mgr inż. Joanna JASIŃSKA
mgr inż. Witold POKORA
Zakład Systemów Jakości i Zarządzania

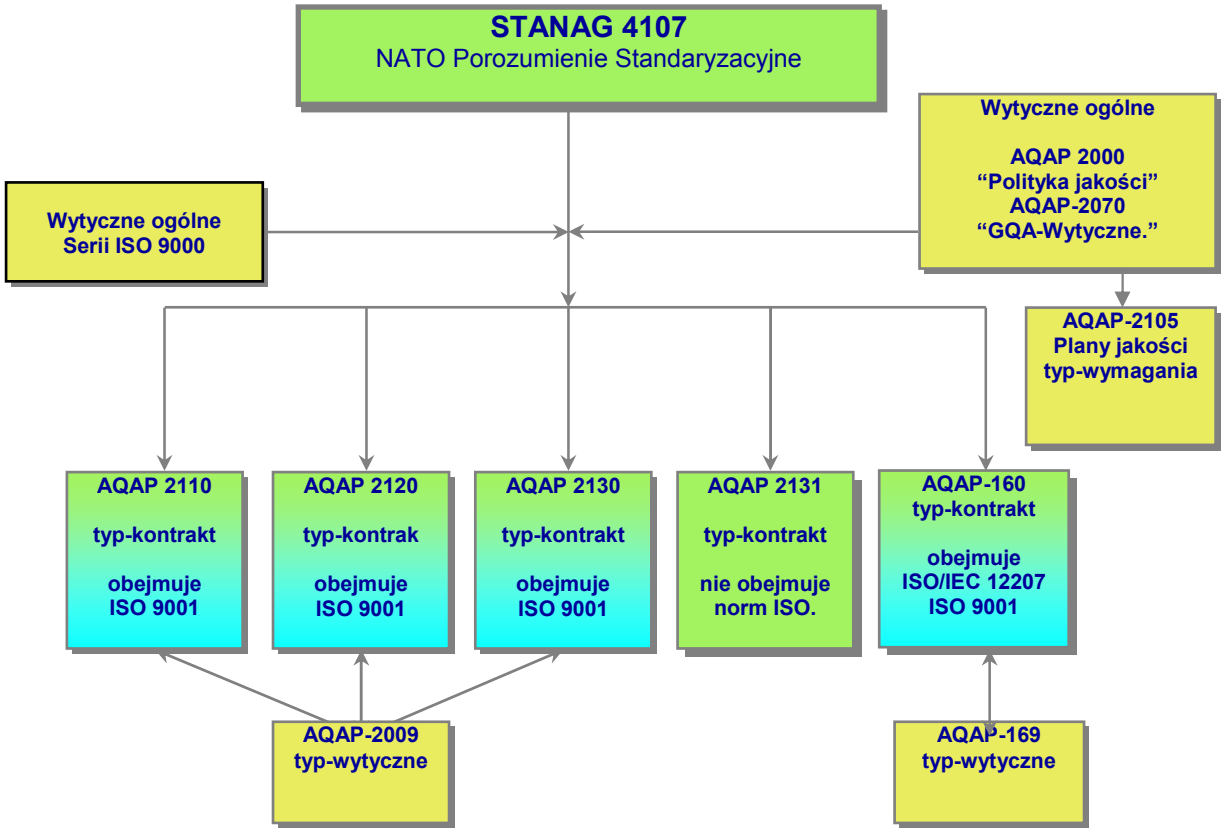
ZARZĄDZANIE RYZYKIEM I KONFIGURACJĄ W PROCESACH REALIZACJI UZBROJENIA I SPRZĘTU WOJSKOWEGO W ŚWIETLE WYMAGAŃ NATO

Zarządzanie ryzykiem i konfiguracją są to dwa elementy stanowiące główne wymagania NATO. Z naszych doświadczeń wynika, że organizacjom uczestniczącym w kontraktach dla wojska wymagania te przysparzają wiele problemów związanych ze zrozumieniem i wdrożeniem. W poniższym referacie przedstawiono interpretację ww. wymagań.

Ze względu na strategiczne zadania, NATO jest organizacją tworzącą różnorodny i specyficzny rynek. Stąd wymagania jakościowe, stawiane dostawcom uzbrojenia i sprzętu wojskowego (UiSW) dla wojska są jednoznacznie określone. Wojsko potrzebuje wyrobów prostych, używanych do codziennego funkcjonowania, jak również zaawansowanego technologicznie sprzętu i uzbrojenia. Z punktu widzenia dostawców różnych branż, jest to rynek ogromny, stabilny i przewidywalny w swoich działaniach. Dlatego przed polskim przemysłem obronnym otwiera się szansa uczestniczenia w międzynarodowych kontraktach, jednak pod warunkiem elastycznego i skutecznego dostosowania się do wymagań NATO.

