**Załącznik nr B7E – Cyberbezpieczeństwo OT– Badanie CS Hazop.**

**Program Funkcjonalno- Użytkowy**

Spis treści

[1 Ogólne informacje na temat HAZOP 4](#_Toc184200930)

[1.1 Wprowadzenie: 4](#_Toc184200931)

[1.2 Założenia metody: 4](#_Toc184200932)

[2 Wymagania odnośnie warsztatów badawczych dotyczące cyberbezpieczeństwa HAZOP. 5](#_Toc184200933)

[2.1 Warsztaty badawcze dotyczące cyberbezpieczeństwa HAZOP należy przeprowadzić w następującej kolejności: 5](#_Toc184200934)

[2.2 Wymagania co do prowadzącego warsztaty cyber HAZOP: 6](#_Toc184200935)

1. Ogólne informacje na temat HAZOP

## Wprowadzenie:

* 1. HAZOP to skrót od HAZard and OPerability study, jest to technika zarządzania ryzykiem i badania systemów.
  2. Bezpieczeństwo systemów OT 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.
  3. Cecha zasobu, która może doprowadzić do zagrożenia, nazywana jest podatnością, przy czym istnienie takiej cechy nie stanowi o pewności wystąpienia zagrożenia, ale o jego możliwości.
  4. 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. Nazywa się ją półformalną inspekcją dokumentową.
  5. Metodologia badania cyber HAZOP łączy podejścia do bezpieczeństwa procesów, kontroli procesów i cyberbezpieczeństwa. Umożliwia współpracę IT/OT, inżynierii i operacji przy użyciu metod już znanych kierownictwu operacji i personelowi obiektu.
  6. Umożliwia również identyfikację i analizę cyberzagrożeń w taki sam sposób, jak w przypadku innych ryzyk procesowych. Badanie dotyczy wszystkich obiektów przemysłowych, nie zakłóca ani nie koliduje z dobrze ugruntowanymi funkcjami bezpieczeństwa procesów i jest odrębną czynnością następczą tradycyjnego HAZOP.

## Założenia metody:

* 1. . W metodzie HAZOP zakłada się istnienie formalnej reprezentacji badanego systemu w postaci modelu zrozumiałego dla członków zespołu analitycznego.
  2. Identyfikacja możliwych hazardów polega na ich wyszukiwaniu w toku ustalonej proceduralnie dyskusji między członkami zespołu ekspertów.
  3. Dyskutowane są podatności elementów widocznych w modelu formalnym oraz związane z nimi możliwości zagrożeń, a także wydawane są zalecenia potrzebnych zmian lub dodatkowych badań.
  4. HAZOP może być stosowany na każdym z etapów w cyklu życia systemu OT, zarówno do analizy projektu, jak i działającego produktu.
  5. 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.).
  6. Zespół dyskutuje nad prawdopodobnymi hazardami w trakcie spotkań prowadzonych przez tzw. lidera. Typowe badanie systemu obejmuje kilka spotkań trwających do dwóch godzin.
  7. 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.
  8. Dopuszczonymi narzędziami do tworzenia modeli są:
     1. diagramy przepływu danych,
     2. diagramy przepływów sterowania,
     3. diagramy związków encji,
     4. diagramy przejść stanów.
  9. Wymaganą cechą reprezentacji systemu OT jest jego hierarchiczność, pozwalająca na przekrojowe spojrzenie na badany system OT.
  10. W celu wykorzystania hierarchiczności należy zastosować diagram przepływu danych równoważonych warstwowo (w górę lub w dół).

1. Wymagania odnośnie warsztatów badawczych dotyczące cyberbezpieczeństwa HAZOP.

## Warsztaty badawcze dotyczące cyberbezpieczeństwa HAZOP należy przeprowadzić w następującej kolejności:

1. . Zdefiniowanie listy systemów OT, jego podsekcje i węzły . Rozbicie poszczególnych systemów na elementy składowe (urządzania sieciowe, HMI, PLC, inne). Wybieranie granice systemów, podzielenie go na łatwe do zarządzania podsekcje i zidentyfikuj rozważane węzły.
2. Zdefiniowanie problemów będące przedmiotem zainteresowania . Określ problemy HSSE będące przedmiotem zainteresowania, które zostaną omówione w analizie. Przypisanie krytyczności do systemówOT.
3. Przypisanie oczekiwanych poziomów SL (Security Level) do systemów według normy IEC 62443.
4. Zastosowanie odchylenia dla każdego węzła . Opracowanie sensowne scenariusze zagrożeń (przyczyny/zagrożenia).
5. Przypisanie możliwych błędów mogących niekorzystnie wpłynąć na poprawne działanie funkcji systemów OT.
6. Opracowanie listy wektorów ataku, które będą rozpatrywane w analizie
7. Zbadanie konsekwencji. Zidentyfikowanie wszystkich istotnych implikacji dla każdego odstępstwa bez względu na jakiekolwiek istniejące zabezpieczenia.
8. Określenie funkcji systemów poddanych analizie. Określenie funkcji systemu względem wpływu na proces produkcji ciepła i energii.
9. Zbadanie przyczyn. Zidentyfikowanie potencjalnych podatności lub przyczyny odchyleń. Przypisanie przyczyny (wektorów ataku) do zdefiniowanych błędów systemów OT.
10. Obliczenie niełagodzonego ryzyka cyberbezpieczeństwa. Ocena prawdopodobieństwa i wpływ tego odchylenia. Określenie skutków wystąpienia poszczególnych błędów.
11. Zidentyfikowanie zabezpieczeń. Określenie najsolidniejszych zabezpieczeń przed każdą konsekwencją. Określenie zabezpieczeń, które zostaną wdrożone w ramach projektu
12. Obliczenie pozostałych ryzyk cyberbezpieczeństwa. Ponowna ocena prawdopodobieństwo i wpływ odstępstwa od istniejących zabezpieczeń.
13. Identyfikacja i zalecenie dodatkowych zabezpieczeń. Określenie innych zabezpieczeń w celu zmniejszenia ryzyka do akceptowalnego (tolerowanego) poziomu.
14. Obliczenie pozostałego ryzyka cyberbezpieczeństwa. Ponownie ocena prawdopodobieństwa i wpływu odchylenia z dodatkowymi zabezpieczeniami.
15. Przygotowanie raportu. Opracowanie listy zaleceń dotyczących zabezpieczeń systemów OT w kolejności priorytetowej.

## Wymagania co do prowadzącego warsztaty cyber HAZOP:

1. . Wymagane jest zapewnienie osoby - facylitatora, który poprowadzi warsztaty cyber HAZOP.
2. Facylitator cyber HAZOP musi posiadać wiedzę i doświadczenie w zakresie systemów IT/OT, cyberbezpieczeństwa, kontroli procesów i inżynierii bezpieczeństwa procesów.
3. Facylitator jest odpowiedzialny za przygotowanie informacji wymaganych do przeprowadzenia warsztatu i współpracę z zespołem warsztatowym w celu dostarczenia możliwie najbardziej wiarygodnej oceny ryzyka.