ÚŘAD PRO CIVILNÍ LETECTVÍ

Směrnice SP

Metodický materiál

K PROKAZOVÁNÍ ZAJIŠTĚNÍ BEZPEČNOSTI SW

CAA/S-SP-002-2/2016

Č. j.: 1809-16-701

Verze: 3

Datum účinnosti: 2. 1. 2020

V Praze dne: 6. 12. 2019

Schválil (podpis):

Ing. Vítězslav Hezký

ředitel Sekce provozní

Záměrně nepoužito.

Historie změn dokumentu

ČÍSLO VERZE	DATUM ZPRACOVÁNÍ	ZPRACOVAL	CHARAKTERISTIKA	POZNÁMKA
1	18. 2. 2016	OLZ	Nové vydání dokumentu	
2	15. 6. 2016	OLZ	Odstraněny odkazyna kapitoly normy ISO/IEC 12207; úprava tabulky; úpravy odkazů na tabulky; zapracování připomínek.	
3	3. 12. 2019	OI	Zapracování PNK (EU) 2017/373 ve smyslu Rozhodnutí výk. ředitele EASA „ED Decision 2019/022/R“ ze dne 29.10.2019	

Záměrně nepoužito.

ÚVODNÍ USTANOVENÍ

Dokument vychází z potřeby stanovit soubor aktivit, které by bylo možno využít pro naplnění požadavků Prováděcího nařízení Komise (EU) 2017/373 ze dne 1. března 2017, kterým se stanoví společné požadavky na poskytovatele služeb v oblasti uspořádání letového provozu / letových navigačních služeb a jiných funkcí sítě uspořádání letového provozu a dohled nad nimi, zrušují nařízení (ES) č. 482/2008, prováděcí nařízení (EU) č. 1034/2011, (EU) č. 1035/2011 a (EU) 2016/1377 a mění nařízení (EU) č. 677/2011, a to v oblasti prokazování bezpečnosti SW, který nedílnou součástí tzv. funkčního systému ANSP.

Obsah tohoto dokumentu je využitelný pro potřeby ANSP a jejich dodavatelů SW, jako návod pro stanovení cílů, jichž má být dosaženo pomocí definovaných kritérií pro jednotlivé úrovně zajištění bezpečnosti SW.

Dokument byl vypracován na základě Rozhodnutí výkonného ředitele EASA „ED Decision 2019/022/R“ ze dne 29.10.2019, ve shodě s ustanovením normy ED-153 „Guidelines for ANS Software Safety Assurance“.

Stejně jako požadavky normy ED-153, ani požadavky v tomto dokumentu uváděné, nejsou pro žádný dotčený subjekt mandatorní, pokud jejich plnění není deklarováno v interních dokumentech subjektu. Dokument nabývá účinnosti v souladu s údaji uvedenými ve schvalovací doložce uvedené na jeho čelní straně.

Záměrně nepoužito.

Záměrně nepoužito.

OBSAH

Záměrně nepoužito.

SEZNAM POUŽITÝCH ZKRATEK

[Zkratka]	[Význam zkratky český]	[Význam zkratky anglický]
ANS	Letové navigační služby	Air Navigation Service
ANSP	Poskytovatel letových navigačních služeb	Air Navigation Service Provider
ATM	Uspořádání letového provozu	Air Traffic Management
COTS	Zkratka pro výrobky, které jsou typizované a připravené k prodeji tak, jak jsou.	Commercial off-the-shelf
CMMI	Stupňovitý model zralosti (model kvality organizace práce určený pro vývojové týmy)	Capability Maturity Model Integration
CNS	Komunikace, navigace, přehled	Communication, Navigation, Surveillance
ED	Dokumenty EUROCAE	EUROCAE Documents
EUROCAE	Evropská organizace pro civilní letecké vybavení	European Organisation for Civil Aviation Equipment
FAT	Akceptační testy u výrobce	Factory Acceptance Test
FHA	Posouzení nebezpečí na úrovni funkčnosti systému *Pozn.: Jedná se o specifický přístup k PHA v souladu s EUROCONTROL SAM.*	Functional Hazard Assessment
HMI	Rozhraní člověk - stroj	Human Machine Interface
HW	Fyzické vybavení	Hardware
IEC	Mezinárodní elektrotechnická komise	International Electrotechnical Commission
ISO	Mezinárodní organizace pro normalizaci	International Organization for Standardization
NSA	Vnitrostátní dozorový orgán (v ČR určené funkce vykonává ÚCL)	National Supervisory Authority
PHA	Předběžné posouzení nebezpečí	Preliminary Hazard Analysis
PNK	Prováděcí nařízení komise	Commission Implementing Regulation
PSSA	Předběžné posouzení bezpečnosti systému *Pozn.: V souladu s EUROCONTROL SAM.*	Preliminary System Safety Assessment
SAM	Metody a techniky posouzení provozní bezpečnosti změn funkčních systémů definované EUROCONTROL	Safety Assessment Methodology
SAT	Akceptační testy u provozovatele	Site Acceptance Test

[Zkratka]	[Význam zkratky český]	[Význam zkratky anglický]
SMS	Systém řízení provozní bezpečnosti	Safety Management System
SP	Sekce provozní	Aeronautical Operations Division
SSA	Zajištění bezpečnosti software *Pozn.: V souvislosti se SW.*	Software Safety Assurance
SSA	Posouzení bezpečnosti systému *Pozn.: V souladu s EUROCONTROL SAM.*	System Safety Assessment
SSAS	Systém zajištění bezpečnosti software	Software Safety Assurance System
SW	Programové vybavení	Software
SWAL	Úroveň zajištění SW	Software Assurance Level
ÚCL	Úřad pro civilní letectví	Civil Aviation Authority

Záměrně nepoužito.

DEFINICE

Pro potřeby tohoto dokumentu se využívají následující definice:

Pojem/definice	Anglický ekvivalent	Význam
Adaptační data	Adaptation data	Data, která přizpůsobují elementy systému uspořádání letového provozu (ATM) pro jejich konečné použití.
Akvizice	Acquisition	Proces získávání systému, SW produktu nebo SW služby.
Audit / prověrka / prověření	Audit	Provedení nezávislého hodnocení SW produktů a procesů řízeného autorizovanou osobou za účelem posouzení, zda jsou tyto produkty / procesy ve shodě s požadavky.
Aplikace COTS	Commercial Off-The-Shelf	Komerčně dostupná aplikace, kterou prodávají obchodníci prostřednictvím veřejně dostupných katalogů a která není určena pro úpravu podle požadavků zákazníka nebo zdokonalování.
COTS	COTS	Softwarové nebo hardwarové produkty, které jsou již vyvinuty a jsou k dispozici k prodeji široké veřejnosti. *Např.: Microsoft Office je COTS produkt, který je vytvořen jako softwarové řešení pro širokou veřejnost. COTS produkty jsou navrženy tak, aby se snadno implementovaly do stávajících systémů bez nutnosti přizpůsobení.* V tomto dokumentu se pod pojmem COTS uvažuje COTS SW.
COTS SW	COTS SW	COTS software zahrnuje širokou škálu software včetně dříve zakoupeného software, nevyvíjeného software a software dříve vyvinutého.
Firmware	Firmware	Kombinace hardwarového zařízení a počítačových instrukcí nebo počítačových dat, která jsou umístěna jako rezidentní SW určený pouze ke čtení v hardwarovém zařízení. Tento SW nemůže být pomocí programu snadno modifikován.
Hodnocení / evaluace	Evaluation	Systematické určování rozsahu, ve kterém entita uspokojuje specifikovaná kritéria.
Konfigurační položka	Configuration item	Entita v konfiguraci, která zabezpečuje jednu funkci konečného užití a může být jednoznačně identifikována v daném referenčním bodě.
Konfigurační data	Configuration data	Data, která konfigurují generický (obecný) softwarový systém pro konkrétní případy jeho použití.
Model životního cyklu	Lifecycle model	Soustava, která obsahuje procesy, činnosti a úlohy zahrnuté do vývoje, provozování a údržby SW produktu, a pokrývá život systému od definování požadavků na něj až po ukončení jeho užívání.

Pojem/definice	Anglický ekvivalent	Význam
Monitorování	Monitoring	Dozorování stavu činností dodavatele a jejich výsledků prováděné akvizitérem nebo třetí stranou.
Nevyvíjený SW	Non developmental software	Software nevyvíjený pro stávající kontrakt.
Ověřování / ověření / Verifikace	Verification	Potvrzení zkouškou a obstarání objektivního důkazu, že byly splněny specifikované požadavky. *Pozn.: Verifikace software zajišťuje, aby výrobek byl postaven v souladu s požadavky a specifikacemi návrhu, zatímco validace software zajišťuje, že výrobek skutečně splňuje potřeby uživatele. Verifikace software zajišťuje, že „je produkt postaven správně." Validace software potvrzuje, že výrobek bude plnit své zamýšlené použití.*
Pokrytí testem	Test coverage	Rozsah, ve kterém testovací případy testují požadavky na systém nebo SW produkt.
Release	Release	Zvláštní verze konfigurační položky, která je zpřístupněna pro specifický účel, např. release pro testování.
Software	Software	Počítačové programy a odpovídající konfigurační data, včetně nevyvíjeného softwaru, ale nezahrnující elektronické součástky jako integrované obvody specifické pro aplikaci, programovatelná hradlová pole nebo logické obvody.
Softwarová jednotka	Software unit	Samostatně kompilovatelná část kódu.
SW produkt	SW product	Množina počítačových programů, procedur a případně připojené dokumentace a dat.
Testování černé skříňky	Black box testing	Při použití testů černé skříňky není k dispozici přístup k programovému kódu. Software si lze v tomto případě představit jako černou skříňku, jejíž obsah (zdrojový kód) není zvenčí viditelný. Nezná se tedy, jak přesně systém pracuje s daty. Dá se pouze sledovat, jaký výsledek se získá po vložení vstupních dat.
Testování šedé skříňky	Grey box testing	Testování šedé skříňky je kombinace kategorií testů černé skříňky a bílé skříňky. V praxi se může jednat např. o situaci, kdy se software testuje přes jeho uživatelské rozhraní. Výsledky operací se pak ověřují pomocí dotazů do databáze.
Testování bílé skříňky	White box testing	U testů bílé skříňky je k dispozici zdrojový kód. Je tak známa vnitřní struktura software. Lépe se pak může otestovat pokud možno všechny průchody zdrojovým kódem, zadání neočekávaných vstupních hodnot a další testy, které vycházejí z kontroly zdrojového kódu.

Pojem/definice	Anglický ekvivalent	Význam
Validace	Validation	Potvrzení zkouškou a obstarání objektivního důkazu, že jsou splněny příslušné požadavky pro specifický cíl užití. *Pozn.: Při návrhu a vývoji SW se validace týká procesu testování produktu za účelem určení shody s požadavky uživatele. Pokud jsou stanoveny různé cíle užití SW, může být validace prováděna vícekrát.*
Základna	Baseline	Formálně odsouhlasená verze konfigurační položky, která je bez ohledu na nosič ve specifickém čase v průběhu životního cyklu položky formálně definována a pevně stanovena.

Popis rolí použitých v tomto dokumentu:

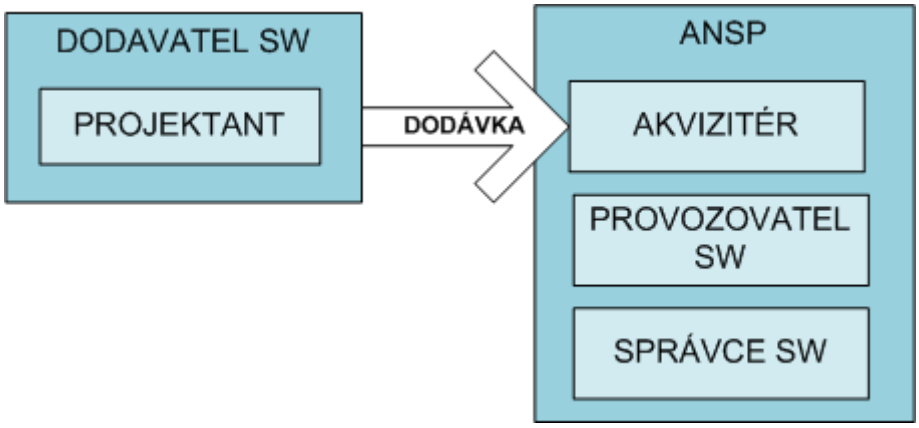
Pojem/definice	Anglický ekvivalent	Význam
Projektant	Developer	Organizace, v níž se vykonávají během životního cyklu SW vývojové činnosti, zahrnující analýzu požadavků, návrh, testování až do akceptace.
Dodavatel	Supplier	Organizace, která uzavírá s akvizitérem kontrakt na dodávku systému, SW produktu nebo SW služby podle podmínek kontraktu. *Pozn.: Akvizitér může určit jako dodavatele část své organizace.*
Akvizitér	Acquirer	Organizace, která získává nebo si opatřuje systém, SW produkt nebo SW službu u dodavatele. *Pozn: Akvizitérem může být např. kupující, zákazník, vlastník, uživatel, nákupčí, atd.*
Provozovatel	Operator	Organizace, která systém provozuje. *Pozn.: Provozovatel se může představit i v jiné roli, např. jako akvizitér, projektant nebo správce.*
Správce	Maintainer	Organizace, která vykonává činnosti spojené s údržbou.

Záměrně nepoužito.

ROLE

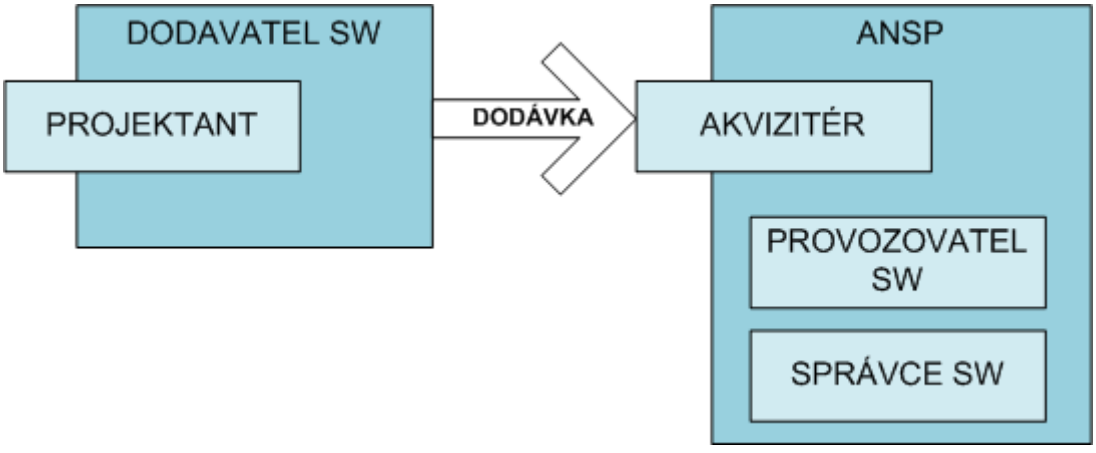
Níže jsou uvedeny některé z možností využití rolí. Nejedná se o vyčerpávající seznam, ale pouze znázornění některých variant, jejichž kombinací mohou vzniknout varianty nové. Vždy je ale za dodávku produktu zodpovědný dodavatel a za proces akvizice akvizitér, popř. organizace, která má s akvizitérem uzavřen smluvní vztah.

1. Na obrázku č. 1 je znázorněna role projektanta, který je součástí organizace, jež je zodpovědná za dodávku produktu (systému, SW, SW služby). ANSP v tomto případě plní roli akvizitéra, který je odpovědný za akvizici produktu. ANSP je zároveň provozovatelem i správcem systému.



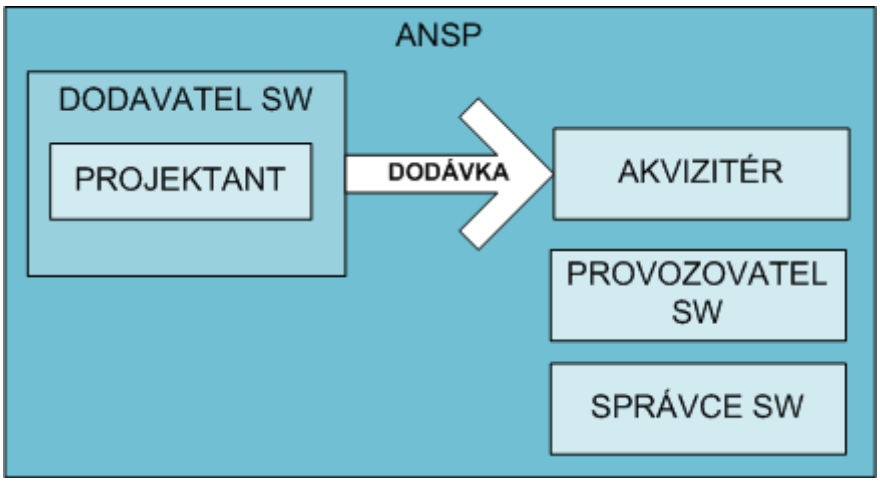
Obrázek č.1. *Role – Varianta 1*

2. Na obrázku č. 2 je znázorněna role projektanta, který není součástí organizace, jež je zodpovědná za dodávku produktu, projektant má s dodavatelem uzavřen smluvní vztah a za dodávku plně odpovídá dodavatel. Akvizitér není v tomto případě součástí ANSP, má s ANSP uzavřen smluvní vztah a ANSP odpovídá i za proces akvizice. ANSP je zároveň provozovatelem i správcem systému.



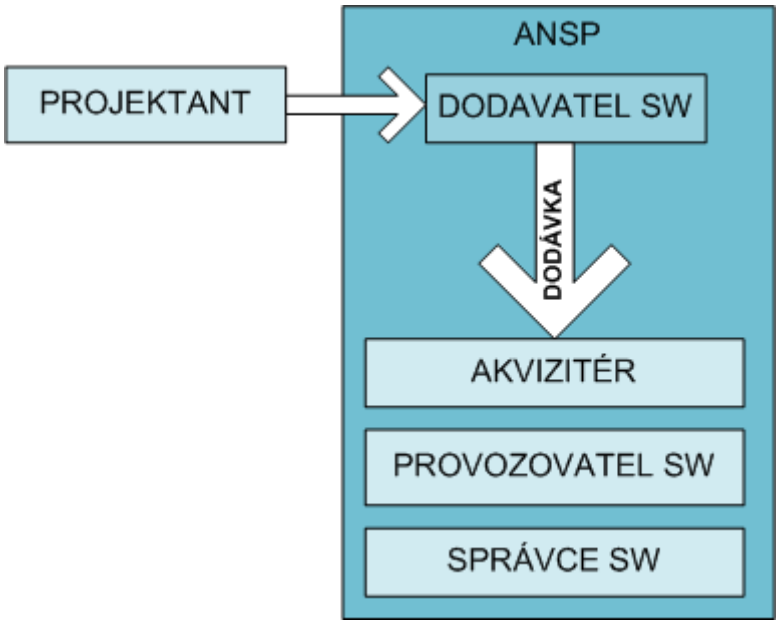
Obrázek č.2. *Role – Varianta 2*

3. Obrázek č. 3 znázorňuje variantu, kdy všechny role zastává ANSP, v tomto případě je tedy ANSP zodpovědný za všechny činnosti v procesu vývoje, dodání a akvizice produktu. ANSP je zároveň provozovatelem i správcem systému.



Obrázek č.3. *Role – Varianta 3*

4. Obrázek č. 4 znázorňuje variantu, kdy ANSP plní roli dodavatele, je tedy odpovědný za dodávku produktu. ANSP je zároveň akvizitérem, provozovatelem i správcem systému.



Obrázek č.4. *Role – Varianta 4*

1 ZÁKLADNÍ USTANOVENÍ

1.1. Cíl dokumentu

Dokument je zpracován se záměrem poskytnutí návodu pro stanovení cílů, jichž má být dosaženo pomocí definovaných kritérií pro jednotlivé úrovně zajištění bezpečnosti SW. Jeho využití se předpokládá úměrně ke složitosti projektu, na který bude aplikován.

Dále je možno využívat jeho jednotlivá ustanovení pro vytváření obecných požadavků na zajištění bezpečnosti SW v rámci ANSP nebo dodavatele SW, pro který musí být úroveň bezpečnosti prokazatelně zajišťována.

1.2. Závaznost a odpovědnost

Použití jednotlivých ustanovení je závazné v rozsahu, který je dotčeným subjektem deklarován. Odpovědnost za použitý rozsah uváděných požadavků je vždy na konkrétním subjektu, který je povinen v rámci kontrol plnění požadavků PNK 2017/373 prokázat, že jednotlivé požadavky uvedeného nařízení na prokazování bezpečnosti funkčního systému, jehož nedílnou součástí je SW, jsou naplněny v odpovídajícím rozsahu.

Záměrně nepoužito.

2 SYSTÉM ZAJIŠTĚNÍ BEZPEČNOSTI SW

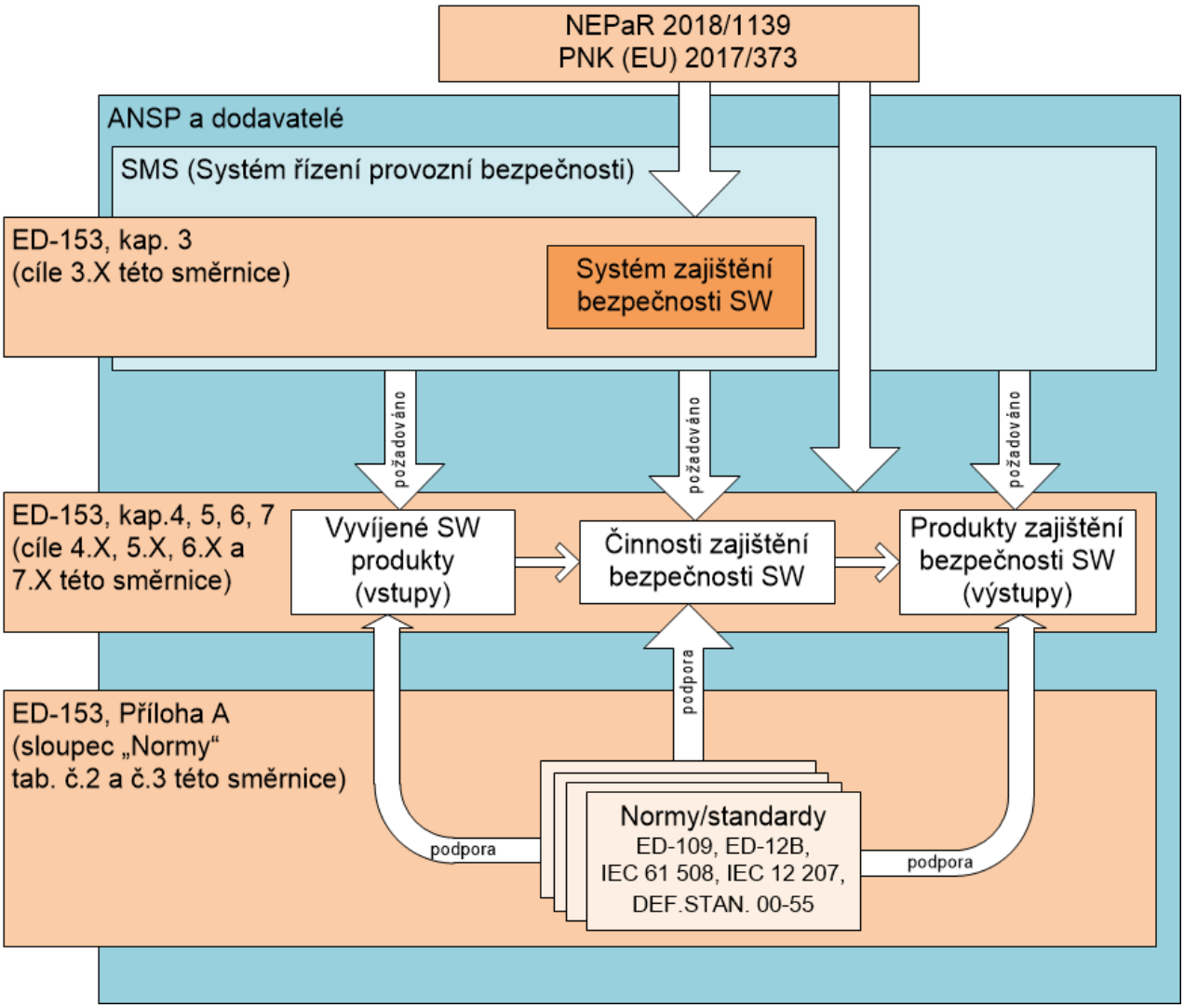
2.1. Obecně

Cílem systému zajištění bezpečnosti softwaru je dosáhnout, aby byly zavedeny vhodné postupy, které zabezpečí, že riziko spojené se zavedením (změnou) SW je sníženo na přijatelnou úroveň.

Tento dokument obsahuje postupy, jejichž aplikací je možné do určité míry prokázat plnění požadavků těchto nařízení EU:

- NEPaR 2018/1139,
- PNK (EU) 2017/373,

což je znázorněno na následujícím obrázku.



Obrázek č.5. *Znázornění návazností NEPaR 2018/1139, PNK (EU) 2017/373 na ED-153 a její podpory dalšími normami*

2.2. Úroveň zajištění SW

Jedním z požadavků PNK (EU) 2017/373 je provádění posuzování provozní bezpečnosti / podpory provozní bezpečnosti v souvislosti se změnou funkčního systému poskytovatele služeb ATM / ANS.

Zajištění požadované v AMC 6 ATM / ANS.OR.C.005 (a) (2) a AMC 4 ATS.OR.205 (a) (2) by mělo být poskytováno s různými úrovněmi důvěry v závislosti na nárocích důkazů a argumentů, které jsou předloženy. Tím pádem se jako nejvhodnější metoda jeví definování tzv. úrovní zajištění SW (SWAL), které odpovídají nárokům na zajištění softwaru podle kritičnosti posuzovaného softwaru v kombinaci s pravděpodobností výskytu určitého nepříznivého účinku.

V tomto dokumentu jsou uvažovány 4 úrovně SWAL (SWAL 1 až SWAL 4) v souladu s normou ED-153, přičemž úroveň zajištění softwaru 1 (SWAL 1) označuje nejkritičtější úroveň.

Dokument poskytuje návod pro stanovení cílů, jichž má být dosaženo pomocí definovaných kritérií pro jednotlivé úrovně zajištění (viz kapitola 3).

V následující tabulce je naznačen základní přístup kategorizace jednotlivých SWAL včetně stanovených základních kritérií (cílů) pro zajištění bezpečnosti pro daný SWAL. Každý SWAL přijímá mimo svých vlastních kritérií kritéria méně přísných SWAL.

SWAL	Chyby, kterým má být zabráněno	Metody pro prokazování zabránění chyb	Nezávislost při ověřování	Důkazy
4	Chyba funkčnosti SW	Platnost požadavků na software, testování.	Ne	Použití testů černé skříňky, aby zajistilo, že software plní své zamýšlené funkční specifikace.
3	Chyba návrhu architektury SW	Platnost a testování požadavků návrhu: testy rozhraní a funkčnosti základních složek SW.	Ne	Použití testů šedé skříňky pro lepší důkaz o zamýšleném fungování.
2	Chyba na úrovni zdrojového kódu	Platnost a testování detailních požadavků návrhu až do úrovně zdrojového kódu pokrývajících: kompatibilitu jednotlivých stavů SW, kompatibilitu HW, standarty pro programovací jazyky.	Pro některé cíle ano	Analýza jednotlivých řádků zdrojového kódu.
1	Chyba na úrovni spustitelného kódu	Detailní testování samotné implementace (spustitelného kódu) s podrobným pokrytím jednotlivých kroků / akcí v samotném SW a vstupních a výstupních podmínek.	Pro většinu cílů ano	Podrobná analýza jednotlivých kroků na úrovni spustitelného kódu a jejich výstupů za daných podmínek.

Tabulka č.1. *Přístup ke SWAL*

3 DOPORUČENÁ KRITÉRIA PRO JEDNOTLIVÉ SWAL

V této kapitole jsou definovány cíle, kterých má být dosaženo pro jednotlivé úrovně SWAL za účelem prokázání zajištění bezpečnosti SW.

3.1. Varianta orientovaná na cíle

Tato varianta je zaměřená na plnění předem definovaných cílů v souladu s normou ED-153. Naplněním jednotlivých cílů definovaných pro projekt / proces je prokazována bezpečnost SW pro oblast definovanou daným cílem. Tento způsob prokazování shody je doporučován pro ANSP. ANSP při definování požadavků na SW určí, které procesy, činnosti a úlohy doporučované v tomto dokumentu jsou pro projekt / proces vhodné, a přizpůsobí je v souladu s požadavky na dosažení SWAL.

Za účelem zavedení SSAS na úrovni organizace jako součást SMS, by měly být řešeny tyto cíle:

- Stanovení SSAS – prostřednictvím cílů 3.0.1.
- Dokumentované postupy – cíle v 3.2.1.
- Neustálé zlepšování procesů – cíle 6.3.X.
- Přidělování SWAL – cíle 3.0.5 a kap.3.6.
- Úroveň zajištění – cíle 3.0.8. a 3.0.9.
- Plánování zajištění bezpečnosti SW – cíle 3.2.X.
- Důkazy o činnostech v rámci zajištění, které byly provedeny – 3.5.X a bezpečnostní složky SW.
- Nezávislost zajištění a důkazy – cíle 3.0.9 a tabulky SWAL.
- Hodnocení a zmírnění rizik – cíle 3.3.X.
- Zmírňování rizik pro SW – cíle 3.3.4.
- Monitorování služby – cíle 3.0.11 a 4.4.5.
- Zpětná vazba – cíle 5.8.X.
- Řešení zaznamenaných poruch nebo selhání SW – cíle 5.8.X.
- Změny – cíle 3.0.12 a 5.8.2.
- Využití SW nástrojů – cíle 4.3.12, 4.3.17 až 4.3.19 a 7.3.X.
- Argument bezpečnosti – kap. 8.
- Zajištění platnosti požadavků na SW s mírou zajištění přiměřené SWAL – cíl 4.3.4.
- Zajištění dosažitelnosti požadavků na SW s mírou zajištění přiměřené SWAL – cíl 5.4.X.
- Zajištění, že oba výše uvedené požadavky jsou vhodně spojeny s posuzovanou verzí softwaru (např. řízení konfigurace) – cíle 5.2.X.

3.1.1. Legenda k tabulce č. 2

- Sloupec „ED-153“ – Jednoznačná identifikace cíle (číslování cílů je plně v souladu s normou ED-153).
- Sloupec „Cíl pro zajištění bezpečnosti SW“ – definuje cíl, jehož naplněním dochází k zajištění bezpečnosti SW v oblasti definované daným cílem.
- Sloupec „SWAL“ – definuje rozdílné nároky odpovídající jednotlivým úrovním zajištění softwaru takto:

Červené pole	Cíle, které musí být dosaženy nezávisle („nezávislým dosažením“ se v případě činností v rámci procesu ověřování softwaru rozumí, že činnosti v rámci procesu ověřování provádí jiná osoba (jiné osoby) než osoba, která ověřovaný prvek vyvinula).
Modré pole	Cíle, které musí být dosaženy.
Zelené pole	Dosažení cílů je na uvážení organizace.
Šedé pole	Není aplikováno.

- Sloupec „Normy“ – obsahuje odkazy na normy, které je možné dále využít při plnění stanovených cílů. Jedná se pouze o doporučení pro využití metodik / postupů vhodných pro zajištění naplnění definovaných cílů. Uvedené normy nemusí být již aktuální, nicméně jimi definované metodiky / postupy jsou pro proces zajištění bezpečnosti SW i nadále využitelné. Organizace může pro prokázání naplnění definovaného cíle využít i jiných norem / standardů, jejichž aplikovatelnost ověří a prokáže v rámci procesu zajištění bezpečnosti SW.

- Sloupec „Odpovědnost“ – obsahuje doporučení pro stanovení odpovědností a povinností pro dodavatele produktu a ANSP. Vychází z varianty 1 a 2 stanovení rolí v kapitole „Definice“ v tomto dokumentu. (viz obrázek č. 1 a č. 2), neboť se předpokládá, že se jedná o nejčastější varianty rozložení rolí. V případě jiného rozložení rolí je nutné vhodně upravit odpovědnosti.