W świetle wymagań polityki jakości NATO określonej w dokumencie standaryzacyjnym AQAP 2000: 2003, w ciągu całego cyklu życia UiSW odpowiedzialność za jego jakość ponoszą zarówno wykonawcy, zamawiający, jak i użytkownicy. Efektywność i skuteczność realizowanego kontraktu zależy od współpracy wszystkich zainteresowanych stron, a przede wszystkim od skuteczności planowania, sterowania i monitorowania funkcjonujących procesów. Trudności w komunikacji między stronami kontraktu mogą negatywnie wpływać w na jakość a także powodować istnienie istotnych zakłóceń w realizacji kontraktu. Ma to szczególne znaczenie w przypadku złożoności i skomplikowania technologii UiSW. W związku z tym konieczne jest zapewnienie spełnienia wymagań klienta przez cały proces realizacji UiSW, począwszy od fazy projektowania a skończywszy na kasacji.

W celu ujednolicenia i sprecyzowania wymagań dla organizacji realizujących dostawy wyrobów obronnych, w tym UiSW, został ustanowiony STANAG 4107 - porozumienie standaryzacyjne NATO, ratyfikowane przez państwa członkowskie NATO, w tym Polskę. Porozumienie to określa zasady nadzorowania realizowanych kontraktów w kierunku zapewnienia jakości dostaw wyrobów będących przedmiotem umów międzynarodowych w ramach procesu Rządowego Zapewniania Jakości (GQA). STANAG 4107 wprowadza też wymagania dotyczące zapewnia jakości dla organizacji realizujących dostawy dla wojska poprzez odpowiednie publikacje standaryzacyjne zapewnienia jakości AQAP. Poniżej przedstawiono strukturę AQAP serii 2000.



Wyróżnia się dwa typy dokumentów AQAP: „wytyczne" i „kontrakt". Pierwszy z wymienionych służy jako pomoc we wdrożeniu i ocenie sytemu zapewnienia jakości w organizacji, stanowi rozwinięcie i komentarz do wymagań. Drugi typ AQAP określa wymagania, jakie musi spełniać organizacja realizująca kontrakt dla wojska.

Wybór odpowiedniego AQAPu (typu kontrakt) przez organizację zobowiązuje do dostarczenia obiektywnego dowodu potwierdzającego spełnienie zawartych w nim wymagań. Podstawowymi kryteriami jest zakres sytemu zapewnienia jakości a także wymagania określone przez zamawiającego w kontrakcie. Organizacja deklarując posiadanie systemu według AQAP 2110:2003 musi wykazać zgodność sytemu zapewnienia jakości w procesie projektowania, pracach rozwojowych i produkcji. Natomiast w przypadku AQAP 2120: 2003 wymaga się udokumentowania systemu zapewnienia jakości tylko w produkcji. AQAP 2130 stosuje się w sytuacji, gdy konieczne staje się potwierdzenie zgodności wyrobu w fazie kontroli podczas procesów realizacji, UiSW, jego części, komponentów, podzespołów oraz wyrobu finalnego. Potwierdzenie zgodności UiSW z wymaganiami po otrzymaniu wyrobu gotowego wymagane jest w AQAP 2131:2003. AQAP 160 określa wymagania zapewnienia jakości dotyczące dostaw oprogramowania. Jeden z ww. AQAP powinien być wtedy określany jako wymaganie kontraktowe.

Publikacje standaryzacyjne AQAP zostały przygotowane w celu określania wymagań kontraktowych, które ma spełnić dostawca w oparciu o funkcjonujący w organizacji system zarządzania jakością. Dotyczy to takich publikacji takich, jak: AQAP 2110, AQAP 2120, AQAP 2130.

Zarządzanie jakością z uwzględnieniem wymagań AQAP ma na celu dostarczenie odbiorcy obiektywnego dowodu, że UiSW będzie w satysfakcjonujący sposób spełniać zdefiniowane w kontrakcie wymagania. Głównym zadaniem takiego systemu jest udzielenie odbiorcy/użytkownikowi UiSW zapewnienia, że wyrób w poszczególnych fazach cyklu życia będzie osiągał zakładane parametry taktyczno-

techniczne, technologiczne, itp., co może być sprawdzane w procesie rządowego zapewnienia jakości GQA.

