, np. FTA lub FMEA, przy czym uznać należy, że badania metodą HAZOP powinny być ich uzupełnieniem, a nie na odwrót.

LITERATURA

1. Grzywak A.: Bezpieczeństwo systemów komputerowych. Wydawnictwo Pracowni Komputerowej Jacka Skalmierskiego, Gliwice 2000.
2. Jurkowlaniec M., Nowicki B., Redmill F.: Wprowadzenie do metody HAZOP. Informatyka, 1997, nr 7-8, s. 24-29.
3. Yourdon E.: Współczesna analiza strukturalna. WNT, Warszawa 1996.
4. Polska norma PN-IEC 1078. Metoda schematów blokowych niezawodności. Polski Komitet Normalizacyjny, 1994.
5. Polska norma PN-IEC 812. Procedura analizy rodzajów i skutków uszkodzeń. Polski Komitet Normalizacyjny, 1994.
6. Polska norma PN-IEC 1025. Analiza drzewa niezdatności. Polski Komitet Normalizacyjny, 1994.
7. Rozporządzenie ministra transportu i gospodarki morskiej w sprawie wydawania uprawnień do kierowania pojazdami, Dz.U.99.58.621 zm. Dz.U.00.15.201.
8. Defence Standard 00-58 HAZOP Studies on Systems Containing Programmable Electronics Part 1 Requirements. Great Britain Ministry of Defence, 2000.
9. Defence Standard 00-58 HAZOP Studies on Systems Containing Programmable Electronics Part 2 General Application Guidance. Great Britain Ministry of Defence, 2000.

Recenzent: Dr inż. Włodzimierz Boroń

Wpłynęło do Redakcji 31 marca 2001 r.

Abstract

Computer systems security is a still growing problem. Some mathematical formal methods for analyzing software and hardware products exists as well as semi formal methods, called also semi formal documents inspections. The scope of application for these semi formal methods is analyzing big, more or less integrated systems with a wide range of functionality. HAZOP methodology is one of the examples.

HAZOP is the abbreviation for *hazard and operability* and concentrate on looking for hazards what means deviations from the desired behavior of the system. Three elements must exists for HAZOP to operate:

- team of experts
- formal model of the system
- discussion stimulated by a team leader describing every item on the model with special *guide word*

During discussion over the system (represented by a model) guide words are applied to all items on the model, reasons and consequences of indicated hazards given as well as conclusions reported.

In the article rules of HAZOP are described and a small example of the research using the method is given.