  Stanovení odpovědností v tomto sloupci poté vychází ze dvou scénářů akvizice SW:

  - 1. scénář (I) – SW jako součást funkčního systému: akvizitér stanovuje požadavky vztažené k funkčnímu systému (stanovení provozních operací, požadavky na provozní a servisní personál, požadavky na postupy údržby, atd.). V tomto případě definuje dodavatel software požadavky na systém odvozené od požadavků akvizitéra. Následně pak definuje dodavatel software požadavky na SW.
  - 2. scénář (II) – SW jako samostatný prvek: akvizitér stanovuje požadavky přímo na SW. V tomto případě definuje akvizitér software požadavky na systém. Následně pak definuje dodavatel software požadavky na SW odvozené od požadavků akvizitéra.

Použitá symbolika ve sloupci „Odpovědnost“:

- L (lead) – řídí,
- C (contribute) – spolupracuje,
- A (accept) – provádí akceptaci.

ED-153	Cíl pro zajištění bezpečnosti SW	SWAL				Normy	Odpovědnost
3.0.1	**Implementace** Systém zajištění bezpečnosti SW musí být definován a implementován (jako součást celkové dokumentace posouzení provozní bezpečnosti systému). *Pozn.: Postupy a metodika pro zajištění bezpečnosti SW jsou součástí dokumentace posouzení bezpečnosti systému, jedná se o komplexní výklad toho, jakým způsobem se zajišťuje bezpečnost SW.*	1	2	3	4	ED-109/DO 278. ED-12B/DO 178B. IEC 61508.	I/II ANSP: L, dodavatel: C.
3.0.2	**Kompletnost a správnost požadavků** Požadavky na software musí správně a úplně stanovit to, co je požadováno od SW, aby splňoval cíle bezpečnosti systému a požadavky bezpečnosti systému identifikované na základě rizik. *Pozn.: Jedná se o přezkumy a analýzy požadavků na nejvyšší úrovni – shoda požadavků na SW se systémovými požadavky (nesmí dojít k rozporu), přesnost a jednoznačnost požadavků (výklad požadavků je stejný u všech zainteresovaných stran), kompatibilita SW s HW cílového počítače, ověřitelnost (dají se všechny cíle ověřit/měřit?), shoda s normami a legislativou, atd.*	1	2	3	4	ISO/IEC 12207. ED-109/DO 278 - 3.2 – Tab. A-2 , 3.3 Tab. A-3. ED-12B/DO 178B - 5.1, 6.3.1. IEC 61508 - 7.2.2. CMMI - RD 1.1, 1.2, 2.1	I ANSP: A, dodavatel: L. II ANSP: L, dodavatel: C.
3.0.3	**Zajištění sledovatelnosti (návaznosti) požadavků** Veškeré požadavky na software musí být vysledovatelné na úroveň požadovanou SWAL.	1	2	3	4	ISO/IEC 12207. ED-109/DO 278 - A3.6, A4.6, A5.6. ED-12B/DO 178B - 5.5. IEC 61508. CMMI - ReqM 1.4.	I/II ANSP: C/A, dodavatel: L.
3.0.4	**Nezamýšlené funkce** Implementace SW nesmí obsahovat funkce, které mohou nepříznivě ovlivnit bezpečnost, nebo jejichž účinek není v souladu s analýzou bezpečnosti. *Pozn.: Tento cíl neznamená, že neexistují žádné nezamýšlené funkce SW, ale že tyto funkce nejsou aktivovány, nebo že následek jejich aktivování je odůvodněn bezpečnostní analýzou.*	1	2	3	4	ED-109/DO 278 – 3.6 Tab. A-5. ED-12B/DO 178B – 6.3.4.a. IEC 61508 – 7.4.7.2.	I/II ANSP: A, dodavatel: L.
3.0.5	**Přiřazení SWAL** ANSP musí minimálně zajistit, aby v rámci SSAS přiděloval SWAL veškerému ANS software provozovanému na pozemních zařízeních. *Pozn.: Viz kapitola 2 oddíl 2 ED-153 - SWAL definice a proces přiřazování SWAL.*	1	2	3	4	ED-12B/DO 178B - 2.2.2, 2.2.3. IEC 61508 - 7.5.2, 7.6.2.	I ANSP: L, dodavatel: C. I/II ANSP: L.

ED-153	Cíl pro zajištění bezpečnosti SW	SWAL				Normy	Odpovědnost
3.0.6	**Zajištění naplnění požadavků** ANS software musí splňovat požadavky na něj kladené na úrovni jistoty, která je v souladu se SWAL, přidělenou při posuzování a zmírňování rizik (např. PSSA).	1	2	3	4	ED-109/DO 278 - 2.1. ED-12B/DO 178B - 5.1. IEC 61508 - 7.2.	I/II ANSP: A, dodavatel: L.
3.0.7	**Zajištění řízení konfigurace** Každé ujištění musí být vždy odvozeno ze známé spustitelné verze SW, známého rozsahu konfiguračních dat, a známých souborů SW produktů a popisů (včetně specifikace), které byly použity ve výrobě konkrétní verze SW. *Pozn.: Proces řízení konfigurace.*	1	2	3	4	ISO/IEC 12207. ED-109/DO 278 - 3.8 Tab. A-8. ED-12B/DO 178B - 7. IEC 61508 - 6.2.3. CMMI - CM.	*Proces vývoje:* I/II ANSP: A, dodavatel: L. *Provoz, údržba:* I/II ANSP: L.
3.0.8	**Zajištění cíle** SWAL musí poskytovat dostatečnou jistotu, že ANS software může být provozován aspoň s minimální přijatelnou úrovní provozní bezpečnosti. *Pozn.: Systém řízení rizik pro SW s definovanou SWAL.*	1	2	3	4	ED-109/DO 278 - 2.1 ED-12B/DO 178B – 2.1, 9 a 11.20 IEC 61508 - 1-7.4.2.	I/II ANSP: L, dodavatel: C.
3.0.9	**Zajištění přísnosti (závažnosti) kritérií** Rozdílné nároky na zajištění SWAL musí obsahovat následující kritéria: • Požadavek na nezávislé dosažení cíle. • Požadavek na dosažení cíle. • Není požadováno. *Pozn.: V této směrnici se jedná o sloupec „SWAL“ a jeho barevné varianty pro jednotlivé SWAL.*	1	2	3	4	ED-109/DO 278 - 3. ED-12B/DO 178B - Appendix A. IEC 61508 - Appendix A.	Dle jednotlivých cílů
3.0.10	**Zajištění SWAL** Zajištění musí poskytovat důvěru, že je dosaženo SWAL. *Pozn.: Ujištění může být založeno na přímých či nepřímých argumentech a důkazech. Metodika viz kap.9 ED-12B/DO 178B.*	1	2	3	4	ED-109/DO 278 - 3.10 Tab. A-10, 5.1. ED-12B/DO 178B - 9, 11.20. IEC 61508 - 6.2.2	I/II ANSP: C, dodavatel: L.

ED-153	Cíl pro zajištění bezpečnosti SW	SWAL				Normy	Odpovědnost
3.0.11	**Sledování SWAL** Pokud SW v provozu splňuje požadavky s mírou důvěry úměrnou SWAL, musí být zajištění prováděno prostřednictvím monitorování SW v provozu. Zpětná vazba ze zkušeností s ANS SW musí být použita na potvrzení toho, že SSAS a přiřazení SWAL jsou vhodné. Pro tento účel musí být hodnocen účinek vyplývající ze všech zaznamenaných závad SW nebo selhání identifikovaná v provozním využití SW (hlášení událostí dle interních postupů ANSP) v souladu s mapováním SWAL. *Pozn.: Hlášené závady SW nebo jeho selhání jsou výstupem systému hlášení událostí jako součást ANSP SMS.*	1	2	3	4	ED-109/DO 278 - 4.1.6.3.	I/II ANSP: L.
3.0.12	**Modifikace SW** Jakákoli změna SW musí vést nejprve k opětovnému posouzení bezpečnostních dopadů této změny na systém, a pak v závislosti na tomto dopadu musí vést k opětovnému posouzení SWAL, přidělenému tomuto SW.	1	2	3	4	ED-109/DO 278 - 4.1.4.2. IEC 61508 - 7.8.	*Vývoj:* I/II ANSP: A, dodavatel: L. *provoz, údržba:* I/II ANSP: L, dodavatel: C.
3.0.13	**COTS** Musí být zajištěna stejná úroveň jistoty prostřednictvím prostředků vybraných a schválených schvalovacím orgánem pro stejnou úroveň zajištění softwaru pro COTS. Tyto prostředky musí poskytovat dostatečnou jistotu, že software splňuje bezpečnostní cíle a požadavky stanovené v rámci hodnocení a zmírňování bezpečnostních rizik.	1	2	3	4	ED-109/DO 278 - 4.1, 4.2.	I/II ANSP: A, dodavatel: L.
3.0.14	**Nezávislost** Těm částem ANS SW, u kterých nemůže být prokázáno, že jsou izolovány od sebe navzájem (jsou na sobě nezávislé), musí být přidělen SWAL odpovídající pro nejkritičtější část.	1	2	3	4	ED-109/DO 278 - 2.2.1. ED-12B/DO 178B - 2.2.3, 2.3.1. IEC 61508.	I Dodavatel: L. II ANSP: L, dodavatel: C.

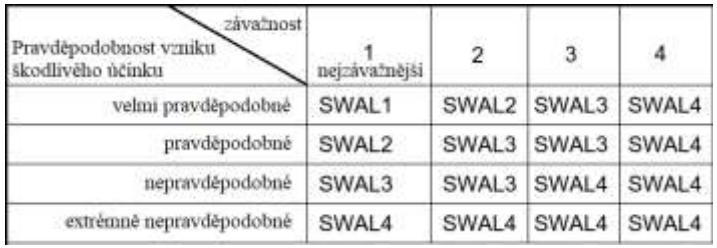
ED-153	Cíl pro zajištění bezpečnosti SW	SWAL				Normy	Odpovědnost
3.0.15	**On-line aspekty provozních změn SW** SSAS se musí zabývat specifickými aspekty souvisejícími se SW, včetně všech on-line provozních změn (např. přepnutí na zálohu / výměna za provozu). *Pozn.: Především pro CNS/ATM systémy, které jsou provozovány v režimu H24 a vyvstává nutnost pro výměnu komponentů za provozu systému. Měl by být popsán mechanismus pro zajištění úrovně dostupnosti a integrity dat během instalace SW, měly by být definovány cíle v rámci celého procesu od začátku instalace po její ukončení, měla by být zajištěna možnost návratu k předchozí konfiguraci a plná kompatibilita nové verze SW s ostatními částmi systému, atd.*	1	2	3	4	ED-109/DO 278 - 2.2.5.	I/II ANSP: L, dodavatel: C.
3.0.16	**Zajištění naplnění cílů** Organizace musí vytvořit potřebné záruky pro NSA, které prokazují, že cíle dle přiděleného SWAL byly splněny.	1	2	3	4	N/A	I/II ANSP: L.
3.0.17	**Tvorba argumentu** Organizace musí předložit argument prokazující, že cíle přiděleného SWAL byly splněny. *Poznámka: Nejsou stanoveny mandatorní postupy, strategie tvorby argumentu je v plné kompetenci organizace.*	1	2	3	4	ED-109/DO 278 - 3. ED-12B/DO 178B - 6.3.1, 6.3.3, 6.3.4, 8.3, 10.2, 11.20, 12.1. IEC 61508 - 3-7, 3-8.	I ANSP: L, dodavatel: C. II ANSP: L, dodavatel: C.
3.1.1	**Popis systému** Musí být definováno: **(3.1.1.1)** Provozní scénáře (např. HMI: Provozní příručka, která definuje provozní režim a HMI, normální režim, degradační režim). **(3.1.1.2)** SW a systémové funkce. **(3.1.1.3)** Meze (parametry) SW (např. funkční / provozní, časové). **(3.1.1.4)** Externí rozhraní SW.	1	2	3	4	ED-109/DO 278 - 2.2. ED-12B/DO 178B - 2.1. IEC 61508 - I-7.2.1. CMMI - a) RD 1.1, b) RD 3.1, TS 1.2, c) RD 3.2, e) RD 2.3, TS 2.3.	I ANSP: C/A, dodavatel: L. II ANSP: L, dodavatel: C.
3.1.2	**Provozní prostředí** Software a jeho prostředí (fyzické, provozní, kontrolní funkce, legislativní atd.) musí být popsáno dostatečně detailně, aby bylo možné uspokojivě provést bezpečnostní úkoly životního cyklu.	1	2	3	4	ED-109/DO 278 - 2.2. ED-12B/DO 178B - 2.1,1. IEC 61508 - I-7.2.1. CMMI - RD 1.1.	I ANSP: C/A, dodavatel: L. II ANSP: L, dodavatel: C.

ED-153	Cíl pro zajištění bezpečnosti SW	SWAL				Normy	Odpovědnost
3.1.3	**Regulatorní rámec** Musí být identifikovány platné regulatorní bezpečnostní cíle a požadavky. *Pozn.: Jedná se o identifikaci požadavků bezpečnosti a cílů bezpečnosti obsažených v aktuálních dokumentech legislativní báze, tj. v platných nařízeních, normách, zákonech, směrnicích, atd.*	1	2	3	4	ED-109/DO 278 - 3.10 Tab. A-10. ED-12B/DO 178B - 2.1.1, 9, 10. IEC 61508 - I-7.2.2.4.	I ANSP: C/A, dodavatel: L. II ANSP: L, dodavatel: C.
3.1.4	**Aplikovatelné procesy a pokyny** Procesy a pokyny vztahující se k zajištění SW musí být odsouhlaseny dle interních postupů organizace. *Pozn.: Např. v rámci systému řízení dokumentace společnosti.*	1	2	3	4	ISO/IEC 12207. ED-109/DO 278. ED-12B/DO 178B. IEC 61508. CMMI.	I ANSP: C/A, dodavatel: L. II ANSP: L, dodavatel: C.
3.1.5	**Výstup procesu řízení rizik** Postupy pro řízení rizik (identifikace, analýza, hodnocení, zmírnění rizik) na úrovni systému musí být znovu provedeny na úrovni softwaru, aby byla zajištěna konsistence s architekturou / návrhem softwaru. *Pozn.: Běžná praxe pro snížení bezpečnostního rizika v návrhu systému je izolace funkcí, které mohou způsobit nebo přispět k selhání systému. Analýza by měla popsat datový tok v systému, aby bylo možné identifikovat, které chyby mohou potenciálně způsobit další negativní reakce. Dále by měly být popsány a řešeny případné konflikty mezi požadavky na ochranu (security) a bezpečnost (safety). Součástí analýzy by měly být i požadavky bezpečnosti v procesu adaptace SW a případné změny SW za provozu systému.*	1	2	3	4	ED-109/DO 278 - 2.2. ED-12B/DO 178B - 2.1.1. IEC 61508 - I-7.	I ANSP: L. II ANSP: L, dodavatel: C.
3.2.1	**Přístup k posouzení bezpečnosti SW** Musí být definován celkový přístup k posuzování bezpečnosti softwaru v rámci životního cyklu softwaru. *Pozn.: Plán pro akceptaci SW by měl obsahovat např. popis systému (funkce, HW, SW, architektura, rozhraní, bezpečnost), popis SW, identifikaci předpisové základny včetně postupů pro dokazovány shody, popis životního cyklu SW s definovanými výstupy a odpovědnostmi osob v rámci tohoto cyklu, časový a věcný plán projektu, specifika v rámci procesu, atd.*	1	2	3	4	ED-109/DO 278 - 5.1. ED-12B/DO 178B - 11.1. IEC 61508 - 8.	I/II ANSP: C/A, dodavatel: L.

ED-153	Cíl pro zajištění bezpečnosti SW	SWAL				Normy	Odpovědnost
		1	2	3	4		
3.2.2	**Plán posouzení bezpečnosti SW** Musí být vypracován plán popisující kroky posuzování bezpečnosti softwaru. *Pozn.: Např. volba metodiky, vztahy mezi posuzováním bezpečnosti a životním cyklem SW, dodávka (obsah a datum dodání), řízení rizik projektu ve vztahu k otázkám bezpečnosti, odpovědnosti, osoby, organizace, schéma klasifikace rizik, definice bezpečnostních cílů, metody identifikace rizik (nebezpečí), činnosti pro zajištění bezpečnosti, plánování, zdroje.*					ED-109/DO 278 - 5.1 - 3.10 Tab. A-10. ED-12B/DO 178B - 11. IEC 61508 - I-7.8.	I/II ANSP: C/A, dodavatel: L.
3.2.3	**Přezkoumání plánu posouzení bezpečnosti SW** Plán posuzování bezpečnosti SW by měl být akceptován NSA.					ED-109/DO 278 - 5.1 - 3.10 Tab. A-10. ED-12B/DO 178B - 9,10.	I/II ANSP: C/A, dodavatel: L.
3.2.4	**Distribuce plánu posouzení bezpečnosti SW** Plán posouzení bezpečnosti SW musí být distribuován všem zainteresovaným stranám. *Pozn.: Proces životního cyklu SW zahrnuje např. tyto strany – akvizitér SW, dodavatel SW, projektant SW, provozovatel SW, správce SW, správce/ manažer procesů, nezávislá strana. Tento dokument nedefinuje, kdo jsou zainteresované strany. Zainteresované strany jsou definovány v souladu se schváleným plánem bezpečnosti SW, v souladu se SMS ANSP a v souladu s příslušnými předpisovými bezpečnostními požadavky.*					ED-109/DO 278 - 5.1. ED-12B/DO 178B - 9,10.	I/II ANSP: C/A, dodavatel: L.
3.3.1	**Identifikace chyb** Případná selhání SW musí být identifikována tak, že se zvažují různé způsoby, jak může software selhat, a dále tím, že se zvažuje sled událostí, které vedou k výskytu poruchy. Musí být vypracován seznam jednotlivých, následných a společných způsobů selhání. *Pozn.: Návod na společnou analýzu režimu (Common Mode Analysis) lze nalézt v ED-79. V rámci FHA – např. dle metodiky ICAO Doc 9859 Safety Management Manual (SMM).*					ED-12B/DO 178B - 2.2, 2.2.2 IEC 61508 - I-7.4.	I/II ANSP: C/A, dodavatel: L.

ED-153	Cíl pro zajištění bezpečnosti SW	SWAL				Normy	Odpovědnost
3.3.2	**Účinky chyb** Musí být hodnoceny účinky výskytu poruchy. Nebezpečí spojená s výskytem selhání SW musí být identifikována pro vytvoření kompletního seznamu nebezpečí, jež byl iniciovaný během procesu vyhodnocení a zmírnění rizika (např. FHA a další doplnění během PSSA).	1	2	3	4	ED-12B/DO 178B - 2.2, 2.2.1. IEC 61508 - I-7.4.	I/II ANSP: C/A, dodavatel: L.
3.3.3	**Posouzení rizik** Počáteční proces posouzení a zmírnění rizik (např. FHA a další doplnění během PSSA) musí být přezkoumán na základě výsledků z 3.3.1 a 3.3.2. *Pozn.: Proces řízení rizik (identifikace rizik, analýza rizik, návrh nápravných a preventivních opatření, aplikace navržených opatření, hodnocení aplikovatelnosti navržených opatření, hodnocení účinnosti zavedených opatření, atd.).*	1	2	3	4	ED-12B/DO 178B - 2.2.1. IEC 61508 - I-7.5.	I ANSP: L. II ANSP: C/A, dodavatel: L.
3.3.4	**Stanovení požadavků na SW** Požadavky na SW musí vyhovět bezpečnostním cílům, na kterých se SW podílí a být v souladu s bezpečnostními systémovými požadavky. *Pozn.: Definice „vyhovět“ musí být vyvinuta jako součást argumentu podporujícího dodržení tohoto cíle. Tato definice by měla zahrnovat dohledatelnost s výše uvedenou úrovní požadavků, prokázat nutnost, dostatečnost, vhodnost a relevanci požadavků k uspokojení výše uvedené úrovně požadavků.* *Jedná se o soulad požadavků na SW se systémovými požadavky v rámci procesu řízení rizik, tzn. např., že snížení rizik na úrovni SW musí zajistit snížení pravděpodobnosti výskytu rizik na úrovni systému.*	1	2	3	4	ED-12B/DO 178B - 2.2.1. IEC 61508 - I-7.4, I-7.6. CMMI - a.1) RD 2.1, 2.2, a.2) TS 2.1, Ver. 1.1, 2.2, 2.3	I/II ANSP: C/A, dodavatel: L.
3.4.1	**Hodnocení (validace) posouzení bezpečnosti SW** **(3.4.1)** Systém zajištění bezpečnosti SW musí poskytnout cestu ke zdůvodnění toho, že požadavky na SW jsou úplné a správné. *Pozn.: Popis metodiky pro proces verifikace a validace v rámci životního cyklu SW – navržená měření, hodnocení výsledků, cykly pro měření, stanovení testovacích nástrojů, atd. Pro validaci mohou být použity tyto metody: testování, analýza, modelování, simulace, atd.*	1	2	3	4	ISO/IEC 12207. ED-109/DO 278 - 3.3 Tab. A-3 3.4 Tab. A-4. ED-12B/DO 178B - 6.3. CMMI - a) RD 3.3, 3.4, 3.5 Ver. 2.1, 2.2, 2.3.	I/II ANSP: C/A, dodavatel: L.

ED-153	Cíl pro zajištění bezpečnosti SW	SWAL				Normy	Odpovědnost
3.4.2	**Ověřování (verifikace) posouzení bezpečnosti SW** Požadavky na SW musí být stanoveny v souladu s postupy pro zmírnění následků nebezpečí (rizika) a s bezpečnostními cíli rizik. *Pozn.: Stanovení SWAL.*	1	2	3	4	ED-109/DO 278 - 2.1. ED-12B/DO 178B - 2.2.2.	I/II ANSP: C/A, dodavatel: L.
3.4.3	**Proces zajištění posouzení bezpečností SW** Posouzení bezpečnosti SW musí být provedeno úplně. *Pozn.: V souladu se schváleným bezpečnostním plánem SW, v souladu s ANSP SMS a v souladu s požadavky příslušných bezpečnostních předpisů.*	1	2	3	4	ISO/IEC 12207 - 3.4. ED-109/DO 278 - 3.9 Tab. A-9 ED-12B/DO 178B - 8.	I/II ANSP: C/A, dodavatel: L.
3.4.4	**Zajištění bezpečnosti SW** Musí být poskytnut důkaz a ujištění, že požadavky na SW jsou plněny. *Pozn.: Např. formou studií bezpečnosti, studií na podporu bezpečnosti, dokladu o posouzení bezpečnosti, nebo jiných dokumentovaných výstupů zpracovávaných v rámci systému řízení dokumentace dotčené organizace.*	1	2	3	4	ISO/IEC 12207.	I/II ANSP: C/A, dodavatel: L.
3.5.1	**Dokumentace výsledků procesu posouzení bezpečnosti SW** Výsledky procesu hodnocení bezpečnosti softwaru musí být dokumentovány. *Pozn.: Proces dokumentování je proces, který zaznamenává informace vytvořené v procesu nebo činnosti životního cyklu, obsahuje soubor činností, kterými se plánují, navrhují, vyvíjejí, vyrábějí, editují, distribuují a udržují ty dokumenty, které jsou potřebné pro všechny zainteresované strany. Lze např. využít také metodiky v rámci systému řízení dokumentace dle ISO 9001.*	1	2	3	4	ISO/IEC 12207. ED-109/DO 278 - 5. ED-12B/DO 178B - 11, Annex A. IEC 61508 - I-7.2.2.6, I-7.3.2.5, I-7.4.2.11. CMMI.	I/II ANSP: C/A, dodavatel: L.
3.5.2	**Řízení konfigurace dokumentace posouzení bezpečnosti SW** Dokumentace procesu posuzování bezpečnosti SW musí podléhat řízení konfigurace. *Pozn.: Proces řízení konfigurace je procesem aplikování administrativních a technických postupů v průběhu celého životního cyklu SW pro identifikaci, definici a vytvoření SW položek, kontrolu modifikací a vydání položek, záznam a podávání zpráv o stavu položek a požadavků na modifikaci, zajištění úplnosti, konzistence a správnosti položek, kontrolu ukládání, manipulace a dodávek položek. Zajišťuje udržení integrity všech produktů.*	1	2	3	4	ISO/IEC 12207. ED-109/DO 278 - 3.8-4.1.7. ED-12B/DO 178B - 7.3, Annex A. IEC 61508 -I-7.4.2.12. CMMI - CM 1.1.	I/II ANSP: C/A, dodavatel: L.

<table>
<tr><th>ED-153</th><th>Cíl pro zajištění bezpečnosti SW</th><th>SWAL</th><th>Normy</th><th>Odpovědnost</th></tr>
<tr><td>3.5.3</td><td>Distribuce dokumentace posouzení bezpečnosti SW
Dokumentace procesu posuzování bezpečnosti SW musí být distribuována zainteresovaným stranám.
Pozn.: Tento dokument nedefinuje, kdo jsou zainteresované strany. Zainteresované strany jsou definovány v souladu se schváleným plánem bezpečnosti SW, v souladu se SMS ANSP a v souladu s příslušnými předpisovými bezpečnostními požadavky.</td><td>1 2 3 4</td><td>ED-109/DO 278 - 5.1- 3.10
Tab. A-10.
ED-12B/DO 178B - 9,10.3 CMMI - GP 2.7.</td><td>I/II
ANSP: C/A,
dodavatel: L.</td></tr>
<tr><td>3.6.0.1</td><td>SWAL
Proces přidělování SWAL se provádí během návrhu ANS systému jako součást procesu posuzování a zmírňování rizik.</td><td>1 2 3 4</td><td>N/A</td><td>I/II
ANSP: L,
dodavatel: C.</td></tr>
<tr><td>3.6.0.2</td><td>SWAL
SWAL musí SW přidělit odborný tým.
Pozn.: Odborný tým by měl zahrnovat i designéry systémů a odborníky na bezpečnost.</td><td>1 2 3 4</td><td>N/A</td><td>I/II
ANSP: L,
dodavatel: C.</td></tr>
<tr><td>3.6.2.0.1</td><td>Přidělení SWAL
Pro přidělení SWAL ANS software je vyžadována aplikace následujících kroků:
• Stanovení pravděpodobnosti, kdy selhání SW může způsobit škodlivý účinek.
• Stanovení závažnosti následků pro každý škodlivý účinek identifikovaného nebezpečí.
• Zdůvodnění pravděpodobnosti výskytu (viz pokyny v 3.6.2.2).
• Identifikace SWAL pro stanovený risk index pomocí matice níže.
• Opakovat předchozí dva kroky pro všechny poruchy / chyby SW.
 
<table>
<tr><th>závažnost / Pravděpodobnost vzniku škodlivého účinku</th><th>1 nejzávažnější</th><th>2</th><th>3</th><th>4</th></tr>
<tr><td>velmi pravděpodobné</td><td>SWAL1</td><td>SWAL2</td><td>SWAL3</td><td>SWAL4</td></tr>
<tr><td>pravděpodobné</td><td>SWAL2</td><td>SWAL3</td><td>SWAL3</td><td>SWAL4</td></tr>
<tr><td>nepravděpodobné</td><td>SWAL3</td><td>SWAL3</td><td>SWAL4</td><td>SWAL4</td></tr>
<tr><td>extrémně nepravděpodobné</td><td>SWAL4</td><td>SWAL4</td><td>SWAL4</td><td>SWAL4</td></tr>
</table></td><td>1 2 3 4</td><td>N/A</td><td>I/II
ANSP: L,
dodavatel: C.</td></tr>
</table>

ED-153	Cíl pro zajištění bezpečnosti SW	SWAL				Normy	Odpovědnost
3.6.2.0.3	**Nezávislost** Těm částem ANS SW, u kterých nemůže být prokázáno, že jsou izolovány od sebe navzájem (jsou na sobě nezávislé), musí být přidělen SWAL odpovídající pro nejkritičtější část.	1	2	3	4	ED-109/DO 278 - 2.2.1. ED-12B/DO 178B - 2.2.3, 2.3.1. IEC 61508.	I Dodavatel: L. II ANSP: L, dodavatel: C.
3.6.2.0.4	Každé uvedení softwaru do provozu musí prokázat, že je splněna přijatelná úroveň bezpečnosti.	1	2	3	4	N/A	I/II ANSP: L.
3.6.5.1	V současné době existuje několik standardů, které definují činnosti, jejichž důkazy se týkají některých cílů uvedených v ED-153 a tomto dokumentu. Pokud je taková norma organizací použita, musí být doplněna do dokumentace jako prostředek shody, aby byly splněny cíle / činnosti stanovené pro daný SWAL.  Příklad:	1	2	3	4	N/A	I ANSP: L. Dodavatel: C. II ANSP: L, dodavatel: C.
4.1.1	**Proces akvizice - Inicializace** Akvizitér začíná proces akvizice popisem koncepce nebo potřeb akvizice, vývoje, nebo rozšíření systému, softwarového produktu nebo SW služby. Akvizitér musí definovat, analyzovat a schválit systémové požadavky *(např. proti požadavkům uživatele).* Tyto systémové požadavky musí zahrnovat požadavky obchodní, organizační a uživatelské, jakož i požadavky na bezpečnost (safety), ochranu (security) a ostatní kritické požadavky spolu se souvisejícími normami a procedurami pro návrh, testování a shodu. Akvizitér musí připravit, dokumentovat a realizovat akviziční plán. *Pozn.: Aplikace tohoto cíle je omezena obsahem kontraktu mezi dodavatelem a akvizitérem. Proto by tento cíl měl být sladěn se 4.3.3.*	1	2	3	4	ISO/IEC 12207. CMMI – SAM 1.1, 2.1, TS 2.4; RD1.2,2.1, ReqM1.4; GP 2.2, 3.1; ISM GP 2.2, 3.1.	I/II ANSP: L.

ED-153	Cíl pro zajištění bezpečnosti SW	SWAL				Normy	Odpovědnost
4.1.2	**Cíle bezpečnosti procesu řízení rizik** Akvizitér musí určit, jak bezpečný SW potřebuje. Za tím účelem musí provést analýzu nebezpečí (např. FHA) a identifikovat cíle bezpečnosti pro jednotlivá nebezpečí.	1	2	3	4	IEC 61508 - 1-7.2, 1-7.3. IEC 61508 - 1-7.4, 1-7.5.	I/II ANSP: L.
4.1.3	**Požadavky bezpečnosti procesu řízení rizik** Akvizitér musí určit (v průběhu fáze návrhu), zda je očekáváno nebo neočekáváno v rámci navrhované architektury dosažení cílů bezpečnosti. Dále musí specifikovat požadavky bezpečnosti včetně přidělení SWAL pro systémové složky.	1	2	3	4	ED-109/DO 278 - 2 ED-12B/DO 178B - 2. IEC 61508 - 1-7.6.	I/II ANSP: L.
4.1.4	**Žádost o nabídku (tendr)** V průběhu definování požadavků pro výběrové řízení musí akvizitér určit, které procesy, činnosti a úlohy doporučované v tomto dokumentu jsou pro projekt vhodné a musí je přizpůsobit v souladu se SWAL. *Pozn.: Požadavky mohou obsahovat např. požadavky na systém, prohlášení o rozsahu, instrukce pro nabízející, seznam SW produktů, termíny a podmínky, zajištění subdodávek, technická omezení, atd.*	1	2	3	4	ISO/IEC 12207. CMMI - SAM 1.2.	I/II ANSP: L.
4.1.5	**Výběr nabídky** Akvizitér stanoví postup pro výběr dodavatele včetně návrhu hodnotících kritérií a hodnocení shody s požadavky.	1	2	3	4	ISO/IEC 12207. CMMI - SAM 1.2.	I/II ANSP: L.
4.1.6	**Proces akvizice – monitorování dodavatele** Akvizitér musí monitorovat a projednat s dodavatelem postup týkající se smluvních aktivit. *Pozn.: Monitorování dodavatele v souladu s procesem společného přezkoumání a auditu.*	1	2	3	4	ISO/IEC 12207. CMMI - SAM 2.2.	I/II ANSP: L, dodavatel: C.