Organizacja realizująca kontrakt z wymaganiami typu AQAP musi spełniać kilka wymagań:

- wdrożenie i utrzymywanie systemu zarządzania jakością zgodnego z normą ISO 9001: 2000,
- stosowanie zasad zarządzania ryzykiem i konfiguracją,
- tworzenie planów jakości i planów zarządzania konfiguracją,
- ocena efektywności systemu jakości oraz takich elementów, jak niezawodność i podatność obsługowa,
- poddanie się procesowi GQA.

W niniejszym referacie skupiono się na dwóch zasadniczych elementach AQAP, jakimi są: zarządzanie ryzykiem i konfiguracją w procesie realizacji UiSW.

Zarządzanie ryzykiem

Wymagania dla dostawców UiSW, dotyczące zarządzania ryzykiem w AQAP zostały określone pkt 5.4 „Planowanie" oraz w pkt 7.4 „Zakupy". W szczegółowym rozwinięciu, wśród podstawowych wymagań AQAP w tym zakresie, należy wymienić:

- określanie ryzyka związanego z kontraktem,
- opracowywanie planów zarządzania ryzykiem,
- wprowadzanie działań zapobiegawczych w celu redukowania ryzyka,
- ustanawianie i utrzymywanie bazy danych dotyczącej zarządzania ryzykiem,
- wprowadzanie zaplanowanych działań na etapie realizacji UiSW,
- dostarczanie Przedstawicielowi Zapewnienia Jakości (QAR) informacji dotyczących ryzyka związanego z wyrobem, procesem lub organizacją,
- wykorzystywanie informacji zwrotnej o ryzyku na zakończenie realizacji.

Zarządzanie ryzykiem powinno być elementem funkcjonującego systemu zarządzania jakością w organizacji i odzwierciedlać rzeczywiste działania nie tylko w stosunku do umów realizowanych w ramach procesu GQA ale też innych umów realizowanych w organizacji. Bez zarządzania ryzykiem nie można mówić o skutecznym zarządzaniu procesami.

Aby jednak działania w zakresie zarządzania ryzykiem były skuteczne (wdrożone, utrzymane i doskonalone), zarządzanie ryzykiem należy potraktować jako proces ciągły, wymagający zbierania danych, analizy i oceny ryzyka w całym procesie realizacji kontraktu.

W rozumieniu podejścia systemowego organizacja powinna wyznaczyć osoby odpowiedzialne za proces zarządzania ryzykiem oraz zapewnić kompetentny i wykwalifikowany personel biorący udział w tym procesie. Ważnym krokiem jest określenie jednoznacznych zasad dotyczących zarządzania ryzykiem w dokumentacji, np. procedurze, instrukcji czy też rozdziale Księgi Jakości.

Zgodnie z wymaganiami AQAP organizacja powinna identyfikować ryzyko już na etapie przeglądu umowy. Ryzyko powinno być też w odpowiednim czasie uaktualniane.

Planowanie działań związanych z ryzykiem powinno obejmować (ale też nie ograniczać się): identyfikację ryzyka i jego analizę, redukowanie i monitorowanie ryzyka. W planowaniu należy jeszcze uwzględnić takie elementy, jak:

- działania w celu zarządzania nie akceptowalnym ryzykiem,

- redukowanie, eliminowanie lub transfer ryzyka do innych obszarów,
- działania w przypadku wystąpienia nieprzewidzianych sytuacji (kiedy wystąpi specyficzny rodzaj ryzyka),
- środki zarządzania, jakie będą stosowane, żeby powstrzymać nie akceptowalne ryzyko,
- zakres realizacji procesu GQA.

Organizacja powinna przedstawić obiektywny dowód w postaci udokumentowania opisu działań redukujących zidentyfikowane ryzyko, sposobu monitorowania ryzyka, zakresu odpowiedzialności i uprawnień wyznaczonych osób, a także terminy wykonania i oceny skuteczności podjętych działań. Powyższe działania mogą być udokumentowane np. w planie jakości, planie zarządzania ryzykiem lub mogą stanowić odrębny dokument związany z realizacją umowy.

Plan zarządzania ryzykiem powinien pozwalać na pewną elastyczność w podejmowaniu decyzji w związku z tym, że oszacowane ryzyko może nigdy nie wystąpić. Model tradycyjnego zarządzania polegał na reagowaniu na już zaistniałe zdarzenie, obecnie preferuje się elastyczne sterowanie zasobami na monitorowanie i redukowania ryzyka, co zapewnia bardziej racjonalne działania.

Aby właściwie zarządzać ryzykiem konieczne jest zrozumienie, co kryje się pod pojęciem ryzyka i zarządzania ryzykiem. Ryzyko stanowi bowiem iloczyn **prawdopodobieństwa** wystąpienia **zagrożenia** oraz **skutku** oddziaływania tego zagrożenia.