ED-153	Cíl pro zajištění bezpečnosti SW	SWAL				Normy	Odpovědnost
4.1.7	**Akceptace** **(4.1.7.1)** Akvizitér musí připravit akceptaci SW na základě definované strategie a kritérií akceptace. Musí v nich být zahrnuta příprava testovacích případů, testovacích dat, testovacích procedur a testovacího prostředí. **(4.1.7.2)** Musí být definován rozsah spoluodpovědnosti (zapojení) dodavatele. **(4.1.7.3)** Akvizitér musí provádět akceptační přezkoumání a testování dodaných SW produktů nebo služeb.	1	2	3	4	ISO/IEC 12207 - 5.1.5. CMMI - SAM 2.3.	I/II ANSP: L, dodavatel: C.
4.2.1	**Proces dodání produktu – inicializace** Dodavatel musí provést přezkum požadavků v žádosti o přijetí návrhu brát v úvahu organizační zásady a další předpisy pro přípravu reakce.	1	2	3	4	ISO/IEC 12207 - 5.2.1. CMMI - RD 1.1, 1.2, 3.3, 3.4.	I/II Dodavatel: L.
4.2.2	**Příprava nabídky** Dodavatel musí definovat a připravit nabídku jako reakci na žádost o nabídku, včetně jejího přizpůsobení aplikovatelným mezinárodním normám / pravidlům.	1	2	3	4	ISO/IEC 12207 - 5.2.2. CMMI – ReqM 1.1.	I/II Dodavatel: L.
4.2.3	**Smlouva** Dodavatel sjedná a uzavře smlouvu s organizací akvizitéra za účelem poskytnutí softwarového produktu nebo služby.	1	2	3	4	ISO/IEC 12207 - 5.2.3. CMMI – ReqM 1.2.	I/II Dodavatel: L.
4.2.4	**Plánování** Dodavatel musí definovat nebo vybrat model životního cyklu SW přiměřený rozsahu, důležitosti a složitosti projektu. Do modelu životního cyklu musí být vybrány a zobrazeny procesy, činnosti a úlohy aplikovaných mezinárodních standardů / pravidel. Dodavatel musí zpracovat a vést plány řízení projektu. *Pozn.: Aplikace tohoto cíle je omezena obsahem kontraktu mezi dodavatelem a akvizitérem. Proto by tento cíl měl být sladěn se 4.3.3. Možný obsah plánu řízení je uveden např. v ISO/IEC 12207.*	1	2	3	4	ISO/IEC 12207. ED-109/DO 278 - 3.1. ED-12B/DO 178B - 4. IEC 61508 - 1-6. CMMI – PP 1.3, 2.7.	I/II Dodavatel: L.

ED-153	Cíl pro zajištění bezpečnosti SW	SWAL				Normy	Odpovědnost
4.2.5	**Proces dodání – realizace a kontrola** Dodavatel musí zavést a realizovat plán řízení projektu. Dodavatel musí monitorovat a kontrolovat postup prací a kvalitu SW produktů nebo služeb v průběhu celého životního cyklu kontraktu.	1	2	3	4	ISO/IEC 12207. ED-109/DO 278 - 3.9, tab. A-9. ED-12B/DO 178B - 4.6. IEC 61508 - 1-6.2.2. CMMI - PMC 1, SAM 2.2.	I/II Dodavatel: L.
4.2.6	**Přezkoumání a hodnocení** Dodavatel musí koordinovat činnosti přezkoumání vyplývající z kontraktu, styky (rozhraní) a komunikaci s organizací akvizitéra. Dodavatel musí vykonávat činnosti při zabezpečování kvality. *Pozn.: Dodavatel by měl provádět neformální schůzky, akceptační přezkoumání a testování, společná přezkoumání (metodika např. viz ISO/IEC 12207, čl. 6.6) a prověrky (metodika např. viz ISO/IEC 12207, čl. 6.7) s akvizitérem podle toho, jak je specifikováno v kontraktu a plánech projektu. Dodavatel by měl vykonávat ověřování a validaci (např. v souladu s ISO/IEC 12207, čl. 6.4 a 6.5). Dodavatel by měl umožnit akvizitérovi přístup k zařízením dodavatele.*	1	2	3	4	ISO/IEC 12207. IEC 61508 - 1-6.2. CMMI - a) PMC 1.5, 1.6, 1.7, b) PPQA, PI 3.4 Ver., Val.	I/II Dodavatel: L.
4.2.7	**Dodání** Dodavatel musí poskytnout akvizitérovi pomoc k podpoře dodaného SW produktu nebo služby. *Pozn.: Rozsah pomoci specifikovat v kontraktu (např. pomoc při akceptačním přezkoumání a testování SW, kompletace a dodávka SW, úvodní a další výcvik a podpora, atd.).*	1	2	3	4	ISO/IEC 12207. IEC 61508 - 1-6.2. CMMI - a) PI 3.4, SAM 2.4.	I/II Dodavatel: L.
4.3.1	**Analýza systémových požadavků** Specifikace systémových požadavků musí min. popisovat: **(4.3.1.1)** Funkce a schopnosti systému. **(4.3.1.2)** Požadované výkonnostní, organizační a uživatelské požadavky **(4.3.1.3)** Požadavky na bezpečnost (safety), ochranu (security), ergonomii, rozhraní, požadavky na provoz a údržbu, navrhovaná omezení a požadavky na validaci (potvrzení zkouškou).	1	2	3	4	ISO/IEC 12207. ED-109/DO 278 - 2, 2.2. ED-12B/DO 178B - 2.1, 2.2. IEC 61508 - 1-7.6, 2-7.2,2-7.9. CMMI - RD 1.1, 2, 2.1, 2.2, 2.3, 3, 3.1, 3.2, REQM 1.4, 1.5.	I/II ANSP: C/A, dodavatel: L.

ED-153	Cíl pro zajištění bezpečnosti SW	SWAL				Normy	Odpovědnost
4.3.2	**Návrh systému** Systémové požadavky musí být stanoveny pro HW, SW, personál a postupy. *Pozn.: Např. výkonnost, fyzické charakteristiky a podmínky prostředí, pod kterými má SW pracovat, externí rozhraní SW, kvalifikační požadavky, specifikace bezpečnosti zahrnující údaje, které se vztahují k metodám provozování a údržby, k vlivu prostředí a ohrožení personálu, specifikace inženýrství lidského faktoru (ruční operace, interakce člověk-stroj, chybování), definice dat a požadavky databáze, požadavky na instalaci a provoz SW, uživatelská dokumentace, požadavky uživatele na provoz a výkon a údržbu, atd.*	1	2	3	4	ISO/IEC 12207. ED-109/DO 278 - 2.1, 2.2. ED-12B/DO 178B - 2.3. IEC 61508 - 2-7.4. CMMI - RD 2.2, REQM 1.4, TS 2.1, 2.2.	I/II ANSP: C/A, dodavatel: L.
4.3.3	**Proces vývoje – implementace** Životní cyklus SW musí odpovídat rozsahu, významu a složitosti projektu a musí být součástí procesu řízení konfigurace. Musí zahrnovat minimálně: • kritéria pro ukončení činnosti/ fáze pro každou činnost / fázi, • společný technický přezkum pro každou činnost / fázi. Normy, metody, nástroje a počítačové programovací jazyky se zvolí a použijí dle úrovně zajištění SW (SWAL). *Pozn.: Implementační proces zahrnuje definici životního cyklu, výstupní dokumentace, řízení konfigurace, problémy SW produktů, definice prostředí, plán vývoje, COTS.*	1	2	3	4	ISO/IEC 12207. ED-109/DO 278 – 3.1 Tab. A-1, A-3. ED-12B/DO 178B – 5.1, 5.5, 11.6, 11.9, 11.10. IEC 61508 – 3-7.2. CMMI – RD 2.1, 2.3, 3.3, TS 2.1, REQM 1.4.	I/II ANSP: C/A, dodavatel: L.
4.3.4	**Analýza požadavků na SW** Projektant musí stanovit a dokumentovat SW požadavky, použité SW standardy/pravidla, jak je definováno v 4.3.9 a 4.3.10. SW požadavky musí jako minimum: **(4.3.4.1)** Specifikovat funkční chování SW, kapacitu, přesnost, časovou výkonnost SW zdroje používaného na cílovém HW robustnost vůči nestandardním stavům, toleranci k přetížení. **(4.3.4.2)** Být kompletní a správné. **(4.3.4.3)** Vyhovovat systémovým požadavkům. **(4.3.4.4)** Identifikovat rozsah konfiguračních/adaptačních dat.	1	2	3	4	ISO/IEC 12207. ED-109/DO 278 - 3.2 Tab. A-2, A-3. ED-12B/DO 178B - 5.1, 5.5, 11.6, 11.9, 11.10. IEC 61508 - 3-7.2. CMMI - RD 2.1, 2.3, 3.3, TS 2.1, REQM 1.4.	I/II ANSP: C/A, dodavatel: L.

ED-153	Cíl pro zajištění bezpečnosti SW	SWAL				Normy	Odpovědnost
4.3.5	**Návrh architektury SW** Projektant musí transformovat požadavky na SW do architektury, která popisuje strukturu jeho nejvyšší úrovně a identifikuje SW složky. *Pozn. Rozsah tohoto cíle je vymezení nejvyšší úrovně SW architektury, vrcholové úrovně návrhu rozhraní, definování SW integrace a definování kritérií SW architektury.*	1	2	3	4	ISO/IEC 12207. ED-109/DO 278 - 3.2 Tab. A-2. ED-12B/DO 178B - 5.2, 5.5, 11.7, 11.10. IEC 61508 - 3-7.4. CMMI - TS 1.1, 1.3. 2.1, 2.2, 2.3, RD 2.2, REQM 1.4, PI 2.1.	I/II ANSP: C/A, dodavatel: L.
4.3.6	**Proces vývoje – detailní návrh SW** Projektant musí vytvořit detailní návrh pro každou SW položku (část) programového vybavení s použitím standardů / pravidel návrhu SW.	1	2	3	4	ISO/IEC 12207. ED-109/DO 278 - 3.2 tab. A-2, 3.5 Tab. A-5, 3.6 Tab. A-6, 3-7 tab. A-7. ED-12B/DO 178B - 5.2,5.3, 5.5, 11.7, 11.8, 11.10, 11.11. IEC 61508 - 3-7.4. CMMI - TS 2.1. 2.2, 2.3, 3.1, Ver., REQM 1.4.	I/II ANSP: C/A, dodavatel: L.
4.3.7	**Proces vývoje – Integrace SW** Musí být vypracován plán integrace pro integraci softwarových jednotek a položek do softwaru. Plán musí zahrnovat požadavky na testování, procedury, data, odpovědnost a časový plán. Plán musí být dokumentován. *Pozn.: Obsahem tohoto cíle je vytvoření plánu integrace SW, definice integrace SW, uživatelské příručky, příprava validace SW, hodnocení (evaluace) integrace SW (částečně).*	1	2	3	4	ISO/IEC 12207. ED-109/DO 278 – 3.1 tab. A-1. ED-12B/DO 178B – 5.4. IEC 61508 – 3-7.4. CMMI – PI 1, 1.1, 1.3, 3.2, 3.3, Ver. 1.3, GP 2.2, 2.3, 3.1, PI GP 2.2, 2.3, 3.1, TS 2.1, 3.1, 3.2, PP 3.1, REQM 1.4.	I/II ANSP: C/A, dodavatel: L.
4.3.8	**Proces vývoje – instalace SW** Musí být vypracován plán integrace pro instalaci SW produktu v cílovém prostředí tak, jak je určeno v kontraktu. Musí být určeny a musí být dostupné zdroje a informace nutné pro instalaci SW produktu.	1	2	3	4	ISO/IEC 12207. IEC 61508 – 1-7.9, 1-7.13. CMMI – PI 1, PP 2, PI GP 2.2, 2.3, 3.1, PI 3.4.	I/II ANSP: C/A, dodavatel: L.

ED-153	Cíl pro zajištění bezpečnosti SW	SWAL				Normy	Odpovědnost
4.3.9	**Definice standardů/pravidel** Plán vývoje Projektant musí vypracovat plány pro řídící aktivity procesu vývoje. Plány musí jako minimum zahrnovat specifikaci standardů / pravidel, metody, nástroje, činnosti a odpovědnosti spojené s vývojem a validací (potvrzení zkouškou) všech požadavků, včetně bezpečnosti. Bude-li nutné, mohou být vytvářeny oddělené plány. Tyto plány musí být dokumentovány a realizovány.	1	2	3	4	ISO/IEC 12207. ED-109/DO 278 - 3.1 Tab. A-1, A-2, pro COTS 4.1.4.2., 3.2 tab. A-2, A-3, A-4, 3-6 tab. A-6, 3-7 tab. A-7. ED-12B/DO 178B - 4.1, 4.2, 4.4, 4.5, 5.3, 5.4.3, 5.5, 6.4.3, 11.2, 11.6 až 11.11. IEC 61508 - 3-7.1.2.6, 3-7.4, 3 Annex A, B, 4.4, 3-7.2.2. CMMI – TS, TS 3.1, PP 2.4, IPM 1.1, GP 2.2, 2.3, 3.1, RD, REQM 1.4, PI 1.2.	I/II ANSP: C/A, dodavatel: L.
4.3.10	**Standardy/pravidla - Plán vývoje SW** Projektant musí identifikovat:					ISO/IEC 12207. ED-109/DO 278 - 3.1 Tab. A-1, 3.2 tab. A-2, A-3, A-4, 3-6 tab. A-6, 3-7 tab. A-7. ED-12B/DO 178B - 4.1, 4.2, 4.4, 4.5, 5.3 až 5.5, 6.4.3, 11.2, 11.6, 11.7, 11.8, 11.10, 11.11. IEC 61508 - 3-7.1.2.6 Annex A, B, 3-7.4, 3-7.2.2. CMMI – TS, TS 3.1, PP 2.4, IPM 1.1, GP 2.2, 2.3, 3.1, RD, REQM 1.4, PI 1.2.	I/II ANSP: C/A, dodavatel: L.
	(4.3.10.1) Požadavky standardů / pravidel na SW (minimálně v rozsahu cíle 4.3.4).	1	2	3	4		
	(4.3.10.2) Standardy / pravidla pro návrh SW.	1	2	3	4		
	(4.3.10.3) Standardy / pravidla pro kódování SW.	1	2	3	4		
	(4.3.10.4) Odkazy na standardy / pravidla pro dříve vyvinutý SW, včetně SW COTS, pokud jsou tyto standardy / pravidla odlišná.	1	2	3	4		
4.3.11	**Řízení požadavků na vývoj - Vývojové prostředí SW** Projektant musí definovat vybrané vývojové prostředí SW z hlediska: **(4.3.11.1)** Vybraných požadavků metod vývoje, procedur a nástrojů (jestliže existují), které budou používány. **(4.3.11.2)** HW platformy pro nástroje (pokud je nějaká), která bude použita. *Pozn.: Metody jsou např. SADT (funkční modelování/návrh), SART (SADT for Real-Time), OOD (objektově orientovaný návrh), atd.*	1	2	3	4	ISO/IEC 12207. ED-109/DO 278 - 3.1 Tab. A-1, 3.2 tab. A-2, A-3, A-4. ED-12B/DO 178B - 4.1, 4.2, 4.4, 4.5, 11.6. IEC 61508 - 3-7.1.2.6 Annex A, B, 3-7.4.4, 3-7.2.2. CMMI - PP 2.4, IPM 1.1, GP 2.2, 2.3, 3.1, RD.	I/II ANSP: C/A, dodavatel: L.

ED-153	Cíl pro zajištění bezpečnosti SW	SWAL				Normy	Odpovědnost
4.3.12	**Použití specifikovaných nástrojů** Musí být použity nástroje požadované specifikací. *Pozn.: Projektant vybírá, přizpůsobuje a použije ty normy a metody, nástroje a počítačové programovací jazyky, které jsou dokumentovány, a jsou vhodné a zavedené v organizaci, pokud není v kontraktu uvedeno jinak.*	1	2	3	4	ISO/IEC 12207. ED-109/DO 278 - 3.1 Tab. A-1, 3.2 tab. A-2, A-3, A-4. ED-12B/DO 178B - 4.4, 4.5, 11.1, 11.2, 11.6 IEC 61508 - 3-7.1.2.6, Annex A, B, 3-7.4, 3-7.2. CMMI - PP 2.4, IPM 1.1, GP 2.2, 2.3, 3.1, RD.	I/II ANSP: C/A, dodavatel: L.
4.3.13	**Řízení zdrojů** **(4.3.13.1)** Pro účely bezpečnosti musí být specifikována nezbytná rezerva s ohledem na využití zdrojů (paměť, výkon CPU, ovladače, atd.).	1	2	3	4	ISO/IEC 12207. ED-109/DO 278 - 3.2 tab. A-2, 3.6 tab.A-6. ED-12B/DO 178B - 5.2, 5.4, 5.5, 11.7, 11.10. IEC 61508 - 3-7.4, 3-7.5. CMMI - TS 1.1,1.3, 2.1, 2.2, RD 2.2, REQM 1.4, PI 2.1, 1.3.	I/II ANSP: C/A, dodavatel: L.
	(4.3.13.2) Rezerva musí být měřitelná nebo ověřitelná s cílem vyhovění specifikaci.	1	2	3	4		
	(4.3.13.3) Pokud více SW sdílí stejné zdroje, pak musí být rezerva hodnocena na systémové úrovni.	1	2	3	4		
4.3.14	**Zdůvodnění volby návrhu** Projektant musí definovat real-time vlastnosti SW položek na úrovni návrhu architektury. Musí být definován soubor následujících vlastností: **(4.3.14.1)** Run-time úkoly a aspekty (priority, události, komunikace, atd.). **(4.3.14.2)** Přerušení (priority, řízení zpoždění, dohledování SW, atd.). **(4.3.14.3)** Ošetření chyb (mechanismus detekce a obnovení, atd.). **(4.3.14.4)** Správa dat (mechanismy ochrany a zablokování, atd.). **(4.3.14.5)** Spuštění/zastavení (výměna dat během těchto fází).	1	2	3	4	ISO/IEC 12207. ED-109/DO 278 – 3.1 Tab. A-1, 3.2 tab. A-2, 3.6 tab. A-6. ED-12B/DO 178B – 4.4, 4.5, 5.2, 5.4, 5.5, 11.7. IEC 61508 – 3-7.1.2.6, Annex A, B, 3-7.4, 3-7.5. CMMI – PP 2.4, IPM 1.1, GP 2.2, 2.3, 3.1, TS 2.1, 2.2, REQM 1.4, PI 2.1, 1.3.	I/II ANSP: C/A, dodavatel: L.
4.3.15	**Sledovatelnost:** Projektant musí zajistit sledovatelnost (návaznost) mezi:					ISO/IEC 12207. ED-109/DO 278 - 3.1 Tab. A-1, 3.2 tab. A-2, A-3, 3-7 tab. A-7. ED-12B/DO 178B - 4.1, 4.3, 5.2, 5.3, 5.5, 11.6 až 11.11. IEC 61508 - 3-7.1.2.7, 2.1.1, 2-7.2.2, 2-7.4, 3-7.2.2, 3-7.4. CMMI - GP 2.2, 3.1, REQM 1.4, 1.5, RD 3, TS 2.1, 2.2, 3.1, PI 2.1.	I/II ANSP: C/A, dodavatel: L.
	(4.3.15.1) Systémovými a SW požadavky.	1	2	3	4		
	(4.3.15.2) SW požadavky a návrhem SW (úroveň návrhu architektury SW položek).	1	2	3	4		
	(4.3.15.3) Návrhem architektury SW a kódem.	1	2	3	4		
	(4.3.15.4) Kódem a spustitelnou aplikací.	1	2	3	4		

ED-153	Cíl pro zajištění bezpečnosti SW	SWAL				Normy	Odpovědnost
4.3.16	**Proces vývoje - ověření/kritéria přechodu** **(4.3.16.1)** Projektant musí popsat procesy životního cyklu SW použité v projektu, včetně přechodových kritérií pro procesy vývoje SW.	1	2	3	4	ISO/IEC 12207. ED-109/DO 278 - 3.1 Tab. A-1, 2, 3, 4.1.4.2, 5.1. ED-12B/DO 178B - 3, 2.2, 4.1, 4.2, 4.3, 11.1, 11.2. IEC 61508 - 3-7.1.2.1 až 3-7.1.2.5, CMMI - PP 1.3, 2.1, PP 2, 2.1, PMC, PMC 1.1, IPM 1.1, 1.3, 1.4, GP 2.2, 2.3, 3.1.	I/II ANSP: C/A, dodavatel: L.
	(4.3.16.2) Všechny základní informace z fáze životního cyklu SW potřebné pro správnou činnost v další fázi musí být dostupné a ověřené. *Pozn.: Viz také kritéria hodnocení pro specifikaci, návrh, kód, testování a integraci.*	1	2	3	4		
	(4.3.16.3) Přechodová kritéria pro všechny fáze musí být definována.	1	2	3	4		
	(4.3.16.4) Musí být definována přechodová kritéria pro analýzu požadavků a verifikační fáze.	1	2	3	4		
4.3.17	**Nástroje pro návrh - Vývojové prostředí SW** Používá-li se nástroj pro navrhování SW, pak projektant musí identifikovat vybrané vývojové prostředí s ohledem na: • Zvolené metody, postupy a nástroje (pokud existují), které mají být použity. • Hardwarové platformy pro nástroje (pokud existují), které mají být použity.	1	2	3	4	ISO/IEC 12207. ED-109/DO 278 – 3.1 Tab. A-1. ED-12B/DO 178B – 11.1, 11.2. IEC 61508 – 3-7.4.4. CMMI – PP 2.4, GP 2.2, 2.3, 3.1.	I/II ANSP: C/A, dodavatel: L.
4.3.18	**Použití nástrojů pro návrh** Musí být použit nástroj pro navrhování SW.	1	2	3	4	ISO/IEC 12207. ED-109/DO 278 – 3.1 Tab. A-1. ED-12B/DO 178B – 11.1, 11.2. IEC 61508 – 3-7.4.4. CMMI – PP 2.4, GP 2.2, 2.3, 3.1.	I/II ANSP: C/A, dodavatel: L.
4.3.19	**Prostředí pro generování kódu** **(4.3.19.1) Vývojové prostředí SW** Projektant musí identifikovat vybrané softwarové vývojové prostředí, s ohledem na: • Programovací jazyky, nástroje kódování, kompilátory, editory a zavaděče, které mají být použity. • Hardwarové platformy pro nástroje, které mají být použity.	1	2	3	4	ISO/IEC 12207. ED-109/DO 278 – 3.1 Tab. A-1, 3.7 Tab. A-7. ED-12B/DO 178B – 4.4, 4.5.5.3, 5.5, 11.2, 11.8, 11.11. IEC 61508 – 3-7.1.2.6, Annex A, B, 3-7.4.4. CMMI – PP 2.4, IPM 1.1, GP 2,2, 2.3, 3.1, TS 3.1, ReqM 1.4.	I/II ANSP: C/A, dodavatel: L.
	(4.3.19.2) Programovací jazyky Výběr vhodných programovacích jazyků musí být odpovídat požadované úrovní zajištění SW.	1	2	3	4		

ED-153	Cíl pro zajištění bezpečnosti SW	SWAL				Normy	Odpovědnost
	(4.3.19.3) Výběr překladačů Musí být definován způsob použití překladačů (compiler).	1	2	3	4		
	(4.3.19.4) Validace nástrojů pro vývoj SW Musí být definováno prostředí pro validaci (potvrzení zkouškou) nástrojů pro vývoj SW.	1	2	3	4		
4.3.20	**Omezení kvůli složitosti** Úroveň složitosti (stejně jako vybraná kritéria definující tuto složitost) musí být definována a měřena. *Pozn.: Proces návrhu SW, proces kódování, sledovatelnost, standardy pro návrh SW, standardy pro kódování SW, zdrojový kód, atd.*	1	2	3	4	ED-12B/DO 178B - 5.2, 5.3, 5.5, 11.7, 11.8, 11.11. IEC 61508 - 3-7.2.2, 3-7.4. CMMI - RD 3.3, REQM 1.4, TS 2.1, 2.2, 3.1, 3.2, PI 1, 2.1, PI GP 2.2, 3.1, PP 3.1.	I/II ANSP: C/A, dodavatel: L.
4.4.1	**Proces provozování – Implementace procesu** Provozní postupy musí být definovány a realizovány. *Pozn.: Provozní dokumentace pro výkon činností a úloh, postupy pro odhalování a řešení problémů, postupy pro testování SW v provozním prostředí, postupy pro údržbu, atd.*	1	2	3	4	ISO/IEC 12207 – 5.4.1. IEC 61508 – 1-7.15.	I/II ANSP: L, dodavatel: C *(Může dodat provozní postupy pro SW.)*.
4.4.2	**Určené provozní prostředí** SW musí být provozován v prostředí určeném uživatelskou dokumentací. *Pozn.: Mělo by se prokázat, že jakékoli použití nastavení SW (např. výběr parametrů uživatelem, přístup do databáze, změna konfiguračního souboru, atd.) dle specifikace SW povede vždy k bezpečnému provozu. Za tímto účelem je vhodné definovat metodiku, pomocí které se uvedený požadavek ověří.*	1	2	3	4	ISO/IEC 12207 – 5.4.3. IEC 61508 - 1-7.15.	I/II ANSP: L, dodavatel: C *(Může dodat provozní postupy pro SW.).*
4.4.3	**Podpora uživatele** Provozovatel musí poskytnout výcvik uživatelům, je-li to relevantní.	1	2	3	4	ISO/IEC 12207 – 5.4.4.	I/II ANSP: L, dodavatel: C *(Může dodat provozní postupy pro SW.).*.

ED-153	Cíl pro zajištění bezpečnosti SW	SWAL				Normy	Odpovědnost
4.4.4	**Provoz SW** Musí být definovány a realizovány postupy pro provoz softwaru (včetně konfiguračních / adaptačních dat, které byly ověřeny a validovány). *Poznámka: Pokud se použije jiná sada dat pro adaptaci / konfiguraci SW, musí být považována za změnu systému.*	1	2	3	4	ISO/IEC 12207– 5.4.3. IEC 61508 – 1-7.15.	I/II ANSP: L, dodavatel: C *(Může dodat provozní postupy pro SW.)*.
4.4.5	**Sledování výkonnosti** Musí existovat přístup ke sledování výkonnosti SW v souladu s přidělenou SWAL.	1	2	3	4	N/A	I/II ANSP: L, dodavatel: C *(Může dodat provozní postupy pro SW.).*
4.5.1	**Proces údržby** **Implementace procesu údržby** Proces údržby musí být definován a prováděn. Údržba zasahující do SW musí podléhat procesu posouzení a zmírnění rizika.	1	2	3	4	ISO/IEC 12207. IEC 61508 - 1-6.2.1, I-7.7, I-7.15. CMMI – PP 2.	I/II ANSP: L, dodavatel: C *(Může dodat postupy údržby pro SW.).*
4.5.2	**Potvrzení přiřazení SWAL** Vliv na přijatelnost rizika problému nebo úpravy, jak stanovuje proces řešení problémů, musí být potvrzen prostřednictvím procesu údržby. *Pozn.: Proces řešení problémů popsán např. v ISO/IEC 12207.* *Proces údržby popsán např. v ISO/IEC 12207.*	1	2	3	4	N/A	I/II ANSP: L, dodavatel: C *(Může dodat postupy údržby pro SW.).*
4.5.3	**Dodržení SWAL** Při provádění údržby musí správce SW zajistit, že každá aktivita údržby je provedena v souladu s přiděleným SWAL. *Pozn. To znamená, že kromě procesu údržby jsou aplikovány ale i další procesy.*	1	2	3	4	ISO/IEC 12207. IEC 61508 – 7.8, I-7.16. CMMI – CM 1.3, 3.2.	I/II ANSP: L, dodavatel: C *(Může dodat postupy údržby pro SW.).*

ED-153	Cíl pro zajištění bezpečnosti SW	SWAL				Normy	Odpovědnost
4.5.4	**Migrace SW** Správce musí definovat postup pro migraci změněného SW a jeho uvedení do provozu. Musí být provedena analýza rizik v rámci migrace SW. *Pozn.: Pojem migrace lze vysvětlit takto: Jedná se v podstatě o přenos definovaných dat z jednoho systému do druhého.*	1	2	3	4	ISO/IEC 12207. CMMI – PI 3.4.	I/II ANSP: L, dodavatel: C *(Může dodat postupy údržby pro SW.).*
4.5.5	**Vyřazení SW** Plán vyřazení SW musí být definován před ukončením jeho provozu. Musí být provedena analýza rizik pro proces vyřazení SW. *Pozn.: Plán by např. mohl obsahovat tyto položky: zastavení podpory produktu a připojené dokumentace, archivace SW a dokumentace, odpovědnost za jakoukoliv budoucí zbývající spornou otázku podpory, přechod na nový SW produkt, přístup k archivovaným kopiím dat.*	1	2	3	4	ISO/IEC 12207. IEC 61508 – 1-7.17	I/II ANSP: L, dodavatel: C *(Může dodat postupy údržby pro SW.).*
5.1.1	**Proces dokumentování – implementace procesu** Musí být vyvinut, dokumentován a implementován plán identifikující dokumenty, které se mají zavést během životního cyklu SW produktu. *Pozn.: Dokumenty mohou obsahovat např. tyto informace: název, účel, distribuční list, postupy a odpovědnost za vstupy, vývoj, přezkoumání, modifikaci, odsouhlasení, výrobu, uložení, distribuci a řízení konfigurace, časový plán pro předběžné a konečné verze, atd.*	1	2	3	4	ISO/IEC 12207. ED-109/DO 278 – 3.1 tab. A-1. ED-12B/DO 178B – 4.3, 11. IEC 61508 – 1-5.1, I-5.2. CMMI – GP 2.2, 3.1, PP 2.3, 2.7, CM 1.1.	I/II ANSP: A, dodavatel: L.
5.1.2	**Proces dokumentování – návrh a vývoj** Každý identifikovaný dokument musí být vytvořen v souladu s aplikovatelnými normami / pravidly pro řízení dokumentace. *Pozn.: Normy definují formát dokumentu, popis obsahu, číslování stran, umístění obrázků a tabulek, označení vlastnictví a ochrany, atd. Řízení dokumentů je uvedeno např. v ISO 9001.*	1	2	3	4	ISO/IEC 12207. ED-12B/DO 178B - 11. IEC 61508 - 1-5.2, I-Annex A. CMMI – PP 2.3, PMC 1.4.	I/II ANSP: C/A, dodavatel: L.

ED-153	Cíl pro zajištění bezpečnosti SW	SWAL				Normy	Odpovědnost
5.1.3	**Proces dokumentování – výroba** Dokumenty musí být vytvořeny a vedeny v souladu s plánem. Dokumenty mohou být v papírové podobě, elektronické podobě nebo v jiné formě. Originály dokumentů musí být uloženy v souladu s požadavky na uchovávání záznamů, požadavky ochranu, údržbu a pořizování kopií.	1	2	3	4	ISO/IEC 12207. ED-109/DO 278 – 3.2 tab. A2, A2.1, A2.2, pro COTS 4.1.2. ED-12B/DO 178B – 4.3, 5.1, 11, 11.9. IEC 61508 - 1-5.2, I-Annex A, 7.2.2. CMMI – RD 2.1, 2.3, PMC 1.4, TS 2.1, 2.2, 3.1, PI 1.1, 1.3, 3.4, CM 1.3.	I/II ANSP: C/A, dodavatel: L.
5.1.4	**Proces dokumentování – údržba** U těch dokumentů, které podléhají řízení konfigurace, musí být modifikace těchto dokumentů řízena v souladu s procesem řízení konfigurace (viz cíl 5.2).	1	2	3	4	ISO/IEC 12207. ED-109/DO 278 – 3.8 tab. A-8. ED-12B/DO 178B – Annex A. CMMI –PMC 1.4.	I/II ANSP: C/A, dodavatel: L.
5.2.1	**Implementace procesu řízení konfigurace** Musí být zpracován plán řízení konfigurace. Musí jako minimum zahrnovat: **(5.2.1.1)** Činnosti řízení konfigurace. **(5.2.1.2)** Postupy a časový plán pro vykonávání těchto činností. **(5.2.1.3)** Organizace odpovědné za vykonávání těchto činností a jejich vztah k jiným organizacím jako např. organizace pro vývoj nebo údržbu SW. **(5.2.1.4)** Řízení kontroly prostředí v životním cyklu SW (nástroje použité pro vývoj nebo ověření SW). **(5.2.1.4)** Definice řízení kontroly dat v životním cyklu SW (každý výstup, týkající se ujištění o bezpečnosti SW). Plán musí být dokumentován, řízen v rámci procesu řízení konfigurace a realizován.	1	2	3	4	ISO/IEC 12207. ED-109/DO 278 – 3.1 tab. A-1, 3.8 Tab. A-8, pro COTS 4.1.7 tab. 4-3. ED-12B/DO 178B – 7.1, 11.4. IEC 61508 - 1-6.2.1. CMMI - CM, 1.2, CM, GP 2.2, 2.4. 3.1.	*Vývoj:* I/II ANSP: A, dodavatel: L. *Provoz, údržba:* I/II ANSP: L.

ED-153	Cíl pro zajištění bezpečnosti SW	SWAL				Normy	Odpovědnost
5.2.2	**Identifikace konfigurace** Pro identifikaci SW a jeho verzí určených ke kontrole během projektu musí být stanoveno schéma. Pro každou verzi SW musí být jako minimum identifikováno následující: **(5.2.2.1)** Základní dokumentace (baseline). **(5.2.2.2)** Reference verzí. **(5.2.2.3)** Seznam zpráv o problémech (ty, které jsou již vyřešeny (stabilní), stabilní ve specifické verzi a doposud otevřené). **(5.2.2.4)** Další identifikační detaily. Aby položky byly konfiguračně identifikovány, musí být identifikovány spolu s jejich úrovní řízení konfigurace.	1	2	3	4	ISO/IEC 12207. ED-109/DO 278 - 3.8 Tab. A-8. ED-12B/DO 178B - 5.4.3, 7.2.1, 7.2.2. IEC 61508 – 6.2.3 c). CMMI - PMC 2.1, 2.2, 2.3, CM 1.1, 2.1, 2.2, 1.3, PI 3.4.	*Vývoj:* I/II ANSP: A, dodavatel: L. *Provoz, údržba:* I/II ANSP: L.
5.2.3	**Kontrola konfigurace** Musí být provedeno: **(5.2.3.1)** Identifikace a záznam požadavků na změny. **(5.2.3.2)** Analýza a zhodnocení změn. **(5.2.3.3)** Schválení nebo zamítnutí požadavků. **(5.2.3.4)** Implementace, ověření a release modifikovaného SW. Záznam o prověření musí existovat pro každou modifikaci, důvod pro modifikaci a ověření modifikace musí být doložitelné. Musí být prováděna kontrola a audit všech přístupů ke kontrolovanému SW, kterými se ovládají z hlediska bezpečnosti nebo ochrany kritické funkce.	1	2	3	4	ISO/IEC 12207. ED-109/DO 278 – 3.8 tab. A-8. ED-12B/DO 178B – 7.2.2, 7.2.3 až 7.2.9, 5.4.3. IEC 61508 – 6.2.3. CMMI - CM, 1.3, 2, 3, CM, GP 2.6.	*Vývoj:* I/II ANSP: A, dodavatel: L. *Provoz, údržba:* I/II ANSP: L.
5.2.4	**Evidence stavu konfigurace** Musí být připraveny záznamy o řízení a zprávy o stavu, které ukazují stav a historii kontrolovaného SW včetně základny Zprávy o stavu musí zahrnovat počet změn v projektu, poslední verze SW, identifikátory release, počet release a porovnání release.	1	2	3	4	ISO/IEC 12207. ED-109/DO 278 – 3.8 tab. A-8. ED-12B/DO 178B – 7.2.6. IEC 61508 – 6.2.3. CMMI – CM 3.1.	*Vývoj:* I/II ANSP: A, dodavatel: L. *Provoz, údržba:* I/II ANSP: L.

ED-153	Cíl pro zajištění bezpečnosti SW	SWAL				Normy	Odpovědnost
5.2.5	**Hodnocení konfigurace** Musí být stanovena a zajištěna: • úplnost funkcí SW ve srovnání s požadavky na něj kladenými, • fyzická úplnosti SW (zda jeho návrh a kód odráží aktuální technický popis).	1	2	3	4	ISO/IEC 12207. ED-109/DO 278 – 3.8 tab. A-8. ED-12B/DO 178B – 7.2.4. IEC 61508 – 6.2.3. CMMI – CM 3.2.	*Vývoj:* I/II ANSP: A, dodavatel: L. *Provoz, údržba:* I/II ANSP: L.
5.2.6	**Řízení a dodávka release** Proces dodávky a release (vydání) SW musí existovat a musí být dokumentován. Release (vydání) a dodávka SW produktů a dokumentace se musí formálně kontrolovat. Kopie kódu a dokumentace musí být udržovány po celý život SW produktu. *Pozn.: Kód a dokumentace obsahující funkce kritické pro bezpečnost nebo ochranu by měly být ošetřovány, ukládány, baleny a dodávány v souladu s politikou zainteresovaných organizací.*	1	2	3	4	ISO/IEC 12207. ED-109/DO 278 – 3.8 tab. A-8. ED-12B/DO 178B – 7.2.7, 7.2.8, 5.4.3. IEC 61508 – 6.2.3. CMMI – CM 1.2, 2.	*Vývoj:* I/II ANSP: A, dodavatel: L. *Provoz, údržba:* I/II ANSP: L.
5.2.7	**Použití nástrojů pro řízení konfigurace** Pro řízení konfigurace SW musí být používán vhodný nástroj (postup).	1	2	3	4	N/A	*Vývoj:* I/II ANSP: A, dodavatel: L. *Provoz, údržba:* I/II ANSP: L.
5.2.8	**Schválení nástrojů pro řízení konfigurace** Akvizitér musí schválit vybraný nástroj řízení konfigurace SW.	1	2	3	4		
5.2.9	**Řízení konfigurace SW jednotky** Řízení konfigurace SW musí být prováděno na úrovni SW jednotky.	1	2	3	4		
5.2.10	**Sledovatelnost řízení konfigurace** Data životního cyklu SW (každý výstup) musí být dohledatelná mezi verzemi. Všechna data v životním cyklu SW musí být dohledatelná k verzi SW, která je provozována.	1	2	3	4	N/A	*Vývoj:* I/II ANSP: A, dodavatel: L. *Provoz, údržba:* I/II ANSP: L.

ED-153	Cíl pro zajištění bezpečnosti SW	SWAL				Normy	Odpovědnost
5.2.11	**Řízení konfigurace na úrovní zdrojového kódu** Řízení konfigurace SW musí být provedeno na úrovni zdrojového kódu SW.	1	2	3	4	N/A	*Vývoj:* I/II ANSP: A, dodavatel: L. *Provoz, údržba:* I/II ANSP: L.
5.3.1	**Proces zajištění kvality - implementace procesu** Musí být zaveden proces zajišťování kvality přizpůsobený projektu. Cíle procesu zabezpečení kvality musí být stanoveny tak, aby zajistily, že SW produkty a procesy využívané pro poskytování těchto SW produktů budou v souladu se stanovenými požadavky a budou se dodržovat stanovené plány. Musí být zpracován, dokumentován, implementován a udržován plán pro vedení činností a úloh v procesu zabezpečování kvality pokrývající životní cyklus SW. *Pozn.: Metodika procesu zajišťování kvality např. viz ISO 9001 v platném znění.*	1	2	3	4	ISO/IEC 12207. ED-109/DO 278 – 3.1 tab. A-1. ED-12B/DO 178B – 8.1, 8.2, 11.5. IEC 61508 –7.1.2.2, 1-6.2.5, I-8. CMMI – PPQA GP 2.2, 3.1.	I/II ANSP: A, dodavatel: L.
5.3.2	**Proces zajištění kvality – zabezpečování produktu** Musí být zajištěno, že všechny plány (definované v normě ED-153, nebo stanovené metodikou dodavatele a v ANSP SMS) jsou definovány, vzájemně se shodují a jsou naplňovány tak, jak je požadováno. Musí být provedeno přezkoumání shody SW.	1	2	3	4	ISO/IEC 12207. ED-109/DO 278 – 3.1 tab. A-1, 3.9 tab. A-9. ED-12B/DO 178B – 8.3. CMMI – GP 2.9, PPQA 2.	I/II ANSP: A, dodavatel: L.
5.3.3	**Proces zajištění kvality – zabezpečování procesu** Musí být zajištěno, že procesy životního cyklu SW (dodání, vývoj, provozování, údržba a podpůrné procesy včetně zajištění kvality) využívané pro projekt jsou v souladu s kontraktem / smlouvou a dodržují plány.	1	2	3	4	ISO/IEC 12207. ED-109/DO 278 - 3.9 tab. A-9. ED-12B/DO 178B – 8.2. CMMI – GP 2.9, PPQA 1.	I/II ANSP: A, dodavatel: L.

ED-153	Cíl pro zajištění bezpečnosti SW	SWAL				Normy	Odpovědnost
5.4.1	**Ověřování implementace procesu** Musí být zaveden proces ověřování (verifikace) SW. Výstup z procesu ověřování musí být zdokumentován a distribuován zainteresovaným stranám. *Pozn.: Měly by být určeny cílové činnosti životního cyklu SW a SW produkty vyžadující ověřování. Pro cílové činnosti a SW produkty jsou poté vybrány činnosti ověřování a úlohy (např. ověřování kontraktu, procesu, požadavků, návrhu, kódu, integrace, dokumentace) zahrnující metody, techniky a nástroje provedení úloh. Na základě určených úloh je vytvořen plán ověřování (viz 5.4.2), který mimo jiné obsahuje i postupy pro zasílání zpráv o ověřování akvizitérovi a ostatním zainteresovaným stranám.*	1	2	3	4	ISO/IEC 12207. ED-109/DO 278 – 3.1 tab. A-1, 3.4, 3.5, 3.7, 3-7 tab. A-7, 3.10 tab. A-10. ED-12B/DO 178B – 2.7, 6, 6.1, 11.3. IEC 61508 – 7.4.1.5, 7.9.2, 1-7.4, 1-7.6, 1-7.8, 1-7.18, I-7.14, 2-7.7.2.3, II-7.7.2. CMMI – GP 2.2, 3.1, Ver. 1, 2, 3, RD 3.3, 3.5, REQM 1.5, Val 1.3, 2.	I/II ANSP: A, dodavatel: L.
5.4.2	**Plán ověřování** Musí být definován plán ověřování (verifikace). Plán musí obsahovat činnosti životního cyklu a SW produkty podléhající ověřování, požadované úlohy ověřování pro každou činnost životního cyklu a SW produkt a příslušné zdroje, odpovědnosti a časový plán. Tento plán musí dále obsahovat postupy pro zasílání zpráv o ověřování akvizitérovi a ostatním zainteresovaným stranám s uvedením opatření, která mají být přijata každou stranou. *Pozn.: Plán ověřování může obsahovat popis různých typů testování v jednotlivých fázích životního cyklu SW (FAT, SAT, testování software. Cíle týkající se ověření konfiguračních / adaptačních dat mohou být rozšířeny v provozním procesu (viz cíle 4.4.X). Strategie pro ověření vhodné kombinace konfiguračních / adaptačních by ale měla být součástí plánu ověřování.*	1	2	3	4	ISO/IEC 12207. ED-109/DO 278 - 3.1 tab. A-1, 2.1, 3.3 tab. A-3, 3.4 tab. A-4, 3.7 tab. A-7, 3.9 tab. A-9, 3.10 tab. A-10. ED-12B/DO 178B – 2.2, 2.3, Annex A, 6.1, 11.3. IEC 61508 - 7.4.1.5, 7.9.2, 1-7.4, 1-7.6, 1-7.18. CMMI – GP 2.2, 2.3, 3.1, Ver. 1, Ver. 1.3, 2, 3, PP 1.3, PMC 1, 2, IPM 1.3, 1.4, 2, CM 2.1, PPQA 1, SAM 1.2, REQM 1.1, 1.3, RD 3.3 až 3.5, PMC GP 2.2, 2.4, 3.1, 2.7.	I/II ANSP: A, dodavatel: L
5.4.3	**Verifikace požadavků na SW** **(5.4.3.1)** Musí být ověřeno, že požadavky na SW jsou správné a úplné.	1	2	3	4	ISO/IEC 12207. ED-109/DO 278 - 3.1 tab. A-1 3.2 tab. A-2, 3.3 tab. A-3,3.5 tab. A-5. ED-12B/DO 178B – Annex A-3 až Annex A-7, 6.1, 6.2, 6.3, 6.4 IEC 61508 - 7.9.2, 1-7.15. CMMI – Ver. 3, Val 2, PI 3.4.	I/II ANSP: A, dodavatel: L.
	Požadavky na SW musí být ověřeny (verifikovány) vzhledem k tomu, zda:						
	(5.4.3.2) Funkční chování implementovaného SW je v souladu s požadavky na SW.	1	2	3	4		
	(5.4.3.3) Výkony v čase implementovaného SW jsou v souladu s požadavky na SW.	1	2	3	4		
	(5.4.3.4) Se SW požadavky shodují, jsou proveditelné a ověřitelné.	1	2	3	4		

ED-153	Cíl pro zajištění bezpečnosti SW	SWAL				Normy	Odpovědnost
	(5.4.3.5) Odolnost implementovaného SW vůči abnormálním provozním podmínkám/stavům vyhovují požadavkům na SW.	1	2	3	4		
	(5.4.3.6) Externí rozhraní vyhovují požadavkům na SW.	1	2	3	4		
	(5.4.3.7) Vnitřní neporušenost SW vyhovuje požadavkům na SW.	1	2	3	4		
	(5.4.3.8) Implementovaný SW vyhovuje kompatibilitě s HW/SW vlastnostmi cílového počítače (časové odezvy, vstup/výstupní HW, provoz na cílovém HW).	1	2	3	4		
	(5.4.3.9) Jsou přizpůsobeny požadavkům SW standardů/ pravidel.	1	2	3	4		
	(5.4.3.10) Použité algoritmy jsou přesné a správné.	1	2	3	4		
	(5.4.3.11) Kapacita implementovaného SW vyhovuje požadavkům na SW.	1	2	3	4		
	(5.4.3.12) Tolerance k přetížení implementovaného SW vyhovuje požadavkům na SW.	1	2	3	4		
5.4.4	**Ověřování integrace:** Integrace musí být ověřována minimálně se zřetelem na tato kritéria:					ISO/IEC 12207. ED-109/DO 278 - 3.1 tab. A-1, 3.5 tab. A-5. ED-12B/DO 178B – Annex A-3 až Annex A-7, 6.2, 6.3, 6.4 IEC 61508 - 7.9.2. CMMI –Ver. 1, 2, 3, PI 3.1, 3.2, PI GP 2.9.	I/II ANSP: A, dodavatel: L.
	(5.4.4.1) SW komponenty byly úplně a správně integrovány do každé SW položky.	1	2	3	4		
	(5.4.4.2) SW jednotky byly úplně a správně integrovány do každé SW položky.	1	2	3	4		
	(5.4.4.3) HW položky, SW položky a ruční operace byly úplně a správně integrovány do systému.	1	2	3	4		
	(5.4.4.4) Integrační úlohy byly vykonány v souladu s plánem integrace.	1	2	3	4		
	Pozn.: Příklady kritérií pro ověřování jsou: • *Přivedená a načítaná data a mapování paměti.* • *Řízení dat a spojování.* • *Nesprávná adresace HW, přeplnění paměti.* • *Chybějící SW komponenty.*						

ED-153	Cíl pro zajištění bezpečnosti SW	SWAL				Normy	Odpovědnost
5.4.5	**Ověřování návrhu** Aby se při hodnocení ověřila architektura SW a uživatelská dokumentace, musí výsledky testů zahrnovat: **(5.4.5.1)** Externí konzistenci se systémovými požadavky (HW-SW kompatibilita). **(5.4.5.2)** Interní konzistenci (tok dat a jeho řízení). **(5.4.5.3)** Pokrytí požadavků SW návrhu. **(5.4.5.4)** Shodu návrhu se standardy/pravidly pro návrh SW. **(5.4.5.5)** Vhodnost norem testování a použitých metod. **(5.4.5.6)** Shodu s očekávanými výsledky. **(5.4.5.7)** Proveditelnost testování návrhu SW. **(5.4.5.8)** Proveditelnost údržby (provoz a údržba). **(5.4.5.9)** Kritéria ověřování, podle kterých bude posuzováno dokončení ověření. Výsledky hodnocení musí být zdokumentovány. *Pozn.: Shoda by měla být ověřena podle definovaných přechodových kritérií mezi fázemi životního cyklu SW (přidělení SWAL pro vývojový proces).*	1	2	3	4	ISO/IEC 12207 – 5.3.7, 6.4.2. ED-109/DO 278 - 3.1 tab. A-1, 3.4 tab. A-4, 3.6 tab. A-6, 3.7 tab. A-7, 3.5 tab. A-5. ED-12B/DO 178B – Annex A-3 až Annex A-7, 6.2, 6.3, 6.4, 5.3, 5.5, 11.8, 11.11. IEC 61508 – 7.4, 7.9.2. CMMI –Ver. 1, 2, 3, TS 1.1, 2.1, 1.3, 3.1, REQM 1.4, TS GP 2.2, 2.3,3.1.	I/II ANSP: A, dodavatel: L.
5.4.6	**Ověřování podrobného návrhu** Při hodnocení (evaluaci) softwarového kódu a výsledků ověřování (verifikace) musí být vzato v úvahu: **(5.4.6.1)** Externí konzistence se systémovými požadavky (HW - SW kompatibilita). **(5.4.6.2)** Vnitřní konzistence mezi detailními požadavky návrhu. **(5.4.6.3)** Ověření pokrytí detailního návrhu položky. **(5.4.6.4)** Shoda kódu se standardy/pravidly. **(5.4.6.5)** Ověření pokrytí struktury software (deklarace pokrytí). *Pozn. Ověření může být provedeno pomocí zkoušky, analýzy, demonstrace nebo kombinací uvedeného v průběhu celého životního cyklu SW.* **(5.4.6.6)** Vhodnost metod kódování a použitých standardů/ pravidel. **(5.4.6.7)** Proveditelnost ověření (verifikace) SW kódu. **(5.4.6.8)** Proveditelnost údržby. Výsledky hodnocení (evaluace) musí být dokumentovány.	1	2	3	4	ISO/IEC 12207. ED-109/DO 278 - 3.1 tab. A-1, 3.5 tab. A-5, 3-6.3, 3.6 tab. A-6, 3.7 tab. A-7. ED-12B/DO 178B – Annex A-3 až Annex A-7, 6.2, 6.3, 6.4, 5.3, 5.5, 11.8, 11.11. IEC 61508 – 7.4, 7.9.2. CMMI –Ver. 1, 2, 3, TS 3.1, REQM 1.4.	I/II ANSP: A, dodavatel: L.

ED-153	Cíl pro zajištění bezpečnosti SW	SWAL	Normy	Odpovědnost
5.4.8	**Ověřování kódu** Spustitelný kód a výsledky ověřování musí být vyhodnoceny na základě níže uvedených kritérií: **(5.4.8.1)** Vnější shoda s kódem SW (např. Vytváří překladač příslušný spustitelný nebo objektový kód?). **(5.4.8.2)** Vnitřní shoda mezi exe požadavky (např.: Vytváří překladač vždy stejný spustitelný nebo objektový kód pro stejné zdroje?). **(5.4.8.3)** Ověření překladu zdrojového kódu softwaru do objektového kódu (např.: Vytváří překladač další a nepotřebný spustitelný nebo objektový kód, jako je třeba „mrtvý spustitelný kód“?). *Pozn.: Mrtvý kód je zbytečný, nefunkční kód, který by měl být odstraněn. Opakem mrtvého kódu je živý, operační kód.* **(5.4.8.4)** Proveditelnost ověření spustitelnosti. **(5.4.8.5)** Ověření struktury SW (MC/DC) *Pozn.: The modified condition/decision coverage (MC/DC) = Zdrojový kód metriky pro měření kvality testovací sady. MC / DC se používá v letectví při vývoji software dle DO-178B a DO-178C pro zajištění testování nejkritičtějšího softwaru (Úroveň A).* Výsledky hodnocení musí být dokumentovány.	1 2 3 4	ED-109/DO 278 - 3.6 tab. A-6. ED-12B/DO 178B – Annex A-6. CMMI –Ver. 3, TS 3.1, REQM 1.4.	I/II ANSP: A, dodavatel: L.
5.4.9	**Ověřování dat** Datové struktury, specifikované v průběhu detailního návrhu musí být ověřeny na: **(5.4.9.1)** Kompletnost (dokončení). **(5.4.9.2)** Vlastní shodu. **(5.4.9.3)** Ochranu proti změně nebo deformaci.	1 2 3 4	ED-109/DO 278 - 3.2 tab. A-2. ED-12B/DO 178B – Annex A-6. IEC 61508 – 7.9.2. CMMI –Ver. 1.3, 2, TS 3.1, PI Ver., Val.	I/II ANSP: A, dodavatel: L.
5.4.10	**Sledovatelnost:** Jako minimum musí být ověřena sledovatelnost (návaznost) mezi:		N/A	I/II ANSP: A, dodavatel: L.
	(5.4.10.1) Systémovými požadavky a SW požadavky.	1 2 3 4		
	(5.4.10.2) SW požadavky a návrhem SW architektury.	1 2 3 4		
	(5.4.10.3) Architekturou SW a prováděcím projektem.	1 2 3 4		
	(5.4.10.4) Prováděcím projektem a strojovým kódem.	1 2 3 4		

ED-153	Cíl pro zajištění bezpečnosti SW	SWAL	Normy	Odpovědnost
	(5.4.10.5) Důkazy ověření a požadavky na SW.	1 2 3 4		
	(5.4.10.6) Důkazy o zajištění bezpečnosti a verzí nasazovaného SW.	1 2 3 4		
5.4.11	**Měření složitosti** Musí být prokázáno analýzou opatření a uplatňováním nápravných opatření, že naměřená složitost je ve vymezené prahové hodnotě. Pokud hodnota překračuje limity (je třeba definovat), musí být poskytnuta odůvodnění.	1 2 3 4	N/A	I/II ANSP: A, dodavatel: L.
5.4.12	**Ověřování a výsledky procesu ověřování:** Testovací případy, postupy a výsledky musí být ověřovány takto:		ISO/IEC 12207. ED-109/DO 278 - 3.5 tab. A-5, 3.6 tab. A-6, 3.7 tab. A-7. ED-12B/DO 178B – Annex A-7, 5.3, 6.3, 6.4 IEC 61508 – 7.4, 7.7, 1-5.2, 1-7.8, I-7.14, 2-7.7. CMMI –Ver. 1, 2, 3, Val 2, TS 2.1, 3.1, REQM 1.4, Ver. GP 2.9, PI GP 2.8, 2.9, CM 3, GP 2.6.	I/II ANSP: A, dodavatel: L.
	(5.4.12.1) Postupy ověřování jsou správné a úplné a rozdíly jsou odůvodněny.	1 2 3 4		
	(5.4.12.2) Výsledky ověření jsou správné a úplné a rozdíly jsou odůvodněny.	1 2 3 4		
	(5.4.12.3) Ověření testovacích případů pro požadavky na SW, souvisejících postupů a výsledků je správné a úplné, a rozdíly jsou odůvodněny.	1 2 3 4		
	(5.4.12.4) Ověření testovacích případů pro návrh SW (úroveň architektury), souvisejících postupů a výsledků je správné a úplné, a rozdíly jsou odůvodněny.	1 2 3 4		
	(5.4.12.5) Ověření testovacích případů pro návrh SW (podrobný návrh), souvisejících postupů a výsledků je správné a úplné, a rozdíly jsou odůvodněny.	1 2 3 4		
	(5.4.12.6) Ověření testovacích případů pro integraci SW, souvisejících postupů a výsledků je správné a úplné, a rozdíly jsou odůvodněny.	1 2 3 4		
	(5.4.12.7) Ověření testovacích případů dat SW, souvisejících postupů a výsledků je správné a úplné.	1 2 3 4		
	(5.4.12.8) Ověření postupů ověřování sledovatelnosti a výsledků je správné a úplné a rozdíly jsou odůvodněny.	1 2 3 4		
5.4.13	**Ověřování procesu načítání a release SW** Procesy pro načtení a release (vydání) SW musí být ověřeny.	1 2 3 4	N/A	I/II ANSP: A, dodavatel: L.

ED-153	Cíl pro zajištění bezpečnosti SW	SWAL				Normy	Odpovědnost
5.6.1	**Proces společného přezkoumání - implementace procesu** Periodická přezkoumání musí být prováděna v předem stanovených termínech (bodech) podle toho, jak je specifikováno v plánech projektu. Výsledky přezkoumání musí být dokumentovány a distribuovány zainteresovaným stranám. *Pozn.: Ad hoc přezkoumání mohou být prováděna, jestliže to považuje za nutné kterákoliv ze stran. Problémy zjištěné při přezkoumání by měly být zaznamenány a měly by vstoupit do procesu řešení problémů. Strany by se měly shodnout na výsledcích přezkoumání.*	1	2	3	4	ISO/IEC 12207. ED-109/DO 278 – 3.9 tab. A-9. ED-12B/DO 178B – 6, 8.3. IEC 61508 –1-6.2, 1-7.18. CMMI – PP 2.1, 2.6, PMC 1.6, 1.7.	I/II ANSP: A, dodavatel: L.
5.6.2	**Proces společného přezkoumání – přezkoumání na úrovni projektu** Stav projektu musí být hodnocen ve vztahu k aplikovaným plánům projektu, časovým plánům, normám, směrnicím a kritériím přechodu. *Pozn.: Výsledek přezkoumání by měl být diskutován oběma stranami a měl by poskytnout podklady pro zajištění pokroku v činnostech podle plánu založeném na zhodnocení činnosti nebo stavu SW, udržení celkové kontroly projektu prostřednictvím přidělování zdrojů, změny směrování projektu nebo určení potřeby pro alternativní plánování a zhodnocení a řízení rizikových faktorů, které mohou ohrozit úspěch projektu.*	1	2	3	4	ISO/IEC 12207. ED-109/DO 278 – 3.9 tab. A-9. ED-12B/DO 178B – 4.6, 8.2. IEC 61508 –1-6.2, 7.3.2. CMMI – PP 2.1, 2.6, PMC 1, 1.6, 1.7.	I/II ANSP: A, dodavatel: L.
5.6.3	**Proces společného přezkoumání – technická přezkoumání** Technická přezkoumání musí být prováděna s cílem zhodnotit uvažované SW produkty nebo SW služby. *Pozn.: A také za účelem podání důkazu, že SW produkty nebo SW služby jsou kompletní, jsou ve shodě s normami a specifikacemi, změny jsou do nich zaváděny správným způsobem a ovlivňují pouze ty oblasti, které jsou identifikovány v procesu řízení konfigurace, dodržují příslušné časové plány, jsou připraveny pro další činnost a vývoj, provoz nebo údržba jsou vykonávány podle plánů, časových plánů, norem a směrnic.*	1	2	3	4	ISO/IEC 12207. ED-109/DO 278 – 3.9 tab. A-9. ED-12B/DO 178B – 6, 8.3. IEC 61508 –1-5.2.11, 7.2.2, 7.3.2, 7.4. CMMI – PP 2.1, 2.6, PMC 1, 1.6, 1.7.	I/II ANSP: A, dodavatel: L.

ED-153	Cíl pro zajištění bezpečnosti SW	SWAL				Normy	Odpovědnost
5.7.1	**Proces prověrky (audity)** Audity se musí konat v předem stanovených termínech, jak je stanoveno v plánu projektu, nebo na zvláštní žádost. Po dokončení auditu musí být výsledky auditu zdokumentovány a poskytnuty auditované straně.	1	2	3	4	ISO/IEC 12207. ED-12B/DO 178B – 8.2, 11.19. IEC 61508 –1-6.2.1, 1-7.7.2.1, 7.8.2, 7.15.2. CMMI – GP 2.7, 2.9.	I/II ANSP: C/A, dodavatel: L.
5.7.2	**<u>Audity na úrovni požadavků na SW</u>** Audity na požadavky SW musí být prováděny v předem stanovených termínech: Audity musí určit, zda: • Přezkum akceptace (přijetí) a verifikace požadavků, které jsou stanoveny v dokumentaci, jsou adekvátní pro akceptaci SW. • Data ověření (verifikace) jsou v souladu se specifikací. • SW byl úspěšně ověřen (verifikován) a odpovídá požadavkům. • Zprávy o ověření (verifikaci) jsou správné a rozdíly mezi skutečnými a očekávanými výsledky byly vyřešeny. • Produkt (požadavek SW) a uživatelská dokumentace jsou v souladu s normami/pravidly, jak je definováno. • Činnosti byly provedeny v souladu s platnými požadavky, plány a smlouvami. • Náklady a harmonogramy jsou v souladu s plány.	1	2	3	4	ISO/IEC 12207 – 6.8.2. ED-12B/DO 178B – 8.2. IEC 61508 –6.2.3. CMMI – Ver. 1, 2, 3, TS 3.1, 3.2, PMC 1.1, 2, 3.2, CM 2.1, 3.2, GP 2.9.	I/II ANSP: C/A, dodavatel: L.

ED-153	Cíl pro zajištění bezpečnosti SW	SWAL				Normy	Odpovědnost
5.7.3	**<u>Audity do úrovně architektury SW</u>** Audity musí být prováděny v předem stanovených termínech a na základě specifických požadavků, aby bylo zajištěno, že: • Přezkum přijetí (akceptace) a požadavky verifikace popsané v dokumentaci jsou přiměřené (dostačující) pro přijetí SW. • Data ověření jsou v souladu se specifikací. • Software byl úspěšně ověřen a splňuje jeho požadavky na SW, požadavky na architekturu a detailní požadavky návrhu. • Zprávy z ověření jsou správné a rozdíly mezi skutečnými a očekávanými výsledky byly vyřešeny. • Produkt (požadavky na SW, SW architektura) a uživatelská dokumentace jsou v souladu s normami/ pravidly. • Činnosti byly provedeny v souladu s platnými požadavky, plány a smlouvami. • Náklady a harmonogramy jsou v souladu s plány.	1	2	3	4	ISO/IEC 12207. ED-12B/DO 178B – 8.2. IEC 61508 –6.2.3. CMMI – Ver. 1, 2, 3, TS 3.1, 3.2, PMC 1.1, 2, 3.2, CM 2.1, 3.2, GP 2.9.	I/II ANSP: C/A, dodavatel: L.
5.7.4	**<u>Audity do úrovně zdrojového kódu SW</u>** Audity musí být prováděny v předem stanovených termínech a na základě specifických požadavků, aby bylo zajištěno, že: • Přezkum přijetí (akceptace) a požadavky verifikace popsané v dokumentaci jsou přiměřené (dostačující) pro přijetí SW. • Data ověření jsou v souladu se specifikací. • Software byl úspěšně ověřen a splňuje jeho požadavky na SW, požadavky na architekturu a detailní požadavky návrhu. • Zprávy z ověření jsou správné a rozdíly mezi skutečnými a očekávanými výsledky byly vyřešeny. • Produkt (požadavky na SW, SW architektura, návrh a zdrojový kód) a uživatelská dokumentace jsou v souladu s normami / pravidly. • Činnosti byly provedeny v souladu s platnými požadavky, plány a smlouvami. • Náklady a harmonogramy jsou v souladu s plány.	1	2	3	4	ISO/IEC 12207. ED-12B/DO 178B – 8.2. IEC 61508 –6.2.3. CMMI – Ver. 1, 2, 3, TS 3.1, 3.2, PMC 1.1, 2, 3.2, CM 2.1, 3.2, GP 2.9.	I/II ANSP: C/A, dodavatel: L.

ED-153	Cíl pro zajištění bezpečnosti SW	SWAL				Normy	Odpovědnost
5.7.5	**<u>Audity kvality do úrovně spustitelnosti SW</u>** Audity musí být prováděny v předem stanovených termínech a na základě specifických požadavků, aby bylo zajištěno, že: • Přezkum přijetí (akceptace) a požadavky verifikace popsané v dokumentaci jsou přiměřené (dostačující) pro přijetí SW. • Data ověření jsou v souladu se specifikací. • Software byl úspěšně ověřen a splňuje jeho požadavky na SW, požadavky na architekturu a detailní požadavky návrhu. • Zprávy z ověření jsou správné a rozdíly mezi skutečnými a očekávanými výsledky byly vyřešeny. • Produkt (požadavky na SW, SW architektura, návrh a zdrojový kód a spustitelný soubor) a uživatelská dokumentace jsou v souladu s normami / pravidly. • Vývojové nástroje SW (např. překladače) jsou způsobilé. • Činnosti byly provedeny v souladu s platnými požadavky, plány a smlouvami. • Náklady a harmonogramy jsou v souladu s plány.	1	2	3	4	ISO/IEC 12207. ED-12B/DO 178B – 8.2. IEC 61508 –6.2.3. CMMI – Ver. 1, 2, 3, TS 3.1, 3.2, PMC 1.1, 2, 3.2, CM 2.1, 3.2, GP 2.9.	I/II ANSP: C/A, dodavatel: L.
5.8.1	**Proces pro řešení problémů – implementace procesu** Proces pro řešení problémů (včetně prokázání úspěšného řešení problému) musí být definován pro zvládnutí všech problémů (včetně neshod), které jsou zjištěny v softwarových produktech a činnostech. *Pozn.: Implementace procesu by mohla například zahrnovat vytvoření hodnotící komise.*	1	2	3	4	ISO/IEC 12207. ED-109/DO 278 – 3.8 tab. A-8. ED-12B/DO 178B – 7, 11.17. IEC 61508 – 7.8, 1-6.2.1, I-7.16. CMMI – PMC GP 2.2, 3.1.	I/II ANSP: L, dodavatel: C.
5.8.2	**Proces pro řešení problémů – řešení problému** Pokud byly v softwarovém produktu nebo činnosti zjištěny problémy (včetně neshod), musí být připravena zpráva o problému, kterou se popíše každý zjištěný problém. Zpráva o problému se musí použít jako součást procesu uzavřené smyčky procesu: od detekce problému, přes průzkum, analýzu a řešení problému a jeho příčiny až po detekci trendů v celkové problematice.	1	2	3	4	ISO/IEC 12207. ED-109/DO 278 – 3.8 tab. A-8. ED-12B/DO 178B – 7, 11.17. IEC 61508 – 7.8.2. CMMI – PMC 2 CAR.	I/II ANSP: L, dodavatel: C.