Zarządzanie ryzykiem jest to proces, ustanowiony w celu zabezpieczenia przed skutkami niepożądanego zjawiska i minimalizowania ryzyka. Zarządzanie ryzykiem jest nierozłącznie związane z podejmowaniem decyzji. Odpowiedzialny za realizację umowy rzadko może pozwolić sobie na komfort zadecydowania w sytuacji całkowitej pewności o podjęciu się realizacji kontraktu i przewidzeniu przyszłych skutków. W większości przypadków konieczne jest założenie pewnego prawdopodobieństwa wystąpienia czynników zakłócających i wspomagających realizację kontraktu. Z tego punktu widzenia decyzje dzielimy na:

- podejmowane w warunkach pewności, gdy dysponujemy wszystkimi potrzebnymi informacjami,
- podejmowane w warunkach niepewności, gdy nie wiemy nic o przyszłych warunkach realizacji kontraktu i otoczenia ,
- podejmowane w warunkach ryzyka, gdy możemy ocenić negatywne skutki zagrożeń i prawdopodobieństwo wystąpienia tych zagrożeń.

W zarządzaniu ryzykiem wyróżnia dwa zasadnicze etapy:

- szacowanie ryzyka
- sterowanie ryzykiem.

Szacowanie ryzyka prowadzi się dla wyrobów UiSW o istotnym znaczeniu lub wyrobów złożonych (technicznie skomplikowanych), jeżeli występuje znaczne ryzyko, lub jeżeli ryzyko nie może być w łatwy sposób określone. Szacowanie ryzyka składa się z:

- identyfikacji ryzyka,
- analizy ryzyka.

Celem **identyfikacji ryzyka** jest określenie obszaru występowania ryzyka dotyczącego danego przedsięwzięcia z oszacowaniem prawdopodobieństwa jego wystąpienia oraz próby umiejscowienia i zaklasyfikowania go pod kątem przyczyn, wzajemnych relacji, wspólnych właściwości lub trendów, częstotliwości występowania czy też skutków. Potencjalne ryzyko może być określane na podstawie:

- analizy danych pochodzących z przeglądu kontraktu,
- przeglądu dokumentacji z uwzględnieniem zmian,
- analizy wniosków z poprzednio realizowanych podobnych kontraktów,
- narady typu „burza mózgów”,
- analizy danych pochodzących od QAR oraz od specjalistów innych dziedzin, np. informatyki, logistyki,
- danych pochodzących z działu odpowiedzialnego za finansowanie realizowanego kontraktu,
- danych pochodzących od dostawcy (obejmują głównie identyfikację ryzyka związanego z dostawcami uczestniczącymi w realizacji kontraktu).

Identyfikację ryzyka można przeprowadzać w stosunku do:

- procesu,
- wyrobu,
- dostawcy,

Metody identyfikacji ryzyka w znacznej mierze zależą od rodzaju i charakteru działalności firmy, a także od specyfiki kontraktu czy też wyrobu. W dokumentach normalizacyjnych NATO zaleca się stosowanie takich metod oceny ryzyka, jak:

- metoda wstępnej analizy zagrożeń (PHA – Preliminary Hazard Analysis),
- metoda „co-gdy” (WI – What - If),
- metoda systematycznej analizy ryzyka (MOSAR - Method Organized for Systematic Analysis of Risk),
- analiza drzewa błędów (FTA – Fault Tree Analysis).

Analiza ryzyka polega na przeprowadzeniu klasyfikacji ryzyka przy zastosowaniu metody:

- **bezwymiarowej** - opisowej dzielącej ryzyko na akceptowalne i nie akceptowalne,
- **ilościowej** – określającej wymierne wartości iloczynu skutku niepożądanego ryzyka oraz prawdopodobieństwa wystąpienia (np. analiza kosztów, metody statystyczne),
- **kombinowanej** – łączącej metodę bezwymiarową z ilościową.

Organizacja powinna określić znaczenie i wagę każdego zidentyfikowanego ryzyka w kontekście możliwości zrealizowania kontraktu.

Metody ilościowe oceny ryzyka są szczególnie zalecane, jeżeli przewidywane skutki ryzyka są duże. Jednak wykorzystywanie metod i technik ilościowych jest niejednokrotnie ograniczone możliwością uzyskania użytecznych danych. Dlatego w wielu zastosowaniach możliwa jest tylko jakościowa ocena ryzyka.