ED-153	Cíl pro zajištění bezpečnosti SW	SWAL				Normy	Odpovědnost
5.8.3	**Proces pro řešení problémů – Účinky na bezpečnost** Musí být provedena analýza zprávy o problému s cílem zjištění: • Zda hlášený problém má bezpečnostní dopad (řízení rizika) a zdali odpovídá přidělenému SWAL. • Zda byla provedena taková nápravná opatření, která mohou prokázat, že bezpečnostně relevantní problémy byly dostatečně zmírněny.	1	2	3	4	ISO/IEC 12207. IEC 61508 – 7.8, 1-7.8, I-7.15. CMMI – REQM 1.3, CM 2.	I/II ANSP: L, dodavatel: C.
5.8.4	**Řízení konfigurace zpráv o problémech** Zprávy o problému musí být považovány za data životního cyklu SW, která spadají pod řízení konfigurace, jak je definováno v cíli 5.2.1. *Pozn.: Metodika popsána např. v ISO/IEC 12207.*	1	2	3	4	ISO/IEC 12207. ED-109/DO 278 – 3.8 tab. A-8. ED-12B/DO 178B – 7.2.3 až 7.2.5. IEC 61508 – 6.2.3. CMMI – CM 2, 3.	I/II ANSP: L, dodavatel: C.
6.1.1	**Proces řízení – implementace procesu** Musí být definován proces řízení přizpůsobený projektu. Výstup procesu řízení musí být dokumentován a distribuován. Odpovědná osoba musí prokázat realizovatelnost procesu kontrolou dostupnosti zdrojů (personál, materiály, technologie a prostředí) požadovaných pro realizaci a řízení procesu, jejich přiměřenosti, vhodnosti, zajištění finančních prostředků a kontrolou toho, že stanovené časové období pro dokončení je dosažitelné.	1	2	3	4	ISO/IEC 12207. CMMI – GP 2.2, 3.1, PP 2.4, 3.2.	I/II ANSP: A, dodavatel: L.
6.1.2	**Proces řízení – plánování** Odpovědná osoba musí připravit plány pro realizaci procesu. Plány spojené s realizací procesu musí obsahovat popis souvisejících činností a úloh a identifikaci SW produktů, které budou poskytovány. Tyto plány musí zahrnovat minimálně následující: • Harmonogramy pro včasné dokončení úloh. • Odhady náročnosti. • Odpovídající zdroje potřebné k provádění úloh. • Přidělení úloh (včetně toho, kdo, co a kdy). • Určení odpovědností. • Kvantifikace projektových rizik souvisejících s úlohami vlastního procesu. • Opatření pro řízení kvality, které mají být použity v průběhu celého procesu. • Náklady spojené s realizací procesu. • Zajištění prostředí a infrastruktury.	1	2	3	4	ISO/IEC 12207. CMMI – all.	I/II ANSP: A, dodavatel: L.

ED-153	Cíl pro zajištění bezpečnosti SW	SWAL				Normy	Odpovědnost
6.1.3	**Proces řízení – realizace a kontrola** Odpovědná osoba musí zahájit implementaci plánu, za účelem splnění cílů a stanovených kritérií, prováděním kontroly v průběhu celého procesu. Odpovědná osoba musí sledovat realizaci procesu a zajišťovat jak interní zprávy o postupu vývoje procesu, tak externí pro akvizitéra SW podle toho, jak je definováno v kontraktu. Odpovědná osoba musí zkoumat, analyzovat a vyřešit problémy zjištěné během provádění celého procesu.	1	2	3	4	ISO/IEC 12207. CMMI – PMC GP 2.8, PMC 1, 2.	I/II ANSP: A, dodavatel: L.
6.1.4	**Proces řízení – Přezkoumání a hodnocení** Odpovědná osoba musí zajistit, že data životního cyklu software jsou hodnocena vůči stanoveným požadavkům. Odpovědná osoba musí ověřit výsledky hodnocení softwarových produktů, činností a úloh dokončených během realizace procesu z hlediska dosažení cílů a dokončení plánů.	1	2	3	4	ISO/IEC 12207. CMMI – REQM 1.5, PMC.	I/II ANSP: A, dodavatel: L.
6.1.5	**Proces řízení – Závěry** Když jsou všechny softwarové produkty, činnosti a úlohy dokončeny, musí odpovědná osoba určit, zda je dokončen proces, a to s ohledem na kritéria specifikovaná v kontraktu nebo příslušné části organizačních postupů. Odpovědná osoba musí zkontrolovat výsledky softwarových produktů, činností a úloh využívaných při dokončení a záznamy o nich. Tyto výsledky a záznamy musí být archivovány ve vhodném prostředí, jak je specifikováno v kontraktu.	1	2	3	4	ISO/IEC 12207. CMMI – IPM 1.3, PMC 1.1, 1.4, 1.6, 1.7, GP 2.8.	I/II ANSP: A, dodavatel: L.
6.2.1	**Proces infrastruktury – implementace procesu** Musí být definována potřebná infrastruktura pro procesy, aby mohly být plněny požadavky procesů (např. vývoj nebo ověřování) s ohledem na aplikované postupy, normy, nástroje a metody. Zřízení infrastruktury musí být plánováno a dokumentováno.	1	2	3	4	ISO/IEC 12207. ED-109/DO 278 - 3.1, tab. A-1. ED-12B/DO 178B - 4.4, 11.2. IEC 61508 - 6.2.3, 7.4.4. CMMI – PP 2, 2.4, GP 2.3.	I/II ANSP: A, dodavatel: L.
6.2.2	**Proces infrastruktury – zřízení infrastruktury** Musí být plánována a dokumentována konfigurace infrastruktury. Musí být přitom uváženy tyto parametry: Funkčnost, výkonnost, provozní bezpečnost (safety), ochrana (security), dostupnost, nároky na prostory, zařízení, náklady a časová omezení.	1	2	3	4	ISO/IEC 12207. ED-109/DO 278 - 3.8, tab. A-8. ED-12B/DO 178B - 4.4, 7.2.9, 11.15. IEC 61508 - 6.2.3, 8.3. CMMI – CM, CM 1.1, GP 2.2, 3.1.	I/II ANSP: A, dodavatel: L.

ED-153	Cíl pro zajištění bezpečnosti SW	SWAL				Normy	Odpovědnost
6.2.3	**Proces infrastruktury – údržba infrastruktury** Infrastruktura musí být udržována, sledována a modifikována podle potřeby k zajištění neustálého plnění požadavků procesů (např. vývoj nebo ověření). Jako součást údržby infrastruktury musí být definován rozsah, v němž infrastruktura podléhá řízení konfigurace.	1	2	3	4	ISO/IEC 12207. ED-109/DO 278 - 3.8, tab. A-8. ED-12B/DO 178B - 7.2.9. IEC 61508 - 6.2.3. CMMI – CM, PMC 1.1.	I/II ANSP: A, dodavatel: L.
6.3.1	**Proces zlepšování – zřízení procesu** Organizace musí vytvořit sadu organizačních procesů pro veškeré procesy životního cyklu SW. Procesy a jejich aplikace v konkrétních případech musí být dokumentovány ve firemní dokumentaci. Podle potřeby musí být stanoveny kontrolní mechanismy procesu za účelem rozvoje, monitorování, kontroly a zlepšování procesu/ů.	1	2	3	4	ISO/IEC 12207. CMMI – OPD 1.3, 2.1, OPD GP 2.6, OPF.	I/II ANSP: A, dodavatel: L.
6.3.2	**Proces zlepšování – posuzování procesu** Musí být definován, dokumentován a uplatňován postup pro posuzování procesů. Záznamy o posouzení musí být uchovávány a udržovány. Organizace musí plánovat a provádět přezkum procesů ve vhodných intervalech za účelem zajištění jejich neustálé vhodnosti a účinnosti s ohledem na výsledky posouzení.	1	2	3	4	ISO/IEC 12207. CMMI – OPF 1.2.	I/II ANSP: A, dodavatel: L.
6.3.3	**Proces zlepšování – zdokonalování procesu** Organizace musí uskutečnit taková zlepšení procesů, která jsou stanovena jako nezbytná na základě posouzení procesů a výsledků přezkumu. Dokumentace procesu musí být aktualizována tak, aby odrážela zlepšení organizačních procesů. *Pozn.: Pro získání porozumění o silných a slabých stránkách místech používaných procesů by se měla sbírat a analyzovat historická, technická a hodnotitelská data.*	1	2	3	4	ISO/IEC 12207. CMMI – OPF 1.3, 2.1, 2.2.	I/II ANSP: A, dodavatel: L.

ED-153	Cíl pro zajištění bezpečnosti SW	SWAL				Normy	Odpovědnost
6.4	**Proces zajištění lidských zdrojů** Proces zajištění lidských zdrojů je procesem pro zajištění a udržení vyškoleného personálu. Akvizice, dodání, vývoj, provoz nebo údržba softwarových produktů jsou do značné míry závislé na poučeném a kvalifikovaném personálu. Např. vývojáři by měli mít základní výcvik v softwarovém managementu a softwarovém inženýrství. Je proto nezbytně nutné, aby školení personálu byla plánována a realizována včas tak, aby vyškolený personál byl k dispozici, kdy SW produkt bude poptáván, dodáván, vyvíjen, provozován nebo udržován. Výcvik zahrnuje použití a přizpůsobení norem/standardů na konkrétní aplikace. *Pozn.: V této části se neřeší školení provozních zaměstnanců odpovědných za provoz SW, ale školení zaměstnanců odpovědných za vývoj a údržbu softwaru.*					N/A	N/A
6.4.1	**Proces zajištění lidských zdrojů – implementace procesu** Musí být prováděn přezkum požadavků projektu tak, aby se zajistilo včasné vyškolení schopných a kvalifikovaných pracovníků požadovaných vedením a technickým štábem. Musí být stanoveny typy a úrovně výcviku a kategorie personálu, který potřebuje výcvik. Musí být zpracován a dokumentován výcvikový plán, který obsahuje adaptační plány *(„postup výcviku od začátku do konce“)*, požadavky na zdroje a úrovně dovedností a znalostí.	1	2	3	4	ISO/IEC 12207. IEC 61508 – 1-6.2.1, I-Annex B. CMMI – PP 2.5, PMC 1.1, GP 2.5, OT 1.1, 1.3.	I/II ANSP: A, dodavatel: L.
6.4.2	**Proces zajištění lidských zdrojů – materiály pro výcvik** Musí být pracovány příručky včetně prezentačních materiálů.	1	2	3	4	ISO/IEC 12207. CMMI – OT 1.4.	I/II ANSP: A, dodavatel: L.
6.4.3	**Proces zajištění lidských zdrojů – implementace plánu výcviku** Plán výcviku musí být implementován. Musí být vedeny a udržovány záznamy o průběhu výcviku.	1	2	3	4	ISO/IEC 12207. IEC 61508 – 1-6.2.2, I-Annex B. CMMI – PP 2.5, OT 2.1, 2.2.	I/II ANSP: A, dodavatel: L.
7.2.1	**Plány COTS** ANSP musí definovat postupy pro akvizici COTS, verifikaci COTS, řízení konfigurace COTS, plány pro zajištění kvality COTS. *Pozn.: Doporučuje se koordinovat proces pro zajištění kvality COTS s dodavatelem COTS.*	1	2	3	4	ED-109/DO 278 – 4.1.9 tab. 4-2. CMMI – SAM GP 2.2, 3.1.	I/II ANSP: A, dodavatel: L.

ED-153	Cíl pro zajištění bezpečnosti SW	SWAL				Normy	Odpovědnost
7.2.2	**Převodní kritéria COTS** ANSP musí definovat převodní kritéria (na základě vztahu mezi procesy pro COTS a odpovídajícími procesy životního cyklu CNS/ATM).	1	2	3	4	ED-109/DO 278 – 4.1.9 tab. 4-2. CMMI – SAM 2.1, TS 2.4, IPM 1.3.	I/II ANSP: A, dodavatel: L. I/II ANSP: A, dodavatel: L.
7.2.3	**Jednotnost COTS plánů** Plány COTS definované dle bodu 7.2.1. musí být v souladu s plány pro ANS SW.	1	2	3	4	ED-109/DO 278 – 4.1.9 tab. 4-2. CMMI – SAM 2.1, TS 2.4.	
7.2.4	**Pokrytí požadavků dosažených COTS** ***Proces ověřování COTS SW*** Je rozšíření procesu ověřování SW popsaného v cíli 5.4.X. Zejména proces akvizice COTS často identifikuje cíle, které mohou být splněné použitím standardních prostředků. Pro cíle, které nemohou být naplněny dostupnými údaji COTS (např. požadavky na jeho vývoj) smí být použity další aktivity, zahrnující alternativní metody, jako je zpětné řízení, které mohou být použity po akceptaci schvalující autoritou. *Pozn.: Musí být prokázáno pokrytí požadavků ANS SW dosažených COTS. Pro splnění tohoto bodu je potřeba nejprve provést definici požadavků na COTS, tzn. určit, do jaké míry jsou požadavky na CNS/ATM relevantní pro COTS – jedná se o jakýsi průnik požadavků CNS/ATM a kapacit COTS. Definici těchto kapacit lze získat z uživ. manuálů, tech. manuálů, tech. specifikací produktu, atd.).*	1	2	3	4	ED-109/DO 278 – 4.1.9 tab. 4-2. CMMI – SAM 2.1, TS 2.4.	I/II ANSP: A, dodavatel: L.
7.2.5	**Životní cyklus COTS** Dostupnost dat životního cyklu COTS musí být stanovena v souladu se SWAL (rozsah dat životního cyklu, která jsou dostupná pro účely ověřování/zajištění).	1	2	3	4	ED-109/DO 278 – 4.1.9 tab. 4-2. CMMI – SAM 2.1, TS 2.4.	I/II ANSP: A, dodavatel: L.
7.2.6	**Odvozené požadavky pro COTS** Musí být definovány odvozené požadavky (požadavky kladené na ANS systém v důsledku používání COTS, nebo požadavky pro potlačení nepotřebných funkcí COTS ovlivňujících systém ANS). *Pozn.: Při používání COTS je možné odvodit další požadavky, které by měly být doplněny k požadavkům na ANS SW. Jedná se např. o požadavky závislé na platformě, omezení použití, procesy přerušení, požadavky na zdroje, atd.*	1	2	3	4	ED-109/DO 278 – 4.1.9 tab. 4-2. CMMI – SAM 2.1, TS 2.4.	I/II ANSP: A, dodavatel: L.

ED-153	Cíl pro zajištění bezpečnosti SW	SWAL				Normy	Odpovědnost
7.2.7	**Kompatibilita COTS s HW** Musí být prokázána kompatibilita COTS s HW, na kterém bude COTS provozován.	1	2	3	4	ED-109/DO 278 – 4.1.9 tab. 4-2. CMMI – TS 2.4, RD 2.2, 3.4.	I/II ANSP: A, dodavatel: L.
7.2.8	**Řízení konfigurace COTS - Identifikace** Musí být stanovena konfigurace COST a datových položek. *Pozn.: Specifický způsob řízení konfigurace pro COTS a datové položky, např. dokumentace SW, úprava dat, atd.*	1	2	3	4	ED-109/DO 278 – 4.1.9 tab. 4-2. CMMI – CM 1.2.	I/II ANSP: A, dodavatel: L.
7.2.9	**Zprávy o problémech COTS** Musí být stanoven postup pro hlášení chyb COTS. *Pozn.: ANSP systém pro hlášení chyb zahrnuje řízení chyb detekovaných v COTS a obousměrný mechanismus podávání zpráv mezi provozovatelem COST a dodavatelem COTS.*	1	2	3	4	ED-109/DO 278 – 4.1.9 tab. 4-2. CMMI – CM 1.1, SAM GP 2.6.	I/II ANSP: A, dodavatel: L.
7.2.10	**Nový release COTS** Instalace nových release COTS musí být řízena. *Pozn.: Možno popsat jako součást systému řízení změn v rámci ANSP. Měla by se provádět analýza dopadu změn na COTS před instalací nových verzí COTS.*	1	2	3	4	ED-109/DO 278 – 4.1.9 tab. 4-2. CMMI – SAM 2.3, CM 1.2.	I/II ANSP: A, dodavatel: L.
7.2.11	**Řízení konfigurace - archivace** Konfigurace COST a datových položek musí být archivována.	1	2	3	4	ED-109/DO 278 – 4.1.9 tab. 4-2. CMMI –CM 2.2.	I/II ANSP: A, dodavatel: L.

ED-153	Cíl pro zajištění bezpečnosti SW	SWAL				Normy	Odpovědnost
7.3 **(COTS)**	Je nutné prokázat způsobilost SW nástrojů (SW tools) v případě, že procesy z této směrnice jsou vyloučeny, redukovány nebo zautomatizovány použitím softwarových nástrojů, aniž by jejich výstupy byly ověřovány tak, jak je specifikováno v popisu procesu ověřování (viz požadavek 7.2.1). Cílem prokázání způsobilosti SW nástrojů je ujištění, že SW nástroj poskytuje míru jistoty alespoň na stejné úrovni jako procesy, které byly vyloučeny (odstraněny), redukovány nebo automatizovány. Ověřovány mohou být pouze deterministické SW nástroje, tzn. programy, které produkují stejný výstup pro stejná vstupní data při provozu ve stejném prostředí. Proces pro prokázání způsobilosti SW nástrojů může být aplikován buď na jeden SW nástroj, nebo na několik SW nástrojů. Softwarové nástroje mohou být klasifikovány jako jeden ze dvou typů: 1. Nástroje pro vývoj softwaru – nástroje, jejichž výstupem je část SW produktu, a mohou tak zanést do SW chyby. **(7.3.1)** Kdykoliv jsou tyto nástroje použity a jejich výstup není ověřen (verifikován), potom musí být tyto nástroje vyvíjeny pro nejvyšší úroveň zajištění produktu (nejvyšší SWAL). Pokud je nástroj pro vývoj softwaru plně verifikován, nemusí být jeho použití ověřováno *(nemusí být prokazována jeho způsobilost)*. 2. Nástroje pro ověřování softwaru – nástroje, které nemohou zanést do SW chyby, ale mohou selhat při jejich odhalování. **(7.3.2)** Kdykoliv jsou tyto nástroje použity a jejich výstup není ověřen (verifikován), potom musí být tyto nástroje ověřovány (prokázána jejich způsobilost) podle ED-12B / DO-178B (kapitola 12.2) a ED-94B / DO-248B. Pokud je nástroj pro ověřování softwaru plně verifikován, nemusí být jeho použití ověřováno *(nemusí být prokazována jeho způsobilost)*.	1	2	3	4	ED-109/DO 278 – 5.2. ED-12B/DO 178B – 12.2. IEC 61508 – 3-7.7.2.7. CMMI – Ver. 1.2.	I/II ANSP: A, dodavatel: L.

Tabulka č.2. *Varianta orientovaná na cíle*

Záměrně nepoužito.

3.2. VARIANTA ORIENTOVANÁ NA PROJEKT

Tato varianta je zaměřená na přiřazení cíle a doložení důkazu pro jednotlivé činnosti projektu v rámci životního cyklu SW.

3.2.1. Legenda k tabulce č.3

- Sloupec „ č.“ – pořadové číslo.
- Sloupec „Název položky“ – definuje činnost.
- Sloupec „číslo cíle“ – jednoznačná identifikace cíle (číslování cílů je plně v souladu s normou ED-153).
- Sloupec „cíl“ - definuje cíl, kterého má být dosaženo.
- Sloupec „SWAL“ – definuje rozdílné nároky odpovídající jednotlivým úrovním zajištění softwaru takto:

Červené pole	Cíle, které musí být dosaženy nezávisle („nezávislým dosažením“ se v případě činností v rámci procesu ověřování softwaru rozumí, že činnosti v rámci procesu ověřování provádí jiná osoba (jiné osoby) než osoba, která ověřovaný prvek vyvinula).
Modré pole	Cíle, které musí být dosaženy.
Zelené pole	Dosažení cílů je na uvážení organizace.
Šedé pole	Není aplikováno.

- Sloupec „Normy“ – obsahuje odkazy na normy, které je možné dále využít při plnění stanovených cílů. Jedná se pouze o doporučení pro využití metodik / postupů vhodných pro zajištění naplnění definovaných cílů. Uvedené normy nemusí být již aktuální, nicméně jimi definované metodiky / postupy jsou pro proces zajištění bezpečnosti SW i nadále využitelné. Organizace může pro prokázání naplnění definovaného cíle využít i jiných norem / standardů, jejichž aplikovatelnost ověří a prokáže v rámci procesu zajištění bezpečnosti SW.
- Sloupec „Odpovědnost“ – obsahuje doporučení pro stanovení odpovědností a povinností pro dodavatele produktu a ANSP. Vychází z varianty 1 a 2 stanovení rolí v kapitole „Definice“ v tomto dokumentu. (viz obrázek č. 1 a č. 2), neboť se předpokládá, že se jedná o nejčastější varianty rozložení rolí. V případě jiného rozložení rolí je nutné vhodně upravit odpovědnosti.

  Stanovení odpovědností v tomto sloupci poté vychází ze dvou scénářů akvizice SW:

  - 1. scénář (I) – SW jako součást funkčního systému: akvizitér stanovuje požadavky vztažené k funkčnímu systému (stanovení provozních operací, požadavky na provozní a servisní personál, požadavky na postupy údržby atd.). V tomto případě definuje dodavatel software požadavky na systém odvozené od

požadavků akvizitéra. Následně pak definuje dodavatel software požadavky na SW.

- 2. scénář (II) – SW jako samostatný prvek: akvizitér stanovuje požadavky přímo na SW. V tomto případě definuje akvizitér software požadavky na systém. Následně pak definuje dodavatel software požadavky na SW odvozené od požadavků akvizitéra.

Použitá symbolika ve sloupci „Odpovědnost“:

- L (lead) – řídí,
- C (contribute) – spolupracuje,
- A (accept) – provádí akceptaci.

Záměrně nepoužito.

č.	Název položky	Číslo cíle	Cíl	SWAL	Normy	Odpovědnost
ČÁST I – PROSTŘEDÍ						
I	Popis systému	**3.1.1**	**Popis systému** Musí být definováno: **(3.1.1.1)** Provozní scénáře (např. HMI: Provozní příručka, která definuje provozní režim a HMI, normální režim, degradační režim). **(3.1.1.2)** SW a systémové funkce. **(3.1.1.3)** Meze (parametry) SW (např. funkční / provozní, časové). **(3.1.1.4)** Externí rozhraní SW.	1 2 3 4	ED-109/DO 278 - 2.2. ED-12B/DO 178B - 2.1. IEC 61508 - I-7.2.1. CMMI - a) RD 1.1, b) RD 3.1, TS 1.2, c) RD 3.2, e) RD 2.3, TS 2.3.	I ANSP: C/A, dodavatel: L. II ANSP: L, dodavatel: C.
		4.1.1	**Proces akvizice - Inicializace** Akvizitér začíná proces akvizice popisem koncepce nebo potřeb akvizice, vývoje, nebo rozšíření systému, softwarového produktu nebo SW služby. Akvizitér musí definovat, analyzovat a schválit systémové požadavky *(např. proti požadavkům uživatele).* Tyto systémové požadavky musí zahrnovat požadavky obchodní, organizační a uživatelské, jakož i požadavky na bezpečnost (safety), ochranu (security) a ostatní kritické požadavky spolu se souvisejícími normami a procedurami pro návrh, testování a shodu. Akvizitér musí připravit, dokumentovat a realizovat akviziční plán. *Pozn.: Aplikace tohoto cíle je omezena obsahem kontraktu mezi dodavatelem a akvizitérem. Proto by tento cíl měl být sladěn se 4.3.3.*	1 2 3 4	ISO/IEC 12207. CMMI – SAM 1.1, 2.1, TS 2.4; RD1.2,2.1, ReqM1.4; GP 2.2, 3.1; ISM GP 2.2, 3.1.	I/II ANSP: L.
		4.3.1	**Analýza systémových požadavků** Specifikace systémových požadavků musí min. popisovat: **(4.3.1.1)** Funkce a schopnosti systému. **(4.3.1.2)** Požadované výkonnostní, organizační a uživatelské požadavky **(4.3.1.3)** Požadavky na bezpečnost (safety), ochranu (security), ergonomii, rozhraní, požadavky na provoz a údržbu, navrhovaná omezení a požadavky na validaci (potvrzení zkouškou).	1 2 3 4	ISO/IEC 12207. ED-109/DO 278 - 2, 2.2. ED-12B/DO 178B - 2.1, 2.2. IEC 61508 - 1-7.6, 2-7.2,2-7.9. CMMI - RD 1.1, 2, 2.1, 2.2, 2.3, 3, 3.1, 3.2, REQM 1.4, 1.5.	I/II ANSP: C/A, dodavatel: L.

č.	Název položky	Číslo cíle	Cíl	SWAL	Normy	Odpovědnost
I	Provozní prostředí	**3.1.2**	**Provozní prostředí** Software a jeho prostředí (fyzické, provozní, kontrolní funkce, legislativní atd.) musí být popsáno dostatečně detailně, aby bylo umožněno uspokojivě provést bezpečnostní úkoly životního cyklu.	1 2 3 4	ED-109/DO 278 – 2.2. ED-12B/DO 178B – 2.1,1. IEC 61508 – I-7.2.1. CMMI – RD 1.1.	I ANSP: C/A, dodavatel: L. II ANSP: L, dodavatel: C.
I	Seznam nástrojů prostředí	**5.2.7**	**Použití nástrojů pro řízení konfigurace** Pro řízení konfigurace SW musí být používán vhodný nástroj (postup).	1 2 3 4	N/A	*Vývoj:* I/II ANSP: A, dodavatel: L. *Provoz, údržba:* I/II ANSP: L.
		6.2.1	**Proces infrastruktury – implementace procesu** Musí být definována potřebná infrastruktura pro procesy, aby mohly být plněny požadavky procesů (např. vývoj nebo ověřování) s ohledem na aplikované postupy, normy, nástroje a metody. Zřízení infrastruktury musí být plánováno a dokumentováno.	1 2 3 4	ISO/IEC 12207. ED-109/DO 278 – 3.1, tab. A-1. ED-12B/DO 178B – 4.4, 11.2. IEC 61508 – 6.2.3, 7.4.4. CMMI – PP 2, 2.4, GP 2.3.	I/II ANSP: A, dodavatel: L.
		6.2.2	**Proces infrastruktury – zřízení infrastruktury** Musí být plánována a dokumentována konfigurace infrastruktury. Musí být přitom uváženy tyto parametry: Funkčnost, výkonnost, provozní bezpečnost (safety), ochrana (security), dostupnost, nároky na prostory, zařízení, náklady a časová omezení.	1 2 3 4	ISO/IEC 12207. ED-109/DO 278 – 3.8, tab. A-8. ED-12B/DO 178B – 4.4, 7.2.9, 11.15. IEC 61508 – 6.2.3, 8.3. CMMI – CM, CM 1.1, GP 2.2, 3.1.	I/II ANSP: A, dodavatel: L.
ČÁST II – SOUVISLOST SE SYSTÉMEM HODNOCENÍ BEZPEČNOSTI						
II	Regulatorní rámec	**3.1.3**	**Regulatorní rámec** Platné regulatorní bezpečnostní cíle a požadavky musí být identifikovány. *Pozn.: Identifikace požadavků z aktuálních dokumentů legislativní báze, tj. z platných nařízení, norem, zákonů, atd.*	1 2 3 4	ED-109/DO 278 – 3.10 Tab. A-10. ED-12B/DO 178B – 2.1.1, 9, 10. IEC 61508 – I-7.2.2.4.	I ANSP: C/A, dodavatel: L. II ANSP: L,

č.	Název položky	Číslo cíle	Cíl	SWAL	Normy	Odpovědnost
II	Aplikovatelné standardy	**3.1.4**	**Aplikovatelné procesy a pokyny** Procesy a pokyny vztahující se k zajištění SW musí být odsouhlaseny dle interních postupů organizace. *Pozn.: Např. v rámci systému řízení dokumentace společnosti.*	1 2 3 4	ISO/IEC 12207. ED-109/DO 278. ED-12B/DO 178B. IEC 61508. CMMI.	dodavatel: C.
II	Výsledek posuzování a zmírňování rizik	**3.0.6**	**Zajištění naplnění požadavků** ANS software musí splňovat požadavky na něj kladené na úrovni jistoty, která je v souladu se SWAL, přidělenou při posuzování a zmírňování rizik (např. PSSA).	1 2 3 4	ED-109/DO 278 – 2.1. ED-12B/DO 178B – 5.1. IEC 61508 – 7.2.	I/II ANSP: A, dodavatel: L.
		4.1.2	**Cíle bezpečnosti procesu řízení rizik** Akvizitér musí určit, jak bezpečný SW potřebuje. Za tím účelem musí provést analýzu nebezpečí (např. FHA) a identifikovat cíle bezpečnosti pro jednotlivá zjištěná rizika.	1 2 3 4	IEC 61508 – 1-7.2, 1-7.3. IEC 61508 – 1-7.4, 1-7.5.	I/II ANSP: L.
		4.1.3	**Požadavky bezpečnosti procesu řízení rizik** Akvizitér musí určit (v průběhu fáze návrhu systému), zda je očekáváno nebo neočekáváno v rámci navrhované architektury dosažení cílů bezpečnosti. Dále musí specifikovat bezpečnostní požadavky včetně přidělení SWAL pro systémové složky.	1 2 3 4	ED-109/DO 278 – 2 ED-12B/DO 178B – 2. IEC 61508 – 1-7.6.	I/II ANSP: L.
II	SW FHA a PSSA	**3.1.5**	**Výstup procesu řízení rizik** Identifikace hodnocení rizik na úrovni systému a identifikace zmírnění musí být znovu posouzena na úrovni softwaru, aby byla zajištěna konsistence s architekturou / návrhem softwaru. *Pozn.: Běžná praxe pro snížení bezpečnostního rizika v návrhu systému je izolace funkcí, které mohou způsobit nebo přispět k selhání systému. Analýza by měla popsat datový tok v systému, aby bylo možné identifikovat, které chyby mohou potenciálně způsobit další negativní reakce. Dále by měly být popsány a řešeny případné konflikty mezi požadavky na ochranu (security) a bezpečnost (safety). Součástí analýzy by měly být i požadavky bezpečnosti v procesu adaptace SW a případné změny SW za provozu systému.*	1 2 3 4	ED-109/DO 278 – 2.2. ED-12B/DO 178B – 2.1.1. IEC 61508 – I-7.	I ANSP: L. II ANSP: L, dodavatel: C.

č.	Název položky	Číslo cíle	Cíl	SWAL	Normy	Odpovědnost
		3.3.1	**Identifikace chyb** Případná selhání musí být identifikována tak, že se zvažují různé způsoby, jak může software selhat a dále tím, že se zvažuje sled událostí, které vedou k výskytu poruchy. Musí být vypracován seznam jednotlivých, následných a společných způsobů selhání. *Pozn.: Návod na společnou analýzu režimu (Common Mode Analysis) lze nalézt v ED-79. V rámci FHA – např. dle metodiky ICAO Doc 9859 Safety Management Manual (SMM).*	1 2 3 4	ED-12B/DO 178B – 2.2, 2.2.2 IEC 61508 – I-7.4.	I/II ANSP: C/A, dodavatel: L.
		3.3.2	**Účinky chyb** Musí být hodnoceny účinky výskytu poruchy. Nebezpečí spojená s výskytem selhání SW musí být identifikována pro vytvoření kompletního seznamu nebezpečí, jež byl iniciovaný během procesu vyhodnocení a zmírnění rizika (např. FHA a další doplnění během PSSA). *Pozn.: Účinky klasifikovat v souladu s PNK (EU) č.1035/2011, čl. 3.2.4. Oddíl 4 Rozpoznání a posouzení závažnosti.*	1 2 3 4	ED-12B/DO 178B – 2.2, 2.2.1. IEC 61508 – I-7.4.	I/II ANSP: C/A, dodavatel: L.
		3.3.3	**Posouzení rizik** Počáteční proces posouzení a zmírnění rizik (např. FHA a další doplnění během PSSA) musí být přezkoumán na základě výsledku z 3.3.1 a 3.3.2. *Pozn.: Proces řízení rizik (identifikace rizik, analýza rizik, návrh nápravných a preventivních opatření, aplikace navržených opatření, hodnocení aplikovatelnosti navržených opatření, hodnocení účinnosti zavedených opatření, atd.).*	1 2 3 4	ED-12B/DO 178B – 2.2.1. IEC 61508 – I-7.5.	I ANSP: L. II ANSP: C/A, dodavatel: L.

č.	Název položky	Číslo cíle	Cíl	SWAL	Normy	Odpovědnost
		3.3.4	**Stanovení požadavků na SW** Požadavky na SW musí „vyhovět“ bezpečnostním cílům, na kterých se SW podílí a být v souladu s bezpečnostními systémovými požadavky. *Pozn.: Definice " vyhovět" musí být vyvinuta jako součást argumentu podporujícího dodržení tohoto cíle. Tato definice by měla zahrnovat dohledatelnost s výše uvedenou úrovní požadavků, prokázat nutnost, dostatečnost, vhodnost a relevanci požadavků k uspokojení výše uvedené úrovně požadavků.* *Jedná se o soulad požadavků na SW se systémovými požadavky v rámci procesu řízení rizik, tzn. např., že snížení rizik na úrovni SW musí zajistit snížení pravděpodobnosti výskytu rizik na úrovni systému.*	1 2 3 4	ED-12B/DO 178B – 2.2.1. IEC 61508 – I-7.6. CMMI – a.1) RD 2.1, 2.2, a.2) TS 2.1, Ver. 1.1, 2.2, 2.3	I/II ANSP: C/A, dodavatel: L.
ČÁST III – PROCES HODNOCENÍ BEZPEČNOSTI SW						
III	Plán pro hodnocení bezpečnosti SW	**3.2.1**	**Přístup k posouzení bezpečnosti SW** Musí být definován celkový přístup k posuzování bezpečnosti softwaru v rámci životního cyklu softwaru. *Pozn.: Plán pro akceptaci SW by měl obsahovat např. popis systému (funkce, HW, SW, architektura, rozhraní, bezpečnost), popis SW, identifikaci předpisové základny včetně postupů pro dokazovány shody, popis životního cyklu SW s definovanými výstupy a odpovědnostmi osob v rámci tohoto cyklu, časový a věcný plán projektu, specifika v rámci procesu, atd.*	1 2 3 4	ED-109/DO 278 – 5.1. ED-12B/DO 178B – 11.1. IEC 61508 – 8.	I/II ANSP: C/A, dodavatel: L.
		3.2.2	**Plán posouzení bezpečnosti SW** Musí být vypracován plán popisující kroky posuzování bezpečnosti softwaru. *Pozn.: Např. volba metodiky, vztahy mezi posuzováním bezpečnosti a životním cyklem SW, dodávka (obsah a datum dodání), řízení rizik projektu ve vztahu k otázkám bezpečnosti, odpovědnosti, osoby, organizace, schéma klasifikace rizik, definice bezpečnostních cílů, metody identifikace rizik (nebezpečí), činnosti pro zajištění bezpečnosti, plánování, zdroje.*	1 2 3 4	ED-109/DO 278 – 5.1 – 3.10 Tab. A-10. ED-12B/DO 178B – 11. IEC 61508 – I-7.8.	I/II ANSP: C/A, dodavatel: L.

č.	Název položky	Číslo cíle	Cíl	SWAL	Normy	Odpovědnost
		6.1.1	**Proces řízení – implementace procesu** Musí být definován proces řízení přizpůsobený projektu. Výstup procesu řízení musí být dokumentován a distribuován. Odpovědná osoba musí prokázat realizovatelnost procesu kontrolou dostupnosti zdrojů (personál, materiály, technologie a prostředí) požadovaných pro realizaci a řízení procesu, jejich přiměřenosti, vhodnosti, zajištění finančních prostředků a kontrolou toho, že stanovené časové období pro dokončení je dosažitelné.	1 2 3 4	ISO/IEC 12207. CMMI – GP 2.2, 3.1, PP 2.4, 3.2.	I/II ANSP: A, dodavatel: L.
		6.1.2	**Proces řízení – plánování** Odpovědná osoba musí připravit plány pro realizaci procesu. Plány spojené s realizací procesu musí obsahovat popis souvisejících činností a úloh a identifikaci SW produktů, které budou poskytovány. Tyto plány musí zahrnovat minimálně následující: • Harmonogramy pro včasné dokončení úloh. • Odhady náročnosti. • Odpovídající zdroje potřebné k provádění úloh. • Přidělení úloh (včetně toho, kdo, co a kdy). • Určení odpovědností. • Kvantifikace projektových rizik souvisejících s úlohami vlastního procesu. • Opatření pro řízení kvality, které mají být použity v průběhu celého procesu. • Náklady spojené s realizací procesu. • Zajištění prostředí a infrastruktury.	1 2 3 4	ISO/IEC 12207. CMMI – vše.	I/II ANSP: A, dodavatel: L.

č.	Název položky	Číslo cíle	Cíl	SWAL	Normy	Odpovědnost
		6.1.3	**Proces řízení – realizace a kontrola** Odpovědná osoba musí zahájit implementaci plánu, za účelem splnění cílů a stanovených kritérií, prováděním kontroly v průběhu celého procesu. Odpovědná osoba musí sledovat realizaci procesu a zajišťovat jak interní zprávy o postupu vývoje procesu, tak externí pro akvizitéra SW podle toho, jak je definováno v kontraktu. Odpovědná osoba musí zkoumat, analyzovat a vyřešit problémy zjištěné během provádění celého procesu.	1 2 3 4	ISO/IEC 12207. CMMI – PMC GP 2.8, PMC 1, 2.	I/II ANSP: A, dodavatel: L.
		6.1.5	**Proces řízení – Závěry** Když jsou všechny softwarové produkty, činnosti a úlohy kompletní, musí odpovědná osoba určit, zda je proces kompletní, a to se zřetelem na kritéria specifikovaná v kontraktu nebo v příslušné části organizačních postupů. Odpovědná osoba musí kontrolovat výsledky softwarových produktů, činností a úloh a záznamy o nich. Tyto výsledky a záznamy musí být archivovány ve vhodném prostředí, jak je specifikováno v kontraktu.	1 2 3 4	ISO/IEC 12207. CMMI – IPM 1.3, PMC 1.1, 1.4, 1.6, 1.7, GP 2.8.	I/II ANSP: A, dodavatel: L.
III	Přezkoumání Plánu pro hodnocení bezpečnosti SW	**3.2.3**	**Přezkoumání plánu posouzení bezpečnosti SW** Plán posuzování bezpečnosti SW by měl být akceptován NSA.	1 2 3 4	ED-109/DO 278 – 5.1 – 3.10 Tab. A-10. ED-12B/DO 178B – 9,10.	I/II ANSP: C/A, dodavatel: L.
		6.1.4	**Proces řízení – přezkoumání a zhodnocení** Odpovědná osoba musí zajistit, že data životního cyklu software jsou hodnocena z hlediska uspokojení požadavků. Odpovědná osoba musí posuzovat výsledky hodnocení SW produktů, činností a úloh dokončených během realizace procesu z hlediska dosažení cílů a dokončení plánů.	1 2 3 4	ISO/IEC 12207. CMMI – REQM 1.5, PMC.	I/II ANSP: A, dodavatel: L.

č.	Název položky	Číslo cíle	Cíl	SWAL	Normy	Odpovědnost
III	Seznam příjemců Plánu pro hodnocení bezpečnosti SW	**3.2.4**	**Distribuce plánu posouzení bezpečnosti SW** Plán posouzení bezpečnosti SW musí být distribuován všem zainteresovaným stranám. *Pozn.: Proces životního cyklu SW zahrnuje např. tyto strany – akvizitér SW, dodavatel SW, projektant SW, provozovatel SW, správce SW, správce/ manažer procesů, nezávislá strana. Tento dokument nedefinuje, kdo jsou zainteresované strany. Zainteresované strany jsou definovány v souladu se schváleným plánem bezpečnosti SW, v souladu se SMS ANSP a v souladu s příslušnými předpisovými bezpečnostními požadavky.*	1 2 3 4	ED-109/DO 278 – 5.1. ED-12B/DO 178B – 9,10.	I/II ANSP: C/A, dodavatel: L.
III	Verifikace a validace	**3.3.1**	**Identifikace chyb** Případná selhání musí být identifikována tak, že se zvažují různé způsoby, jak může software selhat a dále tím, že se zvažuje sled událostí, které vedou k výskytu poruchy. Musí být vypracován seznam jednotlivých, následných a společných způsobů selhání. *Pozn.: Návod na společnou analýzu režimu (Common Mode Analysis) lze nalézt v ED-79. V rámci FHA – např. dle metodiky ICAO Doc 9859 Safety Management Manual (SMM).*	1 2 3 4	ED-12B/DO 178B – 2.2, 2.2.2 IEC 61508 – I-7.4.	I/II ANSP: C/A, dodavatel: L.
		3.4.2	**Ověřování (verifikace) posouzení bezpečnosti SW** SW požadavky musí být v souladu s funkcemi pro zmírnění následků nebezpečí (rizika) a s bezpečnostními cíli rizik. *Pozn.: Stanovení SWAL.*	1 2 3 4	ED-109/DO 278 – 2.1. ED-12B/DO 178B – 2.2.2.	I/II ANSP: C/A, dodavatel: L.
		3.4.3	**Proces zajištění posouzení bezpečností SW** Bezpečnostní posouzení SW musí být provedeno úplně. *Pozn.: V souladu se schváleným bezpečnostním plánem SW, v souladu s ANSP SMS a v souladu s požadavky příslušných bezpečnostních předpisů.*	1 2 3 4	ISO/IEC 12207. ED-109/DO 278 – 3.9 Tab. A-9 ED-12B/DO 178B – 8.	I/II ANSP: C/A, dodavatel: L.

č.	Název položky	Číslo cíle	Cíl	SWAL	Normy	Odpovědnost
		6.3.1	**Proces zlepšování – zřízení procesu** Organizace musí vytvořit sadu organizačních procesů pro veškeré procesy životního cyklu SW. Procesy a jejich aplikace v konkrétních případech musí být dokumentovány ve firemní dokumentaci. Podle potřeby musí být stanoveny kontrolní mechanismy procesu za účelem rozvoje, monitorování, kontroly a zlepšování procesu/ů.	1 2 3 4	ISO/IEC 12207. CMMI – OPD 1.3, 2.1, OPD GP 2.6, OPF.	I/II ANSP: A, dodavatel: L.
		6.3.2	**Proces zlepšování – posuzování procesu** Musí být definován, dokumentován a uplatňován postup pro posuzování procesů. Záznamy o posouzení musí být uchovávány a udržovány. Organizace musí plánovat a provádět přezkum procesů ve vhodných intervalech za účelem zajištění jejich neustálé vhodnosti a účinnosti s ohledem na výsledky posouzení.	1 2 3 4	ISO/IEC 12207. CMMI – OPF 1.2.	I/II ANSP: A, dodavatel: L.
		6.3.3	**Proces zlepšování – zdokonalování procesu** Organizace musí uskutečnit taková zlepšení procesů, která jsou stanovena jako nezbytná na základě posouzení procesů a výsledků přezkumu. Dokumentace procesu musí být aktualizována tak, aby odrážela zlepšení organizačních procesů. *Pozn.: Pro získání porozumění o silných a slabých stránkách místech používaných procesů by se měla sbírat a analyzovat historická, technická a hodnotitelská data.*	1 2 3 4	ISO/IEC 12207. CMMI – OPF 1.3, 2.1, 2.2.	I/II ANSP: A, dodavatel: L.
III	Seznam dokumentů a dokumentace procesu	**5.1.1**	**Proces dokumentování – implementace procesu** Musí být vyvinut, dokumentován a implementován plán identifikující dokumenty, které mají být zavedeny během životního cyklu SW produktu. *Pozn.: Dokumenty mohou obsahovat např. tyto informace: název, účel, distribuční list, postupy a odpovědnost za vstupy, vývoj, přezkoumání, modifikaci, odsouhlasení, výrobu, uložení, distribuci a řízení konfigurace, časový plán pro předběžné a konečné verze, atd.*	1 2 3 4	ISO/IEC 12207. ED-109/DO 278 – 3.1 tab. A-1. ED-12B/DO 178B – 4.3, 11. IEC 61508 – 1-5.1, I-5.2. CMMI – GP 2.2, 3.1, PP 2.3, 2.7, CM 1.1.	I/II ANSP: A, dodavatel: L.

č.	Název položky	Číslo cíle	Cíl	SWAL	Normy	Odpovědnost
		5.1.2	**Proces dokumentování – návrh a vývoj** Každý identifikovaný dokument musí být vytvořen v souladu s aplikovatelnými normami / pravidly pro řízení dokumentace. *Pozn.: Normy definují formát dokumentu, popis obsahu, číslování stran, umístění obrázků a tabulek, označení vlastnictví a ochrany, atd. Řízení dokumentů je uvedeno např. v ISO 9001.*	1 2 3 4	ISO/IEC 12207. ED-12B/DO 178B - 11. IEC 61508 - 1-5.2, I-Annex A. CMMI – PP 2.3, PMC 1.4.	I/II ANSP: C/A, dodavatel: L.
		5.1.3	**Proces dokumentování – výroba** Dokumenty musí být vytvořeny a vedeny v souladu s plánem. Dokumenty mohou být v papírové podobě, elektronické podobě nebo v jiné formě. Originály dokumentů musí být uloženy v souladu s požadavky na uchovávání záznamů, požadavky ochranu, údržbu a pořizování kopií.	1 2 3 4	ISO/IEC 12207. ED-109/DO 278 – 3.2 tab. A2, A2.1, A2.2, pro COTS 4.1.2. ED-12B/DO 178B – 4.3, 5.1, 11, 11.9. IEC 61508 - 1-5.2, I-Annex A, 7.2.2. CMMI – RD 2.1, 2.3, PMC 1.4, TS 2.1, 2.2, 3.1, PI 1.1, 1.3, 3.4, CM 1.3.	I/II ANSP: C/A, dodavatel: L.
		5.1.4	**Proces dokumentování – údržba** U těch dokumentů, které podléhají řízení konfigurace, musí být modifikace těchto dokumentů řízena v souladu s procesem řízení konfigurace (viz cíl 5.2).	1 2 3 4	ISO/IEC 12207. ED-109/DO 278 – 3.8 tab. A-8. ED-12B/DO 178B – Annex A. CMMI –PMC 1.4.	I/II ANSP: C/A, dodavatel: L.
ČÁST IV – POŽADAVKY BEZPEČNOSTI						
I V	SW požadavky bezpečnosti	**3.0.6**	**Zajištění naplnění požadavků** ANS software musí splňovat požadavky na něj kladené na úrovni jistoty, která je v souladu se SWAL, přidělenou při posuzování a zmírňování rizik (např. PSSA).	1 2 3 4	ED-109/DO 278 – 2.1. ED-12B/DO 178B – 5.1. IEC 61508 – 7.2.	I/II ANSP: A, dodavatel: L.
ČÁST V – MODIFIKACE SW						

č.	Název položky	Číslo cíle	Cíl	SWAL	Normy	Odpovědnost
V	Změny	**3.0.12**	**Modifikace SW** Jakákoli změna SW musí vést nejprve k opětovnému posouzení bezpečnostních dopadů této změny na systém, a pak v závislosti na tomto dopadu musí vést k opětovnému posouzení SWAL, přidělenému tomuto SW.	1 2 3 4	ED-109/DO 278 – 4.1.4.2. IEC 61508 – 7.8.	*Vývoj:* I/II ANSP: A, dodavatel: L. *provoz,údržba:* I/II ANSP: L, dodavatel: C.
		4.5.2	**Potvrzení přiřazení SWAL** Vliv na přijatelnost rizika problému nebo úpravy, jak stanovuje proces řešení problémů, musí být potvrzen prostřednictvím procesu údržby. *Pozn.: Proces řešení problémů popsán např. v ISO/IEC 12207, čl. 6.8. Proces údržby popsán např. v ISO/IEC 12207, čl. 5.5.*	1 2 3 4	N/A	I/II ANSP: L, dodavatel: C.
		4.5.4	**Migrace SW** Správce musí definovat postup pro migraci změněného SW a jeho uvedení do provozu. Musí být provedena analýza rizik v rámci migrace SW. *Pozn.: Pojem migrace lze vysvětlit takto: Jedná se v podstatě o přenos definovaných dat z jednoho systému do druhého.*	1 2 3 4	ISO/IEC 12207. CMMI – PI 3.4.	I/II ANSP: L, dodavatel: C.
		5.2.3	**Kontrola konfigurace** Musí být provedeno: **(5.2.3.1)** Identifikace a záznam požadavků na změny. **(5.2.3.2)** Analýza a zhodnocení změn. **(5.2.3.3)** Schválení nebo zamítnutí požadavků. **(5.2.3.4)** Implementace, ověření a release modifikovaného SW. Záznam o prověření musí existovat pro každou modifikaci, důvod pro modifikaci a ověření modifikace musí být doložitelné. Musí být prováděna kontrola a audit všech přístupů ke kontrolovanému SW, kterými se ovládají z hlediska bezpečnosti nebo ochrany kritické funkce.	1 2 3 4	ISO/IEC 12207. ED-109/DO 278 – 3.8 tab. A-8. ED-12B/DO 178B – 7.2.2, 7.2.3 až 7.2.9, 5.4.3. IEC 61508 – 6.2.3. CMMI – CM, 1.3, 2, 3, CM, GP 2.6.	*Vývoj:* I/II ANSP: A, dodavatel: L. *Provoz, údržba:* I/II ANSP: L.

č.	Název položky	Číslo cíle	Cíl	SWAL	Normy	Odpovědnost
		5.2.4	**Evidence stavu konfigurace** Musí být připraveny záznamy o řízení a zprávy o stavu, které ukazují stav a historii kontrolovaného SW včetně základny Zprávy o stavu musí zahrnovat počet změn v projektu, poslední verze SW, identifikátory release, počet release a porovnání release.	1 2 3 4	ISO/IEC 12207. ED-109/DO 278 – 3.8 tab. A-8. ED-12B/DO 178B – 7.2.6. IEC 61508 – 6.2.3. CMMI – CM 3.1.	*Vývoj:* I/II ANSP: A, dodavatel: L. *Provoz, údržba:* I/II ANSP: L.
V	Řešení problému	**4.5.2**	**Potvrzení přiřazení SWAL** Vliv na přijatelnost rizika problému nebo úpravy, jak stanovuje proces řešení problémů, musí být potvrzen prostřednictvím procesu údržby. *Pozn.: Proces řešení problémů popsán např. v ISO/IEC 12207.* *Proces údržby popsán např. v ISO/IEC 12207.*	1 2 3 4	N/A	I/II ANSP: L, dodavatel: C.
		4.5.4	**Migrace SW** Správce musí definovat postup pro migraci změněného SW a jeho uvedení do provozu. Musí být provedena analýza rizik v rámci migrace SW. *Pozn.: Pojem migrace lze vysvětlit takto: Jedná se v podstatě o přenos definovaných dat z jednoho systému do druhého.*	1 2 3 4	ISO/IEC 12207. CMMI – PI 3.4.	I/II ANSP: L, dodavatel: C.
		5.2.3	**Kontrola konfigurace** Musí být provedeno: **(5.2.3.1)** Identifikace a záznam požadavků na změny. **(5.2.3.2)** Analýza a zhodnocení změn. **(5.2.3.3)** Schválení nebo zamítnutí požadavků. **(5.2.3.4)** Implementace, ověření a release modifikovaného SW. Záznam o prověření musí existovat pro každou modifikaci, důvod pro modifikaci a ověření modifikace musí být doložitelné. Musí být prováděna kontrola a audit všech přístupů ke kontrolovanému SW, kterými se ovládají z hlediska bezpečnosti nebo ochrany kritické funkce.	1 2 3 4	ISO/IEC 12207. ED-109/DO 278 – 3.8 tab. A-8. ED-12B/DO 178B – 7.2.2, 7.2.3 až 7.2.9, 5.4.3. IEC 61508 – 6.2.3. CMMI – CM, 1.3, 2, 3, CM, GP 2.6.	*Vývoj:* I/II ANSP: A, dodavatel: L. *Provoz, údržba:* I/II ANSP: L.

č.	Název položky	Číslo cíle	Cíl	SWAL	Normy	Odpovědnost
		5.2.4	**Evidence stavu konfigurace** Musí být připraveny záznamy o řízení a zprávy o stavu, které ukazují stav a historii kontrolovaného SW včetně základny Zprávy o stavu musí zahrnovat počet změn v projektu, poslední verze SW, identifikátory release, počet release a porovnání release.	1 2 3 4	ISO/IEC 12207. ED-109/DO 278 – 3.8 tab. A-8. ED-12B/DO 178B – 7.2.6. IEC 61508 – 6.2.3. CMMI – CM 3.1.	*Vývoj:* I/II ANSP: A, dodavatel: L. *Provoz, údržba:* I/II ANSP: L.
		5.8.1	**Proces pro řešení problémů – implementace procesu** Proces pro řešení problémů (včetně prokázání úspěšného řešení problému) musí být definován pro zvládnutí všech problémů (včetně neshod), které jsou zjištěny v softwarových produktech a činnostech. *Pozn.: Implementace procesu by mohla například zahrnovat vytvoření hodnotící komise.*	1 2 3 4	ISO/IEC 12207. ED-109/DO 278 – 3.8 tab. A-8. ED-12B/DO 178B – 7, 11.17. IEC 61508 – 7.8, 1-6.2.1, I-7.16. CMMI – PMC GP 2.2, 3.1.	I/II ANSP: L, dodavatel: C.
		5.8.2	**Proces pro řešení problémů – řešení problému** Pokud byly v softwarovém produktu nebo činnosti zjištěny problémy (včetně neshod), musí být připravena zpráva o problému, kterou se popíše každý zjištěný problém. Zpráva o problému se musí použít jako součást procesu uzavřené smyčky procesu: od detekce problému, přes průzkum, analýzu a řešení problému a jeho příčiny až po detekci trendů v celkové problematice.	1 2 3 4	ISO/IEC 12207. ED-109/DO 278 – 3.8 tab. A-8. ED-12B/DO 178B – 7, 11.17. IEC 61508 – 7.8.2. CMMI – PMC 2 CAR.	I/II ANSP: L, dodavatel: C.
		5.8.3	**Proces pro řešení problémů – Účinky na bezpečnost** Musí být provedena analýza zprávy o problému s cílem zjištění: • Zda hlášený problém má bezpečnostní dopad (řízení rizika) a zdali odpovídá přidělenému SWAL. • Zda byla provedena taková nápravná opatření, která mohou prokázat, že bezpečnostně relevantní problémy byly dostatečně zmírněny.	1 2 3 4	ISO/IEC 12207. IEC 61508 – 7.8, 1-7.8, I-7.15. CMMI – REQM 1.3, CM 2.	I/II ANSP: L, dodavatel: C.

č.	Název položky	Číslo cíle	Cíl	SWAL	Normy	Odpovědnost
V	Vyřazení z provozu	**4.5.5**	**Vyřazení SW** Plán vyřazení SW musí být definován před ukončením jeho provozu. Musí být provedena analýza rizik pro proces vyřazení SW. *Pozn.: Plán by např. mohl obsahovat tyto položky: zastavení podpory produktu a připojené dokumentace, archivace SW a dokumentace, odpovědnost za jakoukoliv budoucí zbývající spornou otázku podpory, přechod na nový SW produkt, přístup k archivovaným kopiím dat.*	1 2 3 4	ISO/IEC 12207. IEC 61508 – 1-7.17	I/II ANSP: L, dodavatel: C.
ČÁST VI – COTS						
V I	Životní cyklus: Akvizice (pořízení) a integrální plány procesu	**7.2.1**	**Plány COTS** ANSP musí definovat postupy pro akvizici COTS, verifikaci COTS, řízení konfigurace COTS, plány pro zajištění kvality COTS. *Pozn.: Doporučuje se koordinovat proces pro zajištění kvality COTS s dodavatelem COTS.*	1 2 3 4	ED-109/DO 278 – 4.1.9 tab. 4-2. CMMI – SAM GP 2.2, 3.1.	I/II ANSP: A, dodavatel: L.
V I	Životní cyklus: převodní kritéria	**7.2.2**	**Převodní kritéria COTS** ANSP musí definovat převodní kritéria (na základě vztahu mezi procesy pro COTS a odpovídajícími procesy životního cyklu CNS/ATM).	1 2 3 4	ED-109/DO 278 – 4.1.9 tab. 4-2. CMMI – SAM 2.1, TS 2.4, IPM 1.3.	I/II ANSP: A, dodavatel: L.
V I	Zajištění: COTS plány pro zajištění	**7.2.3**	**Jednotnost COTS plánů** Plány COTS definované dle bodu 7.2.1. musí být v souladu s plány pro ANS SW.	1 2 3 4	ED-109/DO 278 – 4.1.9 tab. 4-2. CMMI – SAM 2.1, TS 2.4.	I/II ANSP: A, dodavatel: L.

č.	Název položky	Číslo cíle	Cíl	SWAL	Normy	Odpovědnost
V I	Zajištění naplnění ANS požadavků COTS softwarem	**7.2.4**	**Pokrytí požadavků dosažených COTS** ***Proces ověřování COTS SW*** Je rozšíření procesu ověřování SW popsaného v cíli 5.4.X. Zejména proces akvizice COTS často identifikuje cíle, které mohou být splněné použitím standardních prostředků. Pro cíle, které nemohou být naplněny dostupnými údaji COTS (např. požadavky na jeho vývoj) smí být použity další aktivity, zahrnující alternativní metody, jako je zpětné řízení, které mohou být použity po akceptaci schvalující autoritou. *Pozn.: Musí být prokázáno pokrytí požadavků ANS SW dosažených COTS. Pro splnění tohoto bodu je potřeba nejprve provést definici požadavků na COTS, tzn. určit, do jaké míry jsou požadavky na CNS/ATM relevantní pro COTS – jedná se o jakýsi průnik požadavků CNS/ATM a kapacit COTS. Definici těchto kapacit lze získat z uživatelských manuálů, technických manuálů, technických specifikací produktu, atd.).*	1 2 3 4	ED-109/DO 278 – 4.1.9 tab. 4-2. CMMI – SAM 2.1, TS 2.4.	I/II ANSP: A, dodavatel: L.
V I	Zajištění: Zajištění přiměřenosti dat životního cyklu	**7.2.5**	**Životní cyklus COTS** Dostupnost dat životního cyklu COTS musí být stanovena v souladu se SWAL (rozsah dat životního cyklu, která jsou dostupná pro účely ověřování/zajištění).	1 2 3 4	ED-109/DO 278 – 4.1.9 tab. 4-2. CMMI – SAM 2.1, TS 2.4.	I/II ANSP: A, dodavatel: L.
V I	Požadavky: odvozené požadavky	**7.2.6**	**Odvozené požadavky pro COTS** Musí být definovány odvozené požadavky (požadavky kladené na ANS systém v důsledku používání COTS, nebo požadavky pro potlačení nepotřebných funkcí COTS ovlivňujících systém ANS). *Pozn.: Při používání COTS je možné odvodit další požadavky, které by měly být doplněny k požadavkům na ANS SW. Jedná se např. o požadavky závislé na platformě, omezení použití, procesy přerušení, požadavky na zdroje, atd.*	1 2 3 4	ED-109/DO 278 – 4.1.9 tab. 4-2. CMMI – SAM 2.1, TS 2.4.	I/II ANSP: A, dodavatel: L.
V I	Zajištění kompatibility COTS s cílovým HW (PC)	**7.2.7**	**Kompatibilita COTS s HW** Musí být prokázána kompatibilita COTS s HW, na kterém bude COTS provozován.	1 2 3 4	ED-109/DO 278 – 4.1.9 tab. 4-2. CMMI – TS 2.4, RD 2.2, 3.4.	I/II ANSP: A, dodavatel: L.

č.	Název položky	Číslo cíle	Cíl	SWAL	Normy	Odpovědnost
V I	Zajištění konfigurace COTS a určení datových položek	**7.2.8**	**Řízení konfigurace COTS - Identifikace** Musí být stanovena konfigurace COST a datových položek. *Pozn.: Specifický způsob řízení konfigurace pro COTS a datové položky, např. dokumentace SW, úprava dat, atd.*	1 2 3 4	ED-109/DO 278 – 4.1.9 tab. 4-2. CMMI – CM 1.2.	I/II ANSP: A, dodavatel: L.
V I	Modifikace: hlášení problémů	**7.2.9**	**Zprávy o problémech COTS** Musí být stanoven postup pro hlášení chyb COTS. *Pozn.: ANSP systém pro hlášení chyb zahrnuje řízení chyb detekovaných v COTS a obousměrný mechanismus podávání zpráv mezi provozovatelem COST a dodavatelem COTS.*	1 2 3 4	ED-109/DO 278 – 4.1.9 tab. 4-2. CMMI – CM 1.1, SAM GP 2.6.	I/II ANSP: A, dodavatel: L.
V I	Zajištění řízení (kontroly) procesu zavádění nových verzí COTS	**7.2.10**	**Nový release COTS** Instalace nových release COTS musí být řízena. *Pozn.: Možno popsat jako součást systému řízení změn v rámci ANSP. Měla by se provádět analýza dopadu změn na COTS před instalací nových verzí COTS.*	1 2 3 4	ED-109/DO 278 – 4.1.9 tab. 4-2. CMMI – SAM 2.3, CM 1.2.	I/II ANSP: A, dodavatel: L.
V I	Zajištění archivace konfigurace COTS a datových položek	**7.2.11**	**Řízení konfigurace – archivace** Konfigurace COST a datových položek musí být archivována.	1 2 3 4	ED-109/DO 278 – 4.1.9 tab. 4-2. CMMI –CM 2.2.	I/II ANSP: A, dodavatel: L.
ČÁST VII – ZAJIŠTĚNÍ						
V II	Nástroje zajištění (vývoj, řízení konfigurace, údržba)	**4.3.12**	**Použití specifikovaných nástrojů** Musí být použity nástroje požadované specifikací. *Pozn.: Projektant vybírá, přizpůsobuje a použije ty normy a metody, nástroje a počítačové programovací jazyky, které jsou dokumentovány, vhodné a zavedené v organizaci, pokud není v kontraktu uvedeno jinak.*	1 2 3 4	ISO/IEC 12207. ED-109/DO 278 – 3.1 Tab. A-1, 3.2 tab. A-2, A-3, A-4. ED-12B/DO 178B – 4.4, 4.5, 11.1, 11.2, 11.6 IEC 61508 – 3-7.1.2.6, Annex A, B, 3-7.4, 3-7.2. CMMI – PP 2.4, IPM 1.1, GP 2.2, 2.3, 3.1, RD.	I/II ANSP: C/A, dodavatel: L.