Zarządzający ryzykiem powinien zdecydować, które rodzaje ryzyka są akceptowalne lub nie, w odniesieniu do negatywnego skutku wystąpienia ryzyka w następujących aspektach:

- jakość wyrobu (np. niespełnienie wymagań dotyczących wymaganych parametrów),
- bezpieczeństwo użytkowania,
- harmonogram realizacji (np. opóźnienie realizacji kontraktu),
- koszty (np. zwiększenie kosztów realizacji kontraktu lub kosztów eksploatacji w cyklu życia wyrobu).

Po oszacowaniu każdego rodzaju ryzyka następuje oszacowanie sumy wszystkich rodzajów ryzyka (ryzyko całkowite). Niezbędne jest także wyznaczenie priorytetów ryzyka. Dzięki priorytetyzacji można zidentyfikować nowe obszary ryzyka, które poprzednio nie były uwzględniane oraz można wskazać najlepszy sposób zarządzania ryzykiem.

Po identyfikacji i analizie ryzyka konieczne staje się *planowanie, redukowanie i monitorowanie ryzyka,* co określono wspólnym mianem ***sterowania ryzykiem.***

Planowanie zarządzania ryzykiem opiera się przede wszystkim na stworzeniu planu, który powinien obejmować określenie takich elementów, jak:

- przyczyny ryzyka i ich hierarchię (priorytety),
- działanie, jakie należy podjąć w celu wyeliminowania lub zredukowania ryzyka do poziomu akceptowalnego,
- metody jakimi należy wyeliminować lub zredukować ryzyko,
- osoby odpowiedzialne za zarządzanie ryzykiem,
- środki niezbędne do zarządzania ryzykiem,
- harmonogram działań,
- planowanie działania w przypadku wystąpienia nieprzewidzianych sytuacji, kiedy wystąpi specyficzny rodzaj ryzyka.

Kolejnym etapem po zaplanowaniu działań związanych z ryzykiem jest **monitorowanie ryzyka,** poprzez:

- sprawdzanie stopnia realizacji zaleceń i wniosków,
- identyfikację i szacowanie każdego nowego pojawiającego się rodzaju ryzyka ,
- ocenianie skuteczności zaleceń,
- opracowywanie nowych zaleceń i wniosków jeżeli aktualnie obowiązujące są uważane za nieefektywne.

Organizacja powinna ustalić sposoby monitorowania ryzyka oraz utrzymywać zapisy z monitorowania ryzyka.

Ważnym elementem w sterowaniu ryzykiem jest określenie zasad postępowania oraz metod **redukowania ryzyka** zarówno zidentyfikowanego jak i nieoszacowanego. Istotnym jest udokumentowanie i ocena skuteczności przeprowadzonych działań redukujących ryzyko.

Zarządzanie konfiguracją

Zarządzanie konfiguracją ma zastosowanie przede wszystkim w przedsięwzięciach, dla których wymagane jest zapewnienie ciągłej koordynacji powstających rozwiązań technicznych. Wymaganie takie może wynikać przede wszystkim z obowiązujących w danej branży przepisów prawnych jak również z potrzeby dysponowania wiedzą o aktualnej konfiguracji realizowanych wyrobów. Biorąc pod uwagę charakter wyrobu jakim jest UiSW zarządzanie konfiguracją jest istotne z punktu widzenia obydwu ww. aspektów.

Z punktu widzenia NATO należy wziąć również pod uwagę aspekt zapewnienia spójności rozwiązań w czasie realizacji wielonarodowych projektów UiSW zarówno w czasie projektowania, produkcji, jak i eksploatacji. W przypadku NATO zarządzanie konfiguracją należy rozpatrywać w dwóch płaszczyznach. Pierwsza płaszczyzna to stosowanie wymagań AQAP w ramach realizacji procesu Rządowego Zapewnienia Jakości GQA, natomiast druga płaszczyzna to uczestnictwo w realizacji wielonarodowych przedsięwzięć NATO.

Do zarządzania konfiguracją zgodnie z wymaganiami NATO wykorzystywany jest STANAG 4159 przywołany w publikacjach standaryzacyjnych AQAP.