č.	Název položky	Číslo cíle	Cíl	SWAL	Normy	Odpovědnost
		4.3.17	**Nástroje pro návrh - Vývojové prostředí SW** Používá-li se nástroj pro navrhování SW, pak projektant musí identifikovat vybrané vývojové prostředí s ohledem na: • Zvolené metody, postupy a nástroje (pokud existují), které mají být použity. • Hardwarové platformy pro nástroje (pokud existují), které mají být použity.	1 2 3 4	ISO/IEC 12207. ED-109/DO 278 – 3.1 Tab. A-1. ED-12B/DO 178B – 11.1, 11.2. IEC 61508 – 3-7.4.4. CMMI – PP 2.4, GP 2.2, 2.3, 3.1.	I/II ANSP: C/A, dodavatel: L.
		4.3.18	**Použití nástrojů pro návrh** Musí být použit nástroj pro navrhování SW.	1 2 3 4	ISO/IEC 12207. ED-109/DO 278 – 3.1 Tab. A-1. ED-12B/DO 178B – 11.1, 11.2. IEC 61508 – 3-7.4.4. CMMI – PP 2.4, GP 2.2, 2.3, 3.1.	I/II ANSP: C/A, dodavatel: L.
		4.3.19	**Prostředí pro generování kódu** **(4.3.19.1) Vývojové prostředí SW** Projektant musí identifikovat vybrané softwarové vývojové prostředí, s ohledem na: • Programovací jazyky, nástroje kódování, kompilátory, editory a zavaděče, které mají být použity. • Hardwarové platformy pro nástroje, které mají být použity.	1 2 3 4	ISO/IEC 12207. ED-109/DO 278 – 3.1 Tab. A-1, 3.7 Tab. A-7. ED-12B/DO 178B – 4.4, 4.5.5.3, 5.5, 11.2, 11.8, 11.11. IEC 61508 – 3-7.1.2.6, Annex A, B, 3-7.4.4. CMMI – PP 2.4, IPM 1.1, GP 2,2, 2.3, 3.1, TS 3.1, ReqM 1.4.	I/II ANSP: C/A, dodavatel: L.
			(4.3.19.2) Programovací jazyky Výběr vhodných programovacích jazyků musí být odpovídat požadované úrovní zajištění SW.	1 2 3 4		
			(4.3.19.3) Výběr překladačů Musí být definován způsob použití překladačů (compiler).	1 2 3 4		
			(4.3.19.4) Validace nástrojů pro vývoj SW Musí být definováno prostředí pro validaci (potvrzení zkouškou) nástrojů pro vývoj SW.	1 2 3 4		

č.	Název položky	Číslo cíle	Cíl	SWAL	Normy	Odpovědnost
		5.2.8	**Schválení nástrojů pro řízení konfigurace** Akvizitér musí schválit vybraný nástroj řízení konfigurace SW.	1 2 3 4	N/A	*Vývoj:* I/II ANSP: A, dodavatel: L. *Provoz, údržba:* I/II ANSP: L.
		6.2.3	**Proces infrastruktury – údržba infrastruktury** Infrastruktura musí být udržována, sledována a modifikována podle potřeby k zajištění neustálého plnění požadavků procesů (např. vývoj nebo ověření). Jako součást údržby infrastruktury musí být definován rozsah, v němž infrastruktura podléhá řízení konfigurace.	1 2 3 4	ISO/IEC 12207. ED-109/DO 278 – 3.8, tab. A-8. ED-12B/DO 178B – 7.2.9. IEC 61508 – 6.2.3. CMMI – CM, PMC 1.1.	I/II ANSP: A, dodavatel: L.
V II	Provozní zajištění	**4.4.1**	**Proces provozování – Implementace procesu** Provozní postupy musí být definovány a realizovány. *Pozn.: Provozní dokumentace pro výkon činností a úloh, postupy pro odhalování a řešení problémů, postupy pro testování SW v provozním prostředí, postupy pro údržbu, atd.*	1 2 3 4	ISO/IEC 12207. IEC 61508 – 1-7.15.	I/II ANSP: L, dodavatel: C.
		4.4.2	**Určené provozní prostředí** SW musí být provozován v prostředí určeném uživatelskou dokumentací. *Pozn.: Mělo by se prokázat, že jakékoli použití nastavení SW (např. výběr parametrů uživatelem, přístup do databáze, změna konfiguračního souboru, atd.) dle specifikace SW povede vždy k bezpečnému provozu. Za tímto účelem je vhodné definovat metodiku, pomocí které se uvedený požadavek ověří.*	1 2 3 4	ISO/IEC 12207. IEC 61508 – 1-7.15.	I/II ANSP: L, dodavatel: C.
V II	SWAL: přísnost SWAL, odchylky, zajištění, sledování	**3.0.8**	**Zajištění cíle** SWAL musí poskytovat dostatečnou jistotu, že ANS software může být provozován, alespoň s minimální přijatelnou bezpečností. *Pozn.: Systém řízení rizik pro SW s definovanou SWAL.*	1 2 3 4	ED-109/DO 278 - 2.1 ED-12B/DO 178B – 2.1, 9 a 11.20 IEC 61508 - 1-7.4.2.	I/II ANSP: L, dodavatel: C.

č.	Název položky	Číslo cíle	Cíl	SWAL	Normy	Odpovědnost
		3.0.10	**Zajištění SWAL** Ujištění musí poskytovat důvěru, že je dosaženo SWAL. *Pozn.: Ujištění může být založeno na přímých či nepřímých argumentech a důkazech. Metodika viz kap.9 ED-12B/DO 178B.*	1 2 3 4	ED-109/DO 278 – 3.10 Tab. A-10, 5.1. ED-12B/DO 178B – 9, 11.20. IEC 61508 – 6.2.2	I/II ANSP: C, dodavatel: L.
		3.0.11	**Sledování SWAL** Ujištění prostřednictvím monitorování musí být provedeno, pokud již SW v provozu splňuje požadavky s mírou důvěry úměrnou SWAL. Zpětná vazba ze zkušenosti s ANS SW musí být použita na potvrzení toho, že SSAS a přiřazení SWAL jsou vhodné. Pro tento účel musí být hodnocen účinek, vyplývající ze všech zaznamenaných SW závad nebo selhání z provozních zkušeností ANSP (hlášení událostí dle interních postupů ANSP) v souladu s mapováním SWAL. *Pozn.: Hlášené závady SW nebo jeho selhání jsou výstupem systému hlášení událostí jako součást ANSP SMS.*	1 2 3 4	ED-109/DO 278 – 4.1.6.3.	I/II ANSP: L.
		4.4.3	**Podpora uživatele** Provozovatel musí poskytnout výcvik uživatelům, je-li to relevantní.	1 2 3 4	ISO/IEC 12207.	I/II ANSP: L, dodavatel: C.
V II	Audity, přezkumy	**5.6.1**	**Proces společného přezkoumání - implementace procesu** Periodická přezkoumání musí být prováděna v předem stanovených termínech (bodech) podle toho, jak je specifikováno v plánech projektu. Výsledky přezkoumání musí být dokumentovány a distribuovány zainteresovaným stranám. *Pozn.: Ad hoc přezkoumání mohou být prováděna, jestliže to považuje za nutné kterákoliv ze stran. Problémy zjištěné při přezkoumání by měly být zaznamenány a měly by vstoupit do procesu řešení problémů. Strany by se měly shodnout na výsledcích přezkoumání.*	1 2 3 4	ISO/IEC 12207. ED-109/DO 278 – 3.9 tab. A-9. ED-12B/DO 178B – 6, 8.3. IEC 61508 –1-6.2, 1-7.18. CMMI – PP 2.1, 2.6, PMC 1.6, 1.7.	I/II ANSP: A, dodavatel: L.

č.	Název položky	Číslo cíle	Cíl	SWAL	Normy	Odpovědnost
		5.6.2	**Proces společného přezkoumání – přezkoumání na úrovni projektu** Stav projektu musí být hodnocen ve vztahu k aplikovaným plánům projektu, časovým plánům, normám, směrnicím a kritériím přechodu. *Pozn.: Výsledek přezkoumání by měl být diskutován oběma stranami a měl by poskytnout podklady pro zajištění pokroku v činnostech podle plánu založeném na zhodnocení činnosti nebo stavu SW, udržení celkové kontroly projektu prostřednictvím přidělování zdrojů, změny směrování projektu nebo určení potřeby pro alternativní plánování a zhodnocení a řízení rizikových faktorů, které mohou ohrozit úspěch projektu.*	1 2 3 4	ISO/IEC 12207. ED-109/DO 278 – 3.9 tab. A-9. ED-12B/DO 178B – 4.6, 8.2. IEC 61508 –1-6.2, 7.3.2. CMMI – PP 2.1, 2.6, PMC 1, 1.6, 1.7.	I/II ANSP: A, dodavatel: L.
		5.6.3	**Proces společného přezkoumání – technická přezkoumání** Technická přezkoumání musí být prováděna s cílem zhodnotit uvažované SW produkty nebo SW služby. *Pozn.: A také za účelem podání důkazu, že SW produkty nebo SW služby jsou kompletní, jsou ve shodě s normami a specifikacemi, změny jsou do nich zaváděny správným způsobem a ovlivňují pouze ty oblasti, které jsou identifikovány v procesu řízení konfigurace, dodržují příslušné časové plány, jsou připraveny pro další činnost a vývoj, provoz nebo údržba jsou vykonávány podle plánů, časových plánů, norem a směrnic.*	1 2 3 4	ISO/IEC 12207. ED-109/DO 278 – 3.9 tab. A-9. ED-12B/DO 178B – 6, 8.3. IEC 61508 –1-5.2.11, 7.2.2, 7.3.2, 7.4. CMMI – PP 2.1, 2.6, PMC 1, 1.6, 1.7.	I/II ANSP: A, dodavatel: L.
		5.7.1	**Proces prověrky (audity)** Audity se musí konat v předem stanovených termínech, jak je stanoveno v plánu projektu, nebo na zvláštní žádost. Po dokončení auditu musí být výsledky auditu zdokumentovány a poskytnuty auditované straně.	1 2 3 4	ISO/IEC 12207. ED-12B/DO 178B – 8.2, 11.19. IEC 61508 –1-6.2.1, 1-7.7.2.1, 7.8.2, 7.15.2. CMMI – GP 2.7, 2.9.	I/II ANSP: C/A, dodavatel: L.

č.	Název položky	Číslo cíle	Cíl	SWAL	Normy	Odpovědnost
		5.7.2	**<u>Audity na úrovni požadavků na SW</u>** Audity na požadavky SW musí být prováděny v předem stanovených termínech: Audity musí určit, zda: • Přezkum akceptace (přijetí) a verifikace požadavků, které jsou stanoveny v dokumentaci, jsou adekvátní pro akceptaci SW. • Data ověření (verifikace) jsou v souladu se specifikací. • SW byl úspěšně ověřen (verifikován) a odpovídá požadavkům. • Zprávy o ověření (verifikaci) jsou správné a rozdíly mezi skutečnými a očekávanými výsledky byly vyřešeny. • Produkt (požadavek SW) a uživatelská dokumentace jsou v souladu s normami/pravidly, jak je definováno. • Činnosti byly provedeny v souladu s platnými požadavky, plány a smlouvami. • Náklady a harmonogramy jsou v souladu s plány.	1 2 3 4	ISO/IEC 12207. ED-12B/DO 178B – 8.2. IEC 61508 –6.2.3. CMMI – Ver. 1, 2, 3, TS 3.1, 3.2, PMC 1.1, 2, 3.2, CM 2.1, 3.2, GP 2.9.	I/II ANSP: C/A, dodavatel: L.
		5.7.3	**<u>Audity do úrovně architektury SW</u>** Audity musí být prováděny v předem stanovených termínech a na základě specifických požadavků, aby bylo zajištěno, že: • Přezkum přijetí (akceptace) a požadavky verifikace popsané v dokumentaci jsou přiměřené (dostačující) pro přijetí SW. • Data ověření jsou v souladu se specifikací. • Software byl úspěšně ověřen a splňuje jeho požadavky na SW, požadavky na architekturu a detailní požadavky návrhu. • Zprávy z ověření jsou správné a rozdíly mezi skutečnými a očekávanými výsledky byly vyřešeny. • Produkt (požadavky na SW, SW architektura) a uživatelská dokumentace jsou v souladu s normami/ pravidly. • Činnosti byly provedeny v souladu s platnými požadavky, plány a smlouvami. • Náklady a harmonogramy jsou v souladu s plány.	1 2 3 4	ISO/IEC 12207. ED-12B/DO 178B – 8.2. IEC 61508 –6.2.3. CMMI – Ver. 1, 2, 3, TS 3.1, 3.2, PMC 1.1, 2, 3.2, CM 2.1, 3.2, GP 2.9.	I/II ANSP: C/A, dodavatel: L.

č.	Název položky	Číslo cíle	Cíl	SWAL	Normy	Odpovědnost
		5.7.4	**<u>Audity do úrovně zdrojového kódu SW</u>** Audity musí být prováděny v předem stanovených termínech a na základě specifických požadavků, aby bylo zajištěno, že: • Přezkum přijetí (akceptace) a požadavky verifikace popsané v dokumentaci jsou přiměřené (dostačující) pro přijetí SW. • Data ověření jsou v souladu se specifikací. • Software byl úspěšně ověřen a splňuje jeho požadavky na SW, požadavky na architekturu a detailní požadavky návrhu. • Zprávy z ověření jsou správné a rozdíly mezi skutečnými a očekávanými výsledky byly vyřešeny. • Produkt (požadavky na SW, SW architektura, návrh a zdrojový kód) a uživatelská dokumentace jsou v souladu s normami / pravidly. • Činnosti byly provedeny v souladu s platnými požadavky, plány a smlouvami. • Náklady a harmonogramy jsou v souladu s plány.	1 2 3 4	ISO/IEC 12207. ED-12B/DO 178B – 8.2. IEC 61508 –6.2.3. CMMI – Ver. 1, 2, 3, TS 3.1, 3.2, PMC 1.1, 2, 3.2, CM 2.1, 3.2, GP 2.9.	I/II ANSP: C/A, dodavatel: L.
		5.7.5	**<u>Audity kvality do úrovně spustitelnosti SW</u>** Audity musí být prováděny v předem stanovených termínech a na základě specifických požadavků, aby bylo zajištěno, že: • Přezkum přijetí (akceptace) a požadavky verifikace popsané v dokumentaci jsou přiměřené (dostačující) pro přijetí SW. • Data ověření jsou v souladu se specifikací. • Software byl úspěšně ověřen a splňuje jeho požadavky na SW, požadavky na architekturu a detailní požadavky návrhu. • Zprávy z ověření jsou správné a rozdíly mezi skutečnými a očekávanými výsledky byly vyřešeny. • Produkt (požadavky na SW, SW architektura, návrh a zdrojový kód a spustitelný soubor) a uživatelská dokumentace jsou v souladu s normami / pravidly. • Vývojové nástroje SW (např. překladače) jsou způsobilé. • Činnosti byly provedeny v souladu s platnými požadavky, plány a smlouvami. Náklady a harmonogramy jsou v souladu s plány.	1 2 3 4	ISO/IEC 12207. ED-12B/DO 178B – 8.2. IEC 61508 –6.2.3. CMMI – Ver. 1, 2, 3, TS 3.1, 3.2, PMC 1.1, 2, 3.2, CM 2.1, 3.2, GP 2.9.	I/II ANSP: C/A, dodavatel: L.

č.	Název položky	Číslo cíle	Cíl	SWAL	Normy	Odpovědnost
VII	Zajištění výcviku	**6.4.1**	**Proces zajištění lidských zdrojů – implementace procesu** Musí být prováděn přezkum požadavků projektu tak, aby se zajistilo včasné vyškolení schopných a kvalifikovaných pracovníků požadovaných vedením a technickým štábem. Musí být stanoveny typy a úrovně výcviku a kategorie personálu, který potřebuje výcvik. Musí být zpracován a dokumentován výcvikový plán, který obsahuje adaptační plány *(„postup výcviku od začátku do konce“)*, požadavky na zdroje a úrovně dovedností a znalostí.	1 2 3 4	ISO/IEC 12207. IEC 61508 – 1-6.2.1, I-Annex B. CMMI – PP 2.5, PMC 1.1, GP 2.5, OT 1.1, 1.3.	I/II ANSP: A, dodavatel: L.
		6.4.2	**Proces zajištění lidských zdrojů – materiály pro výcvik** Musí být pracovány příručky včetně prezentačních materiálů.	1 2 3 4	ISO/IEC 12207. CMMI – OT 1.4.	I/II ANSP: A, dodavatel: L.
		6.4.3	**Proces zajištění lid. zdrojů – implementace plánu výcviku** Plán výcviku musí být implementován. Musí být vedeny a udržovány záznamy o průběhu výcviku.	1 2 3 4	ISO/IEC 12207. IEC 61508 – 1-6.2.2, I-Annex B. CMMI – PP 2.5, OT 2.1, 2.2.	I/II ANSP: A, dodavatel: L.
VII	Zajištění požadavků na úplnost a správnost	**3.0.2**	**Kompletnost a správnost požadavků** Požadavky na software musí správně a úplně stanovit to, co je požadováno od SW, aby splňoval cíle bezpečnosti systému a požadavky bezpečnosti systému identifikované na základě rizik. *Pozn.: Jedná se o přezkumy a analýzy požadavků na nejvyšší úrovni – shoda požadavků na SW se systémovými požadavky (nesmí dojít k rozporu), přesnost a jednoznačnost požadavků (výklad požadavků je stejný u všech zainteresovaných stran), kompatibilita SW s HW cílového počítače, ověřitelnost (dají se všechny cíle ověřit/měřit?), shoda s normami a legislativou, atd.*	1 2 3 4	ISO/IEC 12207. ED-109/DO 278 – 3.2 – Tab. A-2 , 3.3 Tab. A-3. ED-12B/DO 178B – 5.1, 6.3.1. IEC 61508 – 7.2.2. CMMI – RD 1.1, 1.2, 2.1	I ANSP: A, dodavatel: L. II ANSP: L, dodavatel: C.

č.	Název položky	Číslo cíle	Cíl	SWAL	Normy	Odpovědnost
		4.1.7	**Akceptace** **(4.1.7.1)** Akvizitér musí připravit akceptaci SW na základě definované strategie a kritérií akceptace. Musí v nich být zahrnuta příprava testovacích případů, testovacích dat, testovacích procedur a testovacího prostředí. **(4.1.7.2)** Musí být definován rozsah spoluodpovědnosti (zapojení) dodavatele. **(4.1.7.3)** Akvizitér musí provádět akceptační přezkoumání a testování dodaných SW produktů nebo služeb.	1 2 3 4	ISO/IEC 12207. CMMI – SAM 2.3.	I/II ANSP: L.
		4.2.6	**Přezkoumání a hodnocení** Dodavatel musí koordinovat činnosti přezkoumání vyplývající z kontraktu, styky (rozhraní) a komunikaci s organizací akvizitéra. Dodavatel musí vykonávat činnosti při zabezpečování kvality. *Pozn.: Dodavatel by měl provádět neformální schůzky, akceptační přezkoumání a testování, společná přezkoumání (metodika např. viz ISO/IEC 12207, čl. 6.6) a prověrky (metodika např. viz ISO/IEC 12207, čl. 6.7) s akvizitérem podle toho, jak je specifikováno v kontraktu a plánech projektu. Dodavatel by měl vykonávat ověřování a validaci (např. v souladu s ISO/IEC 12207, čl. 6.4 a 6.5). Dodavatel by měl umožnit akvizitérovi přístup k zařízením dodavatele.*	1 2 3 4	ISO/IEC 12207. IEC 61508 – 1-6.2. CMMI – a) PMC 1.5, 1.6, 1.7, b) PPQA, PI 3.4 Ver., Val.	I/II Dodavatel: L.
		5.4.1	**Ověřování implementace procesu** Musí být zaveden proces ověřování (verifikace) SW. Výstup z procesu ověřování musí být zdokumentován a distribuován zainteresovaným stranám. *Pozn.: Měly by být určeny cílové činnosti životního cyklu SW a SW produkty vyžadující ověřování. Pro cílové činnosti a SW produkty jsou poté vybrány činnosti ověřování a úlohy (např. ověřování kontraktu, procesu, požadavků, návrhu, kódu, integrace, dokumentace) zahrnující metody, techniky a nástroje provedení úloh. Na základě určených úloh je vytvořen plán ověřování (viz 5.4.2), který mimo jiné obsahuje i postupy pro zasílání zpráv o ověřování akvizitérovi a zainteresovaným stranám.*	1 2 3 4	ISO/IEC 12207. ED-109/DO 278 – 3.1 tab. A-1, 3.4, 3.5, 3.7, 3-7 tab. A-7, 3.10 tab. A-10. ED-12B/DO 178B – 2.7, 6, 6.1, 11.3. IEC 61508 – 7.4.1.5, 7.9.2, 1-7.4, 1-7.6, 1-7.8, 1-7.18, I-7.14, 2-7.7.2.3, II-7.7.2. CMMI – GP 2.2, 3.1, Ver. 1, 2, 3, RD 3.3, 3.5, REQM 1.5, Val 1.3, 2.	I/II ANSP: A, dodavatel: L.

č.	Název položky	Číslo cíle	Cíl	SWAL	Normy	Odpovědnost
		5.4.2	**Plán ověřování** Musí být definován plán ověřování (verifikace). Plán musí obsahovat činnosti životního cyklu a SW produkty podléhající ověřování, požadované úlohy ověřování pro každou činnost životního cyklu a SW produkt a příslušné zdroje, odpovědnosti a časový plán. Tento plán musí dále obsahovat postupy pro zasílání zpráv o ověřování akvizitérovi a ostatním zainteresovaným stranám s uvedením opatření, která mají být přijata každou stranou. *Pozn.: Plán ověřování může obsahovat popis různých typů testování v jednotlivých fázích životního cyklu SW (FAT, SAT, testování software. Cíle týkající se ověření konfiguračních / adaptačních dat mohou být rozšířeny v provozním procesu (viz cíle 4.4.X). Strategie pro ověření vhodné kombinace konfiguračních / adaptačních by ale měla být součástí plánu ověřování.*	1 2 3 4	ISO/IEC 12207. ED-109/DO 278 – 3.1 tab. A-1, 2.1, 3.3 tab. A-3, 3.4 tab. A-4, 3.7 tab. A-7, 3.9 tab. A-9, 3.10 tab. A-10. ED-12B/DO 178B – 2.2, 2.3, Annex A, 6.1, 11.3. IEC 61508 – 7.4.1.5, 7.9.2, 1-7.4, 1-7.6, 1-7.18. CMMI – GP 2.2, 2.3, 3.1, Ver. 1, Ver. 1.3, 2, 3, PP 1.3, PMC 1, 2, IPM 1.3, 1.4, 2, CM 2.1, PPQA 1, SAM 1.2, REQM 1.1, 1.3, RD 3.3 až 3.5, PMC GP 2.2, 2.4, 3.1, 2.7.	I/II ANSP: A, dodavatel: L.
		5.4.3	**Ověřování softwarových požadavků** **(5.4.3.1)** Musí být ověřeno, že požadavky na SW jsou správné a úplné.	1 2 3 4	ISO/IEC 12207. ED-109/DO 278 – 3.1 tab. A-1 3.2 tab. A-2, 3.3 tab. A-3,3.5 tab. A-5. ED-12B/DO 178B – Annex A-3 až Annex A-7, 6.1, 6.2, 6.3, 6.4 IEC 61508 – 7.9.2, 1-7.15. CMMI – Ver. 3, Val 2, PI 3.4.	I/II ANSP: A, dodavatel: L.
			Požadavky na SW musí být ověřeny (verifikovány) vzhledem k tomu, zda:			
			(5.4.3.2) Funkční chování implementovaného SW je v souladu s požadavky na SW.	1 2 3 4		
			(5.4.3.3) Výkony v čase implementovaného SW jsou v souladu s požadavky na SW.	1 2 3 4		
			(5.4.3.4) Se SW požadavky shodují, jsou proveditelné a ověřitelné.	1 2 3 4		
			(5.4.3.5) Odolnost implementovaného SW vůči abnormálním provozním podmínkám/stavům vyhovují požadavkům na SW.	1 2 3 4		
			(5.4.3.6) Externí rozhraní vyhovují požadavkům na SW.	1 2 3 4		
			(5.4.3.7) Vnitřní neporušenost SW vyhovuje požadavkům na SW.	1 2 3 4		

č.	Název položky	Číslo cíle	Cíl	SWAL				Normy	Odpovědnost
			(5.4.3.8) Implementovaný SW vyhovuje kompatibilitě s HW/SW vlastnostmi cílového počítače (časové odezvy, vstup/výstupní HW, provoz na cílovém HW).	1	2	3	4		
			(5.4.3.9) Jsou přizpůsobeny požadavkům SW standardů/pravidel.	1	2	3	4		
			(5.4.3.10) Použité algoritmy jsou přesné a správné.	1	2	3	4		
			(5.4.3.11) Kapacita implementovaného SW vyhovuje požadavkům na SW.	1	2	3	4		
			(5.4.3.12) Tolerance k přetížení implementovaného SW vyhovuje požadavkům na SW.	1	2	3	4		
		5.4.4	**Ověřování integrace** Integrace musí být ověřována minimálně se zřetelem na tato kritéria:					ISO/IEC 12207. ED-109/DO 278 – 3.1 tab. A-1, 3.5 tab. A-5. ED-12B/DO 178B – Annex A-3 až Annex A-7, 6.2, 6.3, 6.4 IEC 61508 – 7.9.2. CMMI –Ver. 1, 2, 3, PI 3.1, 3.2, PI GP 2.9.	I/II ANSP: A, dodavatel: L.
			(5.4.4.1) SW komponenty byly úplně a správně integrovány do každé SW položky.	1	2	3	4		
			(5.4.4.2) SW jednotky byly úplně a správně integrovány do každé SW položky.	1	2	3	4		
			(5.4.4.3) HW položky, SW položky a ruční operace byly úplně a správně integrovány do systému.	1	2	3	4		
			(5.4.4.4) Integrační úlohy byly vykonány v souladu s plánem integrace.	1	2	3	4		
			Pozn.: Příklady ověřovacích kritérií jsou: • *Přivedená a načítaná data a mapování paměti.* • *Řízení dat a spojování.* • *Nesprávná adresace HW.* • *Přeplnění paměti, chybějící SW komponenty.*						

č.	Název položky	Číslo cíle	Cíl	SWAL	Normy	Odpovědnost
		5.4.5	**Ověřování návrhu** **(5.4.5)** Aby se při hodnocení ověřila architektura SW a uživatelská dokumentace, musí výsledky testů zahrnovat: **(5.4.5.1)** Externí konzistenci se systémovými požadavky (HW-SW kompatibilita). **(5.4.5.2)** Interní konzistenci (tok dat a jeho řízení). **(5.4.5.3)** Pokrytí požadavků SW návrhu. **(5.4.5.4)** Shodu návrhu se standardy/pravidly pro návrh SW. **(5.4.5.5)** Vhodnost norem testování a použitých metod. **(5.4.5.6)** Shodu s očekávanými výsledky. **(5.4.5.7)** Proveditelnost testování návrhu SW. **(5.4.5.8)** Proveditelnost údržby (provoz a údržba). **(5.4.5.9)** Kritéria ověřování, podle kterých bude posuzováno dokončení ověření. Výsledky hodnocení musí být zdokumentovány. *Pozn.: Shoda by měla být ověřena podle definovaných přechodových kritérií mezi fázemi životního cyklu SW (přidělení SWAL pro vývojový proces).*	1 2 3 4	ISO/IEC 12207. ED-109/DO 278 – 3.1 tab. A-1, 3.4 tab. A-4, 3.6 tab. A-6, 3.7 tab. A-7, 3.5 tab. A-5. ED-12B/DO 178B – Annex A-3 až Annex A-7, 6.2, 6.3, 6.4, 5.3, 5.5, 11.8, 11.11. IEC 61508 – 7.4, 7.9.2. CMMI –Ver. 1, 2, 3, TS 1.1, 2.1, 1.3, 3.1, REQM 1.4, TS GP 2.2, 2.3,3.1.	I/II ANSP: A, dodavatel: L.

č.	Název položky	Číslo cíle	Cíl	SWAL	Normy	Odpovědnost
		5.4.6	**Ověřování podrobného návrhu** **(5.4.6)** Při hodnocení (evaluaci) softwarového kódu a výsledků ověřování (verifikace) musí být vzato v úvahu: **(5.4.6.1)** Externí konzistence se systémovými požadavky (HW-SW kompatibilita). **(5.4.6.2)** Vnitřní konzistence mezi detailními požadavky návrhu. **(5.4.6.3)** Ověření pokrytí detailního návrhu položky. **(5.4.6.4)** Shoda kódu se standardy/pravidly. **(5.4.6.5)** Ověření pokrytí struktury software (deklarace pokrytí). *Pozn. Ověření může být provedeno pomocí zkoušky, analýzy, demonstrace nebo kombinací uvedeného v průběhu celého životního cyklu SW.* **(5.4.6.6)** Vhodnost metod kódování a použitých standardů/ pravidel, **(5.4.6.7)** Proveditelnost ověření (verifikace) SW kódu, **(5.4.6.8)** proveditelnost údržby, Výsledky hodnocení (evaluace) musí být dokumentovány.	1 2 3 4	ISO/IEC 12207. ED-109/DO 278 – 3.1 tab. A-1, 3.5 tab. A-5, 3-6.3, 3.6 tab. A-6, 3.7 tab. A-7. ED-12B/DO 178B – Annex A-3 až Annex A-7, 6.2, 6.3, 6.4, 5.3, 5.5, 11.8, 11.11. IEC 61508 – 7.4, 7.9.2. CMMI –Ver. 1, 2, 3, TS 3.1, REQM 1.4.	I/II ANSP: A, dodavatel: L.

č.	Název položky	Číslo cíle	Cíl	SWAL	Normy	Odpovědnost
		5.4.8	**Ověřování kódu** Spustitelný kód a výsledky ověřování musí být vyhodnoceny na základě níže uvedených kritérií: **(5.4.8.1)** Vnější shoda s kódem SW (např. Vytváří překladač příslušný spustitelný nebo objektový kód?). **(5.4.8.2)** Vnitřní shoda mezi exe požadavky (např. Vytváří překladač vždy stejný spustitelný nebo objektový kód pro stejné zdroje?). **(5.4.8.3)** Ověření překladu zdrojového kódu softwaru do objektového kódu (např. Vytváří překladač další a nepotřebný spustitelný nebo objektový kód, jako je třeba „mrtvý spustitelný kód“?). *Pozn.: Mrtvý kód je zbytečný, nefunkční kód, který by měl být odstraněn. Opakem mrtvého kódu je živý, operační kód.* **(5.4.8.4)** Proveditelnost ověření spustitelnosti. **(5.4.8.5)** Ověření struktury SW (MC/DC). *Pozn.: The modified condition/decision coverage (MC/DC) = Zdrojový kód metriky pro měření kvality testovací sady. MC / DC se používá v letectví při vývoje software dle DO-178B a DO-178C pro zajištění testování nejkritičtějšího softwaru (Úroveň A).* Výsledky hodnocení musí být dokumentovány.	1 2 3 4	ED-109/DO 278 – 3.6 tab. A-6. ED-12B/DO 178B – Annex A-6. CMMI –Ver. 3, TS 3.1, REQM 1.4.	I/II ANSP: A, dodavatel: L.
		5.4.9	**Ověřování dat** Datové struktury, specifikované v průběhu detailního návrhu musí být ověřeny na: **(5.4.9.1)** Kompletnost (dokončení). **(5.4.9.2)** Vlastní shodu. **(5.4.9.3)** Ochranu proti změně nebo deformaci.	1 2 3 4	ED-109/DO 278 – 3.2 tab. A-2. ED-12B/DO 178B – Annex A-6. IEC 61508 – 7.9.2. CMMI –Ver. 1.3, 2, TS 3.1, PI Ver., Val.	I/II ANSP: A, dodavatel: L.