Wymagania STANAG 4159, a w szczególności przywołane w nim publikacje standaryzacyjne ACMP są zbieżne z międzynarodowymi wytycznymi zawartymi w PN ISO 10007 : 1988. STANAG 4159 wprowadza następujące publikacje ACMP:

ACMP-1, którego, celem jest ustanowienie jednolitych zasad planowania zarządzania konfiguracją UiSW.
ACMP-2, który zawiera wymagania dotyczące identyfikacji obiektów konfiguracji, konfiguracji odniesienia oraz zasad identyfikacji wszystkich egzemplarzy sprzętu (podzespołów sprzętu) objętych zarządzaniem konfiguracją CM.
ACMP-3, który zawiera wymagania dotyczące zasad wprowadzania zmian i odstępstw do zatwierdzonej konfiguracji.
ACMP-4, który zawiera wymagania dotyczące rejestrowania i zapisywania danych określających status konfiguracji wszystkich zidentyfikowanych obiektów konfiguracji.
ACMP-5, który zawiera wymagania dotyczące zasad realizacji auditów konfiguracji.
ACMP-6, który zawiera definicje i terminy z dziedziny zarządzania konfiguracją.
ACMP-7, który rady do stosowania ww. ACMP.

Zgodnie z wymaganiami AQAP, zarządzanie konfiguracją odnosi się do przedmiotu zamówienia, czyli wyrobu określonego w umowie. Należy zauważyć, że przedmiotem zamówienia jest przede wszystkim przedmiot materialny, tj. uzbrojenie i sprzęt wojskowy, a także zastosowane materiały przetworzone, tj. produkty naftowe, wytwór intelektualny, tj. oprogramowanie oraz usługi, tj. badania czy naprawy.

Aby zapewnić właściwą konfiguracje realizowanego UiSW w AQAP 2110: 2003, AQAP 2120: 2003 i AQAP 2130: 2003 wprowadzono wymaganie opracowania przez dostawcę dla wojska procedur zarządzania konfiguracją. Zgodnie z AQAP 2110: 2003, który obejmuje projektowanie, rozwój i produkcję, zarządzanie konfiguracją dotyczy czterech obszarów:

- identyfikacji konfiguracji,
- sterowania konfiguracją,
- charakteryzowania statusu konfiguracji,
- auditów konfiguracji.

Zgodnie z AQAP 2120: 2003 odnoszącego się do produkcji i AQAP 2130: 2003 odnoszącego się do dostarczania wyrobów gotowych, zarządzanie konfiguracją ograniczone jest do identyfikacji konfiguracji oraz sterowania konfiguracją.

Zakres identyfikacji konfiguracji czy sterowania konfiguracją jest różny w zależności od rodzaju AQAP. Im wyższy numer AQAP tym zakresy te są bardziej ograniczone.

W AQAP 2110: 2003 oraz AQAP 2120: 2003 wymagane jest dodatkowo opracowanie planu zarządzania konfiguracją.
Udokumentowana procedura zarządzania konfiguracją powinna określać opis działań, tj.:

- zapewnienie odpowiedzialności za zarządzanie konfiguracją, z uwzględnieniem:
- wzajemnych powiązań pomiędzy działaniami związanymi z zarządzaniem konfiguracją,
- zainteresowanych stron w organizacji i poza nią, które mogą brać dział w zarządzaniu konfiguracją,
- identyfikacja konfiguracji, w tym :
- opis realizowanego wyrobu UiSW z uwzględnieniem typowych cech funkcjonalnych i fizycznych,
- mające zastosowanie fazy cyklu życia UiSW oferowanego przez organizację,
- określenie typowych obiektów konfiguracji i konfiguracji odniesienia,
- zasady numerowania z przywołaniem niezbędnych procedur,

- sterowanie konfiguracją z uwzględnieniem poszczególnych etapów realizacji UiSW,
- charakteryzowanie statusu konfiguracji, które może być uwzględnione w ramach opisu identyfikacji, sterowania czy auditowania konfiguracji,
- auditowanie konfiguracji, w tym określenie zasad ich przeprowadzania,
- planowanie zarządzania konfiguracją.

Identyfikacja konfiguracji

Do istotnych elementów identyfikacji konfiguracji należy określenie struktury UiSW. Powinna ona być określona poprzez dekompozycję z uwzględnieniem podziału na: układy, instalacje, zespoły, podzespoły, urządzenia, agregaty, detale, czy części.

Na podstawie właściwej struktury UiSW możliwe jest dokonanie wyboru obiektów konfiguracji. Obiekty konfiguracji rozumiane są jako połączenie przedmiotu materialnego, wytworu intelektualnego, wyrobów wytwarzanych w procesach ciągłych, możliwych do samodzielnego zarządzania konfiguracją. Dokonanie właściwego wyboru obiektów pozwala na sprawne zarządzanie konfiguracją. Obiekty konfiguracji powinny być ustalane według określonych kryteriów wyboru. Kryteria wyboru obiektów konfiguracji określane są przede wszystkim w umowie, ale mogą także wynikać z zastosowania UiSW. Do podstawowych kryteriów można zaliczyć :

- bezpieczeństwo użytkowania - obiektami konfiguracji powinny być wszystkie elementy składające się na UiSW mające wpływ na bezpieczeństwo,
- niezawodność – obiektami konfiguracji powinny być te elementy UiSW, które wpływają na takie cechy, jak nieuszkadzalność czy trwałość,
- ryzyko zastosowania – obiektami konfiguracji powinny być elementy zidentyfikowane w trakcie szacowania ryzyka jako mające istotny wpływ na zastosowanie,
- aspekty logistyczne – podział na obiekty powinien zapewnić właściwą zamienność czy podatność obsługowo-naprawczą.

Ponadto identyfikacja konfiguracji obejmuje określenie typów dokumentacji konfiguracyjnej wymaganej dla każdego obiektu konfiguracji, niepowtarzalnych numerów i innych identyfikatorów przyporządkowanych do określonych obiektów konfiguracji oraz do dokumentacji konfiguracyjnej.

Szczegółowe opisanie UiSW w specyfikacjach technicznych i w dokumentacji projektowej zarówno od strony fizycznej (wymiary, dokładność wykonania, skład materiałowy), jak i funkcjonalnej (cechy użyteczności, logistyczne, podatności, ergonomiczności, odporności, zdolność poruszania się po terenie) oraz nadzorowanie wprowadzania zmian tworzy zbiór dokumentów, nazywany konfiguracjami odniesienia.

Ustanowienie konfiguracji odniesienia do zarządzania konfiguracją wymaga realizacji formalnej procedury według następujących kroków:

- dostawca przedstawia opracowaną dokumentację dla odbiorcy, a odbiorca i dostawca wspólnie prowadzą analizę techniczną;
- po analizie technicznej dostawca wprowadza konieczne zmiany;
- odbiorca zatwierdza i wprowadza do użytku dokumentację konfiguracyjną jako obowiązującą funkcjonalną konfigurację odniesienia;
- zatwierdzona konfiguracja odniesienia stanowi swoistą część wymagań umowy.

Konfiguracja powinna być opisana do najniższego poziomu wymaganej szczegółowości tak, aby spełnić warunki określone dla danego przedsięwzięcia z uwzględnieniem możliwości wielokrotnego użycia, podatności technologicznej i produkcyjnej, wymogów bezpieczeństwa i jakości, niezawodności, podatności

obsługowo-naprawczej, odporności na oddziaływanie środków bojowych przeciwnika, zamienności części i podzespołów oraz interoperacyjności.

Sterowanie konfiguracją

Sterowanie konfiguracją służy do zapewnienia, że w zatwierdzonej dokumentacji konfiguracji nie wprowadzano nieautoryzowanych zmian. System sterowania konfiguracją ma zapewnić, że nie będą występowały problemy logistyczne, interoperacyjne oraz związane z odtwarzaniem zdolności technicznej UiSW.

Sterowanie konfiguracją może dotyczyć obiektów konfiguracji w odniesieniu do propozycji zmian wygenerowanych z takich źródeł jak : od klienta, od dostawcy, od organizacji.

Procedura sterowania konfiguracją powinna zawierać zasady przygotowania i tryb składania wniosków: propozycji zmiany, o zgody na odstępstwo przed realizacją, o zgodę na odstępstwo po realizacji.

Charakteryzowanie statusu konfiguracji

Charakteryzowanie statusu konfiguracji jest formalnym zapisywaniem i rejestrowaniem dokumentów. Forma zapisywania i rejestrowania może być uzgodniona z klientem lub wykonawcami innych obiektów konfiguracji.

Wszystkie dokumenty i zapisy wykorzystywane w zarządzaniu konfiguracją powinny uwzględniać m.in. :

- numer identyfikacyjny, nazwę, datę wejścia w życie, status wydania, status zmian, historię zmian,
- jednoznaczne oznaczenie zakończenia dokumentów,
- numery części, status projektowania i lub obiektów konfiguracji UiSW,
- status wydania informacji o konfiguracji UiSW lub obiektach konfiguracji,
- wdrażane zmiany.

Do charakteryzowania statusu konfiguracji niezbędne jest prowadzenie :

- listy dokumentów określających niezbędne konfiguracje odniesienia,
- listy obiektów konfiguracji i ich konfiguracje odniesienia,
- rejestrów zmian określające szczegóły aktualnego statusu zmian,
- rejestrów zezwoleń i/lub odstępstw,
- wykazów dostarczanych i utrzymywanych wyrobów i ich statusu zmian, oraz sporządzanie sprawozdań z auditów konfiguracji.