č.	Název položky	Číslo cíle	Cíl	SWAL	Normy	Odpovědnost
		5.4.11	**Měření složitosti** Musí být prokázáno analýzou opatření a uplatňováním nápravných opatření, že naměřená složitost je ve vymezené prahové hodnotě. Pokud hodnota překračuje limity (je třeba definovat), musí být poskytnuta odůvodnění.	1 2 3 4	N/A	I/II ANSP: A, dodavatel: L.
V II	Zajištění požadavků na sledovatelnost	**3.0.3**	**Zajištění sledovatelnosti (návaznosti) požadavků** Veškeré požadavky na software musí být vysledovatelné na úroveň požadovanou SWAL.	1 2 3 4	ISO/IEC 12207. ED-109/DO 278 – A3.6, A4.6, A5.6. ED-12B/DO 178B – 5.5. IEC 61508. CMMI – ReqM 1.4.	I/II ANSP: C/A, dodavatel: L.
		4.3.15	**Sledovatelnost** Projektant musí zajistit sledovatelnost (návaznost) mezi:		ISO/IEC 12207. ED-109/DO 278 – 3.1 Tab. A-1, 3.2 tab. A-2, A-3, 3-7 tab. A-7. ED-12B/DO 178B – 4.1, 4.3, 5.2, 5.3, 5.5, 11.6 až 11.11. IEC 61508 – 3-7.1.2.7, 2.1.1, 2-7.2.2, 2-7.4, 3-7.2.2, 3-7.4. CMMI – GP 2.2, 3.1, REQM 1.4, 1.5, RD 3, TS 2.1, 2.2, 3.1, PI 2.1.	I/II ANSP: C/A, dodavatel: L.
			(4.3.15.1) Systémovými a SW požadavky.	1 2 3 4		
			(4.3.15.2) SW požadavky a návrhem SW (úroveň návrhu architektury SW položek).	1 2 3 4		
			(4.3.15.3) Návrhem architektury SW a kódem.	1 2 3 4		
			(4.3.15.4) Kódem a spustitelnou aplikací.	1 2 3 4		
		5.4.10	**Sledovatelnost** Jako minimum musí být ověřena sledovatelnost (návaznost) mezi:		N/A	I/II ANSP: A, dodavatel: L.
			(5.4.10.1) Systémovými požadavky a SW požadavky.	1 2 3 4		
			(5.4.10.2) SW požadavky a návrhem SW architektury.	1 2 3 4		
			(5.4.10.3) Architekturou SW a prováděcím projektem.	1 2 3 4		
			(5.4.10.4) Prováděcím projektem a strojovým kódem.	1 2 3 4		
			(5.4.10.5) Důkazy ověření a požadavky na SW.	1 2 3 4		
			(5.4.10.6) Důkazy o zajištění bezpečnosti a verzí nasazovaného SW.	1 2 3 4		

č.	Název položky	Číslo cíle	Cíl	SWAL	Normy	Odpovědnost
VII	Zajištění nezamýšlených funkcí	**3.0.4**	**Nezamýšlené funkce** Implementace SW nesmí obsahovat funkce, které mohou nepříznivě ovlivnit bezpečnost, nebo jejichž účinek není v souladu s analýzou bezpečnosti. *Pozn.: Tento cíl neznamená, že neexistují žádné nezamýšlené funkce SW, ale že tyto funkce nejsou aktivovány, nebo že následek jejich aktivování je odůvodněn bezpečnostní analýzou.*	1 2 3 4	ED-109/DO 278 – 3.6 Tab. A-5. ED-12B/DO 178B – 6.3.4.a. IEC 61508 – 7.4.7.2.	I/II ANSP: A, dodavatel: L.
VII	Zajištění dosažení požadavků	**3.0.6**	**Zajištění naplnění požadavků** ANS software musí splňovat požadavky na něj kladené na úrovni jistoty, která je v souladu se SWAL, přidělenou při posuzování a zmírňování rizik (např. PSSA).	1 2 3 4	ED-109/DO 278 – 2.1. ED-12B/DO 178B – 5.1. IEC 61508 – 7.2.	I/II ANSP: A, dodavatel: L.
		3.4.4	**Zajištění bezpečnosti SW** Musí být poskytnut důkaz a ujištění toho, že SW požadavky jsou plněny. *Pozn.: např. formou studií bezpečnosti, studií na podporu bezpečnosti, dokladu o posouzení bezpečnosti, nebo jiných dokumentovaných výstupů v rámci systému řízení dokumentace.*	1 2 3 4	ISO/IEC 12207.	I/II ANSP: C/A, dodavatel: L.
VII	Zajištění řízení konfigurace	**3.0.7**	**Zajištění řízení konfigurace** Každé ujištění musí být vždy odvozeno ze známé spustitelné verze SW, známého rozsahu konfiguračních dat, a známých souborů SW produktů a popisů (včetně specifikace), které byly použity ve výrobě konkrétní verze SW. *Pozn.: proces řízení konfigurace.*	1 2 3 4	ISO/IEC 12207. ED-109/DO 278 – 3.8 Tab. A-8. ED-12B/DO 178B – 7. IEC 61508 – 6.2.3. CMMI – CM.	*Proces vývoje:* I/II ANSP: A, dodavatel: L. *Provoz, údržba:* I/II ANSP: L.

č.	Název položky	Číslo cíle	Cíl	SWAL	Normy	Odpovědnost
		5.2.1	**Implementace procesu řízení konfigurace** Musí být zpracován plán řízení konfigurace. Musí jako minimum zahrnovat: **(5.2.1.1)** Činnosti řízení konfigurace. **(5.2.1.2)** Postupy a časový plán pro vykonávání těchto činností. **(5.2.1.3)** Organizace odpovědné za vykonávání těchto činností a jejich vztah k jiným organizacím jako např. organizace pro vývoj nebo údržbu SW. **(5.2.1.4)** Řízení kontroly prostředí v životním cyklu SW (nástroje použité pro vývoj nebo ověření SW). **(5.2.1.4)** Definice řízení kontroly dat v životním cyklu SW (každý výstup, týkající se ujištění o bezpečnosti SW). Plán musí být dokumentován, řízen v rámci procesu řízení konfigurace a realizován.	1 2 3 4	ISO/IEC 12207. ED-109/DO 278 – 3.1 tab. A-1, 3.8 Tab. A-8, pro COTS 4.1.7 tab. 4-3. ED-12B/DO 178B – 7.1, 11.4. IEC 61508 – 1-6.2.1. CMMI – CM, 1.2, CM, GP 2.2, 2.4. 3.1.	*Vývoj:* I/II ANSP: A, dodavatel: L. *Provoz, údržba:* I/II ANSP: L.
		5.2.2	**Identifikace konfigurace** Pro identifikaci SW a jeho verzí určených ke kontrole během projektu musí být stanoveno schéma. Pro každou verzi SW musí být jako minimum identifikováno následující: **(5.2.2.1)** Základní dokumentace (baseline). **(5.2.2.2)** Reference verzí. **(5.2.2.3)** Seznam zpráv o problémech (ty, které jsou již vyřešeny (stabilní), stabilní ve specifické verzi a doposud otevřené). **(5.2.2.4)** Další identifikační detaily. Aby položky byly konfiguračně identifikovány, musí být identifikovány spolu s jejich úrovní řízení konfigurace.	1 2 3 4	ISO/IEC 12207. ED-109/DO 278 – 3.8 Tab. A-8. ED-12B/DO 178B – 5.4.3, 7.2.1, 7.2.2. IEC 61508 – 6.2.3 c). CMMI – PMC 2.1, 2.2, 2.3, CM 1.1, 2.1, 2.2, 1.3, PI 3.4.	*Vývoj:* I/II ANSP: A, dodavatel: L. *Provoz, údržba:* I/II ANSP: L.
		5.2.4	**Evidence stavu konfigurace** Musí být připraveny záznamy o řízení a zprávy o stavu, které ukazují stav a historii kontrolovaného SW včetně základny Zprávy o stavu musí zahrnovat počet změn v projektu, poslední verze SW, identifikátory release, počet release a porovnání release.	1 2 3 4	ISO/IEC 12207. ED-109/DO 278 – 3.8 tab. A-8. ED-12B/DO 178B – 7.2.6. IEC 61508 – 6.2.3. CMMI – CM 3.1.	*Vývoj:* I/II ANSP: A, dodavatel: L. *Provoz, údržba:*

č.	Název položky	Číslo cíle	Cíl	SWAL	Normy	Odpovědnost
		5.2.5	**Hodnocení konfigurace** Musí být stanoveno a zajištěno toto: funkční úplnost SW ve srovnání s požadavky na něj a fyzická úplnosti SW.	1 2 3 4	ISO/IEC 12207. ED-109/DO 278 – 3.8 tab. A-8. ED-12B/DO 178B – 7.2.4. IEC 61508 – 6.2.3. CMMI – CM 3.2.	I/II ANSP: L.
		5.2.6	**Řízení a dodávka release** Proces dodávky a release SW musí existovat a musí být dokumentován. Release a dodávka SW produktů a dokumentace se musí formálně kontrolovat. Originální kopie kódu a dokumentace musí být udržovány po celý život SW produktu. *Pozn.: Kód a dokumentace obsahující funkce kritické pro bezpečnost nebo ochranu by měly být ošetřovány, ukládány, baleny a dodávány v souladu s politikou zainteresovaných organizací.*	1 2 3 4	ISO/IEC 12207. ED-109/DO 278 – 3.8 tab. A-8. ED-12B/DO 178B – 7.2.7, 7.2.8, 5.4.3. IEC 61508 – 6.2.3. CMMI – CM 1.2, 2.	*Vývoj:* I/II ANSP: A, dodavatel: L. *Provoz, údržba:* I/II ANSP: L.
		5.2.9	**Řízení konfigurace SW jednotky** Řízení konfigurace SW musí být prováděno na úrovni SW jednotky.	1 2 3 4	N/A	
		5.2.10	**Sledovatelnost řízení konfigurace** Data životního cyklu SW (každý výstup) musí být dohledatelná mezi verzemi. Všechna data v životním cyklu SW musí být dohledatelná k verzi SW, která je provozována.	1 2 3 4	N/A	*Vývoj:* I/II ANSP: A, dodavatel: L. *Provoz, údržba:* I/II ANSP: L.
		5.2.11	**Řízení konfigurace na úrovní zdrojového kódu** Řízení konfigurace SW musí být provedeno na úrovni zdrojového kódu SW.	1 2 3 4	N/A	*Vývoj:* I/II ANSP: A, dodavatel: L. *Provoz, údržba:* I/II ANSP: L.

č.	Název položky	Číslo cíle	Cíl	SWAL	Normy	Odpovědnost
		5.4.13	**Ověřování procesu načítání a release SW** Procesy pro načtení a release SW musí být ověřeny.	1 2 3 4	N/A	I/II ANSP: A, dodavatel: L.
V II	Zajištění vývoje (plán vývoje SW)	**4.3.3**	**Proces vývoje – implementace** Musí být definován životní cyklus SW odpovídající rozsahu, významu a složitosti projektu a musí být součástí procesu řízení konfigurace. Musí zahrnovat minimálně: • kritéria pro ukončení činnosti/ fáze pro každou činnost/fázi, • společný technický přezkum se pro každou činnost/fázi. Normy, metody, nástroje a počítačové programovací jazyky se zvolí a použijí dle úrovně zajištění SW (SWAL). *Pozn.: Implementační proces zahrnuje definici životního cyklu, výstupní dokumentace, řízení konfigurace, problémy SW produktů, definice prostředí, plán vývoje, COTS.*	1 2 3 4	ISO/IEC 12207. ED-109/DO 278 – 3.1 Tab. A-1, A-3. ED-12B/DO 178B – 5.1, 5.5, 11.6, 11.9, 11.10. IEC 61508 – 3-7.2. CMMI – RD 2.1, 2.3, 3.3, TS 2.1, REQM 1.4.	I/II ANSP: C/A, dodavatel: L.
		4.3.4	**Analýza požadavků na SW** Projektant musí stanovit a dokumentovat SW požadavky, použité SW standardy/pravidla, jak je definováno v 4.3.9 a 4.3.10. SW požadavky musí jako minimum: **(4.3.4.1)** Specifikovat funkční chování SW, kapacitu, přesnost, časovou výkonnost SW zdroje používaného na cílovém HW robustnost vůči nestandardním stavům, toleranci k přetížení. **(4.3.4.2)** Být kompletní a správné. **(4.3.4.3)** Vyhovovat systémovým požadavkům. **(4.3.4.4)** Identifikovat rozsah konfiguračních/adaptačních dat.	1 2 3 4	ISO/IEC 12207. ED-109/DO 278 – 3.2 Tab. A-2, 4.1.4, 4.1.9. ED-12B/DO 178B – 3, 4, 11.1, 11.2. IEC 61508 – 3-7.1.2, 3-7.4.1. CMMI – PP 1.1, 1.3, 2, 2.4, GP 2.2, 3.1, PI, Ver.	I/II ANSP: C/A, dodavatel: L.
		4.3.5	**Návrh architektury SW** Projektant musí transformovat požadavky na SW do architektury, která popisuje jeho strukturu nejvyšší úrovně a identifikuje SW složky. *Pozn. Rozsah tohoto cíle je vymezení nejvyšší úrovně SW architektury, vrcholové úrovně návrhu rozhraní, definování SW integrace a definování kritérií SW architektury.*	1 2 3 4	ISO/IEC 12207. ED-109/DO 278 – 3.2 Tab. A-2. ED-12B/DO 178B – 5.2, 5.5, 11.7, 11.10. IEC 61508 – 3-7.4. CMMI – TS 1.1, 1.3. 2.1, 2.2, 2.3, RD 2.2, REQM 1.4, PI 2.1.	I/II ANSP: C/A, dodavatel: L.

č.	Název položky	Číslo cíle	Cíl	SWAL	Normy	Odpovědnost
		4.3.6	**Proces vývoje – detailní návrh SW** Projektant musí vytvořit detailní návrh pro každou SW komponentu (část) programového vybavení s použitím standardů/pravidel návrhu SW.	1 2 3 4	ISO/IEC 12207. ED-109/DO 278 – 3.2 tab. A-2, 3.5 Tab. A-5, 3.6 Tab. A-6, 3-7 tab. A-7. ED-12B/DO 178B – 5.2,5.3, 5.5, 11.7, 11.8, 11.10, 11.11. IEC 61508 – 3-7.4. CMMI – TS 2.1. 2.2, 2.3, 3.1, Ver., REQM 1.4.	I/II ANSP: C/A, dodavatel: L.
		4.3.7	**Proces vývoje – Integrace SW** Musí být vypracován plán integrace pro integraci softwarových jednotek a komponent do softwaru. Plán musí zahrnovat požadavky na testování, procedury, data, odpovědnost a časový plán. Plán musí být dokumentován. *Pozn.: Obsahem tohoto cíle je vytvoření plánu integrace SW, definice integrace SW, uživatelské příručky, příprava validace SW, hodnocení (evaluace) integrace SW (částečně).*	1 2 3 4	ISO/IEC 12207. ED-109/DO 278 – 3.1 tab. A-1. ED-12B/DO 178B – 5.4. IEC 61508 – 3-7.4. CMMI – PI 1, 1.1, 1.3, 3.2, 3.3, Ver. 1.3, GP 2.2, 2.3, 3.1, PI GP 2.2, 2.3, 3.1, TS 2.1, 3.1, 3.2, PP 3.1, REQM 1.4.	I/II ANSP: C/A, dodavatel: L.
		4.3.8	**Proces vývoje – instalace SW** Plán integrace musí být vypracován pro instalaci SW produktu v cílovém prostředí tak, jak je určeno v kontraktu. Musí být určeny a musí být dostupné zdroje a informace nutné pro instalaci SW produktu.	1 2 3 4	ISO/IEC 12207. IEC 61508 – 1-7.9, 1-7.13. CMMI – PI 1, PP 2, PI GP 2.2, 2.3, 3.1, PI 3.4.	I/II ANSP: C/A, dodavatel: L.
		4.3.9	**Definice standardů/pravidel** ***Plán vývoje*** Projektant musí vypracovat plány pro řídící aktivity procesu vývoje. Plány musí jako minimum zahrnovat specifikaci standardů/pravidel, metody, nástroje, činnosti a odpovědnosti spojené s vývojem a validací (potvrzení zkouškou) všech požadavků, včetně bezpečnosti. Bude-li to nutné, mohou být vytvářeny oddělené plány. Tyto plány musí být dokumentovány a realizovány.	1 2 3 4	ISO/IEC 12207. ED-109/DO 278 – 3.1 Tab. A-1, A-2, pro COTS 4.1.4.2., 3.2 tab. A-2, A-3, A-4, 3-6 tab. A-6, 3-7 tab. A-7. ED-12B/DO 178B – 4.1, 4.2, 4.4, 4.5, 5.3, 5.4.3, 5.5, 6.4.3, 11.2, 11.6, až 11.11. IEC 61508 – 3-7.1.2.6, 3-7.4, 3 Annex A, B, 4.4, 3-7.2.2. CMMI – TS, TS 3.1, PP 2.4, IPM 1.1, GP 2.2, 2.3, 3.1, RD, REQM 1.4, PI 1.2.	I/II ANSP: C/A, dodavatel: L.

č.	Název položky	Číslo cíle	Cíl	SWAL	Normy	Odpovědnost
		4.3.10	**Standardy/pravidla** ***Plán vývoje SW (standardy/pravidla):*** Projektant musí identifikovat:		ISO/IEC 12207. ED-109/DO 278 – 3.1 Tab. A-1, 3.2 tab. A-2, A-3, A-4, 3-6 tab. A-6, 3-7 tab. A-7. ED-12B/DO 178B – 4.1, 4.2, 4.4, 4.5, 5.3 až 5.5, 6.4.3, 11.2, 11.6, 11.7, 11.8, 11.10, 11.11. IEC 61508 – 3-7.1.2.6 Annex A, B, 3-7.4, 3-7.2.2. CMMI – TS, TS 3.1, PP 2.4, IPM 1.1, GP 2.2, 2.3, 3.1, RD, REQM 1.4, PI 1.2.	I/II ANSP: C/A, dodavatel: L.
			(4.3.10.1) Požadavky SW standardů/pravidel (minimálně v rozsahu 4.3.4).	1 2 3 4		
			(4.3.10.2) Standardy/pravidla návrhu SW.	1 2 3 4		
			(4.3.10.3) Standardy/pravidla kódování SW.	1 2 3 4		
			(4.3.10.4) Odkazy na standardy/pravidla pro dříve vyvinutý SW, včetně SW COTS, pokud jsou tyto standardy/pravidla odlišná.	1 2 3 4		
		4.3.11	**Řízení požadavků na vývoj** ***Vývojové prostředí SW*** Projektant musí definovat vybrané vývojové prostředí SW z hlediska: **(4.3.11.1)** Vybraných požadavků metod vývoje, procedur a nástrojů (jestliže existují), které budou používány. **(4.3.11.2)** HW platformy pro nástroje (pokud je nějaká), která bude použita. *Pozn.: Metody jsou např. SADT (funkční modelování/návrh), SART (SADT for Real-Time), OOD (objektově orientovaný návrh), atd.*	1 2 3 4	ISO/IEC 12207 ED-109/DO 278 – 3.1 Tab. A-1, 3.2 tab. A-2, A-3, A-4. ED-12B/DO 178B – 4.1, 4.2, 4.4, 4.5, 11.6. IEC 61508 – 3-7.1.2.6 Annex A, B, 3-7.4.4, 3-7.2.2. CMMI – PP 2.4, IPM 1.1, GP 2.2, 2.3, 3.1, RD.	I/II ANSP: C/A, dodavatel: L.
		4.3.13	**Řízení zdrojů** **(4.3.13.1)** Pro účely bezpečnosti musí být specifikována nezbytná rezerva s ohledem na využití zdrojů (paměť, výkon CPU, ovladače, atd.).	1 2 3 4	ISO/IEC 12207. ED-109/DO 278 – 3.2 tab. A-2, 3.6 tab.A-6. ED-12B/DO 178B – 5.2, 5.4, 5.5, 11.7, 11.10. IEC 61508 – 3-7.4, 3-7.5. CMMI – TS 1.1,1.3, 2.1, 2.2, RD 2.2, REQM 1.4, PI 2.1, 1.3.	I/II ANSP: C/A, dodavatel: L.
			(4.3.13.2) Rezerva musí být měřitelná nebo ověřitelná s cílem vyhovění specifikaci.	1 2 3 4		
			(4.3.13.3) Pokud více SW sdílí stejné zdroje, pak musí být rezerva hodnocena na systémové úrovni.	1 2 3 4		

č.	Název položky	Číslo cíle	Cíl	SWAL	Normy	Odpovědnost
		4.3.14	**Zdůvodnění volby návrhu** Projektant musí definovat real-time vlastnosti SW komponent na úrovni návrhu architektury. Musí být definován soubor následujících vlastností: **(4.3.14.1)** Run-time úkoly a aspekty (priority, události, komunikace, atd.). **(4.3.14.2)** Přerušení (priority, řízení zpoždění, dohled SW, atd.). **(4.3.14.3)** Ošetření chyb (mechanismus detekce a obnovení, atd.). **(4.3.14.4)** Správa dat (mechanismy ochrany a zablokování, atd.). **(4.3.14.5)** Spuštění/zastavení (výměna dat během těchto fází).	1 2 3 4	ISO/IEC 122077. ED-109/DO 278 – 3.1 Tab. A-1, 3.2 tab. A-2, 3.6 tab. A-6. ED-12B/DO 178B – 4.4, 4.5, 5.2, 5.4, 5.5, 11.7. IEC 61508 – 3-7.1.2.6, Annex A, B, 3-7.4, 3-7.5. CMMI – PP 2.4, IPM 1.1, GP 2.2, 2.3, 3.1, TS 2.1, 2.2, REQM 1.4, PI 2.1, 1.3.	I/II ANSP: C/A, dodavatel: L.
		4.3.16	**Proces vývoje** **Ověření/kritéria přechodu** **(4.3.16.1)** Projektant musí popsat procesy životního cyklu SW použité v projektu, včetně přechodových kritérií pro procesy vývoje SW.	1 2 3 4	ISO/IEC 12207. ED-109/DO 278 – 3.1 Tab. A-1, 2, 3, 4.1.4.2, 5.1. ED-12B/DO 178B – 3, 2.2, 4.1, 4.2, 4.3, 11.1, 11.2. IEC 61508 – 3-7.1.2.1 až 3-7.1.2.5, CMMI – PP 1.3, 2.1, PP 2, 2.1, PMC, PMC 1.1, IPM 1.1, 1.3, 1.4, GP 2.2, 2.3, 3.1.	I/II ANSP: C/A, dodavatel: L.
			(4.3.16.2) Všechny základní informace z fáze životního cyklu SW potřebné pro správnou činnost v další fázi musí být dostupné a ověřené. *Pozn.: Viz také kritéria hodnocení pro specifikaci, návrh, kód, testování a integraci.*	1 2 3 4		
			(4.3.16.3) Přechodová kritéria pro všechny fáze musí být definována.	1 2 3 4		
			(4.3.16.4) Musí být definována přechodová kritéria pro analýzu požadavků a verifikační fáze.	1 2 3 4		
		4.3.20	**Omezení kvůli složitosti** Úroveň složitosti (stejně jako vybraná kritéria definující tuto složitost) musí být definována a měřena. *Pozn.: Proces návrhu SW, proces kódování, sledovatelnost, standardy pro návrh SW, standardy pro kódování SW, zdrojový kód, atd.*	1 2 3 4	ED-12B/DO 178B – 5.2, 5.3, 5.5, 11.7, 11.8, 11.11. IEC 61508 – 3-7.2.2, 3-7.4. CMMI – RD 3.3, REQM 1.4, TS 2.1, 2.2, 3.1, 3.2, PI 1, 2.1, PI GP 2.2, 3.1, PP 3.1.	I/II ANSP: C/A, dodavatel: L.

č.	Název položky	Číslo cíle	Cíl	SWAL	Normy	Odpovědnost
V II	Zajištění údržby	**4.5.1**	**Proces údržby** **Implementace procesu údržby** Musí být nastavěn a prováděn proces údržby. Údržba zasahující do SW musí podléhat procesu posouzení a zmírnění rizika.	1 2 3 4	ISO/IEC 12207. IEC 61508 – 1-6.2.1, I-7.7, I-7.15. CMMI – PP 2.	I/II ANSP: L, dodavatel: C.
		4.5.3	**Dodržení SWAL** Při provádění údržby musí správce zajistit, že každá aktivita údržby je provedena v souladu s přiděleným SWAL. *Pozn. Nejen proces údržby, ale i další procesy musí být zahrnuty.*	1 2 3 4	ISO/IEC 12207. IEC 61508 – 7.8, I-7.16. CMMI – CM 1.3, 3.2.	I/II ANSP: L, dodavatel: C.
V II	Zajištění verifikace (ověření výsledků procesu verifikace)	**5.4.1**	**Ověřování implementace procesu** Musí být zaveden proces ověřování (verifikace) SW. Výstup z procesu ověřování musí být zdokumentován a distribuován zainteresovaným stranám. *Pozn.: Měly by být určeny cílové činnosti životního cyklu SW a SW produkty vyžadující ověřování. Pro cílové činnosti a SW produkty jsou poté vybrány činnosti ověřování a úlohy (např. ověřování kontraktu, procesu, požadavků, návrhu, kódu, integrace, dokumentace) zahrnující metody, techniky a nástroje provedení úloh. Na základě určených úloh je vytvořen plán ověřování (viz 5.4.2), který mimo jiné obsahuje i postupy pro zasílání zpráv o ověřování akvizitérovi a ostatním stranám.*	1 2 3 4	ISO/IEC 12207. ED-109/DO 278 – 3.1 tab. A-1, 3.4, 3.5, 3.7, 3-7 tab. A-7, 3.10 tab. A-10. ED-12B/DO 178B – 2.7, 6, 6.1, 11.3. IEC 61508 – 7.4.1.5, 7.9.2, 1-7.4, 1-7.6, 1-7.8, 1-7.18, I-7.14, 2-7.7.2.3, II-7.7.2. CMMI – GP 2.2, 3.1, Ver. 1, 2, 3, RD 3.3, 3.5, REQM 1.5, Val 1.3, 2.	I/II ANSP: A, dodavatel: L.

č.	Název položky	Číslo cíle	Cíl	SWAL	Normy	Odpovědnost
		5.4.2	**Plán ověřování** Musí být definován plán ověřování (verifikace). Plán musí obsahovat činnosti životního cyklu a SW produkty podléhající ověřování, požadované úlohy ověřování pro každou činnost životního cyklu a SW produkt a příslušné zdroje, odpovědnosti a časový plán. Tento plán musí dále obsahovat postupy pro zasílání zpráv o ověřování akvizitérovi a ostatním zainteresovaným stranám s uvedením opatření, která mají být přijata každou stranou. *Pozn.: Plán ověřování může obsahovat popis různých typů testování v jednotlivých fázích životního cyklu SW (FAT, SAT, testování software. Cíle týkající se ověření konfiguračních / adaptačních dat mohou být rozšířeny v provozním procesu (viz cíle 4.4.X). Strategie pro ověření vhodné kombinace konfiguračních / adaptačních by ale měla být součástí plánu ověřování.*	1 2 3 4	ISO/IEC 12207. ED-109/DO 278 – 3.1 tab. A-1, 2.1, 3.3 tab. A-3, 3.4 tab. A-4, 3.7 tab. A-7, 3.9 tab. A-9, 3.10 tab. A-10. ED-12B/DO 178B – 2.2, 2.3, Annex A, 6.1, 11.3. IEC 61508 – 7.4.1.5, 7.9.2, 1-7.4, 1-7.6, 1-7.18. CMMI – GP 2.2, 2.3, 3.1, Ver. 1, Ver. 1.3, 2, 3, PP 1.3, PMC 1, 2, IPM 1.3, 1.4, 2, CM 2.1, PPQA 1, SAM 1.2, REQM 1.1, 1.3, RD 3.3 až 3.5, PMC GP 2.2, 2.4, 3.1, 2.7.	I/II ANSP: A, dodavatel: L.
		5.4.12	**Ověřování a výsledky procesu ověřování** Testovací případy, postupy a výsledky musí být ověřovány takto:		ISO/IEC 12207. ED-109/DO 278 – 3.5 tab. A-5, 3.6 tab. A-6, 3.7 tab. A-7. ED-12B/DO 178B – Annex A-7, 5.3, 6.3, 6.4 IEC 61508 – 7.4, 7.7, 1-5.2, 1-7.8, I-7.14, 2-7.7. CMMI –Ver. 1, 2, 3, Val 2, TS 2.1, 3.1, REQM 1.4, Ver. GP 2.9, PI GP 2.8, 2.9, CM 3, GP 2.6.	I/II ANSP: A, dodavatel: L.
			(5.4.12.1) Postupy ověřování jsou správné a úplné a rozdíly jsou odůvodněny.	1 2 3 4		
			(5.4.12.2) Výsledky ověření jsou správné a úplné a rozdíly jsou odůvodněny.	1 2 3 4		
			(5.4.12.3) Ověření testovacích případů pro požadavky na SW, souvisejících postupů a výsledků je správné a úplné, a rozdíly jsou odůvodněny.	1 2 3 4		
			(5.4.12.4) Ověření testovacích případů pro návrh SW (úroveň architektury), souvisejících postupů a výsledků je správné a úplné, a rozdíly jsou odůvodněny.	1 2 3 4		
			(5.4.12.5) Ověření testovacích případů pro návrh SW (podrobný návrh), souvisejících postupů a výsledků je správné a úplné, a rozdíly jsou odůvodněny.	1 2 3 4		

č.	Název položky	Číslo cíle	Cíl	SWAL	Normy	Odpovědnost
			(5.4.12.6) Ověření testovacích případů pro integraci SW, souvisejících postupů a výsledků je správné a úplné, a rozdíly jsou odůvodněny.	1 2 3 4		
			(5.4.12.7) Ověření testovacích případů dat SW, souvisejících postupů a výsledků je správné a úplné.	1 2 3 4		
			(5.4.12.8) Ověření postupů ověřování sledovatelnosti a výsledků je správné a úplné a rozdíly jsou odůvodněny.	1 2 3 4		
V II	Zajištění kvality	**5.3.1**	**Proces zajištění kvality - implementace procesu** Musí být zaveden proces zajišťování kvality, přizpůsobený projektu. Cíle procesu zabezpečení kvality musí být stanoveny tak, aby zajistily, že SW produkty a procesy využívané pro poskytování těchto SW produktů budou v souladu se stanovenými požadavky a budou se dodržovat stanovené plány. Musí být zpracován, dokumentován, implementován a udržován plán pro vedení činností a úloh v procesu zabezpečování kvality pokrývající životní cyklus SW. *Pozn.: Metodika procesu zajišťování kvality např. viz ISO 9001 v platném znění.*	1 2 3 4	ISO/IEC 12207. ED-109/DO 278 – 3.1 tab. A-1. ED-12B/DO 178B – 8.1, 8.2, 11.5. IEC 61508 –7.1.2.2, 1-6.2.5, I-8. CMMI – PPQA GP 2.2, 3.1.	I/II ANSP: A, dodavatel: L.
		5.3.2	**Proces zajištění kvality – zabezpečování produktu** Musí být zajištěno, že všechny plány (definované v normě ED-153, nebo stanovené metodikou dodavatele a v ANSP SMS) jsou definovány, vzájemně se shodují a jsou naplňovány tak, jak je požadováno. Musí být provedeno přezkoumání shody SW.	1 2 3 4	ISO/IEC 12207. ED-109/DO 278 – 3.1 tab. A-1, 3.9 tab. A-9. ED-12B/DO 178B – 8.3. CMMI – GP 2.9, PPQA 2.	I/II ANSP: A, dodavatel: L.
		5.3.3	**Proces zajištění kvality – zabezpečování procesu** Musí být zajištěno, že procesy životního cyklu SW (dodání, vývoj, provozování, údržba a podpůrné procesy včetně zajištění kvality) využívané pro projekt jsou v souladu s kontraktem a dodržují plány.	1 2 3 4	ISO/IEC 12207. ED-109/DO 278 – 3.9 tab. A-9. ED-12B/DO 178B – 8.2. CMMI – GP 2.9, PPQA 1.	I/II ANSP: A, dodavatel: L.

č.	Název položky	Číslo cíle	Cíl	SWAL	Normy	Odpovědnost
		6.3.1	**Proces zlepšování – zřízení procesu** Organizace musí vytvořit sadu organizačních procesů pro veškeré procesy životního cyklu SW. Procesy a jejich aplikace v konkrétních případech musí být dokumentovány ve firemní dokumentaci. Podle potřeby musí být stanoveny kontrolní mechanismy procesu za účelem rozvoje, monitorování, kontroly a zlepšování procesu/ů.	1 2 3 4	ISO/IEC 12207. CMMI – OPD 1.3, 2.1, OPD GP 2.6, OPF.	I/II ANSP: A, dodavatel: L.
		6.3.2	**Proces zlepšování – posuzování procesu** Musí být definován, dokumentován a uplatňován postup pro posuzování (měření) procesů. Záznamy o posouzení musí být uchovávány a udržovány. Organizace musí plánovat a provádět přezkum procesů ve vhodných intervalech za účelem zajištění jejich neustálé vhodnosti a účinnosti s ohledem na výsledky posouzení.	1 2 3 4	ISO/IEC 12207. CMMI – OPF 1.2.	I/II ANSP: A, dodavatel: L.
		6.3.3	**Proces zlepšování – zdokonalování procesu** Organizace musí uskutečnit taková zlepšení procesů, která jsou stanovena jako nezbytná na základě posouzení procesů a výsledků přezkumu. Dokumentace procesu musí být aktualizována tak, aby odrážela zlepšení organizačních procesů. *Pozn.: Pro zjištění slabých a silných míst v používaných procesech by se měla sbírat a analyzovat data.*	1 2 3 4	ISO/IEC 12207. CMMI – OPF 1.3, 2.1, 2.2.	I/II ANSP: A, dodavatel: L.
V II	Zajištění, že SW je přijatelně bezpečný	**3.0.16**	**Zajištění naplnění cílů** Organizace musí vytvořit potřebné záruky pro NSA, které prokazují, že cíle dle přiděleného SWAL byly splněny.	1 2 3 4	N/A	I/II ANSP: L.

Tabulka č.3. *Varianta orientovaná na projekt*

Záměrně nepoužito.

4. Literatura

- ED-153 „Guidelines for ANS Software Safety Assurance
- DO-278/ED-109 „Software Standard for non-Airborne Systems“
- ED-12B/DO-178B „Software Considerations in Airborne Systems and Equipment Certification“
- ISO/IEC 12207 „Informační technologie - Procesy v životním cyklu softwaru“

Záměrně nepoužito.