Auditowanie konfiguracji

Celem auditów konfiguracji jest formalne sprawdzenie potwierdzenia zgodności UiSW z charakterystykami funkcjonalnymi i/lub fizycznymi wyrobów. Audity konfiguracji powinny być zaplanowane w ramach realizowanego przedsięwzięcia. Nie zastępują one weryfikacji, przeglądu, badań i kontroli, ale dotyczą rezultatów tych działań.

Organizacja powinna rozróżnić dwa typy auditów konfiguracji:

- audit konfiguracji funkcjonalnej, który jest formalną oceną uzyskania przez UiSW lub obiekt konfiguracji określonych cech funkcjonalnych,
- audit konfiguracji fizycznej, który jest formalną oceną tego, czy wyrób lub obiekt konfiguracji uzyskał wyspecyfikowane cechy fizyczne.

Audity konfiguracji powinny być wykonane przed formalnym zatwierdzeniem wyrobu lub obiektu konfiguracji i mogą być połączone, jako audity konfiguracji funkcjonalnej i fizycznej.

Planowanie zarządzania konfiguracją

Planowanie zarządzania konfiguracją powinno być udokumentowane w postaci „Planu zarządzania konfiguracją” lub „Planu jakości”, który będzie zawierał elementy

zarządzania konfiguracją lub w inny sposób. Dla każdej umowy powinien być przygotowywany jeden plan zarządzania konfiguracją. Plan może być podzielony na kilka powiązanych ze sobą planów składowych dla specyficznych obiektów konfiguracji.

W planie powinny być uwzględnione przede wszystkim specyficzne działania wynikające z realizowanego przedsięwzięcia. Pozostałe działania powinny być opisane poprzez przywołanie procedury zarządzania konfiguracją.

Podsumowanie

Zarówno zarządzanie konfiguracją jak i zarządzanie ryzykiem to dwie dziedziny zależne od siebie i mające istotny wpływ na realizację przedsięwzięć. Zarządzanie ryzykiem przede wszystkim ma odpowiedzieć na pytanie, jakie są zagrożenia realizacyjne, w tym zagrożenia związane z osiąganiem i utrzymywaniem konfiguracji UiSW. Jeżeli występuje takie zagrożenie, niezbędnym jest zastosowanie odpowiednich procedur zarządzania konfiguracją.

Biorąc pod uwagę, że zarządzanie ryzykiem powinno być procesem ciągłym, w ramach sterowania ryzykiem podczas całego procesu realizacyjnego, szczególnie w czasie projektowania, istotne jest rozpatrywanie ryzyka związanego z osiąganiem cech funkcjonalnych i fizycznych poszczególnych obiektów konfiguracji.

Jednoznacznie należy podkreślić, że obie dziedziny muszą mieć odpowiednie zastosowanie w realizacji uzbrojenia i sprzętu wojskowego.

Literatura:

ACMP – 1 - „Wymagania NATO do przygotowania Planów Zarządzania Konfiguracją”
ACMP – 2 - „Wymagania NATO dotyczące identyfikacji konfiguracji”
ACMP – 3 - „Wymagania NATO dotyczące Sterowania Konfiguracją – Zmiany, Zgoda na odstępstwo przed realizacją oraz Zgoda na odstępstwo po realizacji”
ACMP – 4 - „Wymagania NATO dotyczące charakteryzowania statusu konfiguracji”
ACMP – 5 - „Wymagania NATO dotyczące auditów konfiguracji”
ACMP – 6 - „Zarządzanie konfiguracją NATO - Definicje i podstawowe określenia”
ACMP – 7 - „Zarządzanie konfiguracją NATO - Poradnik dotyczący stosowania ACMP od 01 do numeru 6”
AQAP 2000 – Polityka NATO dotycząca zintegrowanego systemowego podejścia do jakości w cyklu życia.
AQAP 2009 – Wytyczne NATO do stosowania AQAP serii 2000.
AQAP 2050 – Metodologia NATO dotycząca oceny przedsięwzięcia.
AQAP 2070 – Proces NATO dotyczący wzajemnej realizacji Rządowego Zapewnienia Jakości GQA
AQAP 2131 – Wymagania NATO dotyczące zapewnienia jakości w kontroli końcowej.
AQAP 2130 – Wymagania NATO dotyczące zapewnienia jakości w kontroli i badaniach.
AQAP 2120 – Wymagania NATO dotyczące zapewnienia jakości w produkcji.
AQAP 2110 – Wymagania NATO dotyczące zapewnienia jakości w projektowaniu, pracach rozwojowych i produkcji.
AQAP 2105 – Wymagania NATO dotyczące planów jakości dla wyrobu objętego

umową.