ÚŘAD PRO OBRANNOU STANDARDIZACI,
KATALOGIZACI A STÁTNÍ OVĚŘOVÁNÍ JAKOSTI

ČESKÝ OBRANNÝ STANDARD

051667 **1. vydání** **Změna 2**	**INSTRUKCE PRO VYTVÁŘENÍ POŽADAVKŮ NA SPOLEHLIVOST**

ZAVÁDÍ	ADMP-01, Ed. B GUIDANCE FOR DEVELOPING DEPENDABILITY REQUIREMENTS Pokyny pro tvorbu požadavků spolehlivosti
NAHRAZUJE	ČOS 051667, 1. vydání, Změna 1 INSTRUKCE PRO VYTVÁŘENÍ POŽADAVKŮ NA SPOLEHLIVOST

Praha 2022

(VOLNÁ STRANA)

ČOS 051667
1. vydání
Změna 2

ČESKÝ OBRANNÝ STANDARD

INSTRUKCE PRO VYTVÁŘENÍ POŽADAVKŮ NA SPOLEHLIVOST

Základem pro tvorbu tohoto standardu byly originály následujících dokumentů:

ADMP-01, Ed. B	GUIDANCE FOR DEVELOPING DEPENDABILITY REQUIREMENTS Pokyny pro tvorbu požadavků spolehlivosti
STANREC 4174, Ed. 5	GUIDANCE FOR DEPENDABILITY MANAGEMENT Pokyny pro řízení spolehlivosti

Praha 2022

OBSAH

Table of Contents

Předmět standardu

ČOS 051667, 1. vydání, Změna 2, zavádí ADMP-01, Ed. B (GUIDANCE FOR DEVELOPING DEPENDABILITY REQUIREMENTS, česky Pokyny pro tvorbu požadavků spolehlivosti) do prostředí České republiky. Účelem tohoto dokumentu je poskytnout návod pro vytváření požadavků na spolehlivost. Vysvětluje, jaké potřeby jsou uvažovány pro spolehlivostní část specifikace pro akvizici a proč je důležitá. Charakteristiky spolehlivosti jakékoli položky jsou neoddělitelně spjaty s jejím návrhem, proto má být spolehlivost sledována od počátku předkoncepční etapy a má pokračovat přes celý životní cyklus takovým způsobem, že se zavedou pravidla pro realizaci spolehlivosti, jak je popsáno v řadě norem IEC 60300. Na ty se také kapitola 1.4 tohoto standardu odvolává. Standard poskytuje šablonu, ze které mohou být jednoduše vybrány všechny nové požadavky a bere v úvahu koncepce, sporné body a faktory, které ovlivní nastavení požadavků.

Standard je vydán jako česko-anglická verze ADMP-01, Ed. B.

Nahrazení standardů (norem)

Tento standard nahrazuje ČOS 051667, 1. vydání, Změna 1.

Související dokumenty

V tomto ČOS jsou normativní odkazy na následující citované dokumenty (celé nebo jejich části), které jsou nezbytné pro jeho použití. U odkazů na datované citované dokumenty platí tento dokument bez ohledu na to, zda existují novější vydání/edice tohoto dokumentu. U odkazů na nedatované citované dokumenty se používá pouze nejnovější vydání/edice dokumentu (včetně všech změn).

IEC 60300-1, Ed. 2	Dependability Management – Part 1: Dependability management systems
ČSN EN 60300-1	Management spolehlivosti - Část 1: Návod pro management a použití
IEC 60300-3-10, Ed. 1	Dependability Management Part 3-10: Application guide – Maintainability
ČSN IEC 60300-3-10	Management spolehlivosti – Část 3-10: Návod k použití – Udržovatelnost
IEC 60300-3-15, Ed. 1	Dependability Management Part 3-15: Application guide – Engineering of System Dependability
ČSN EN 60300-3-15	Management spolehlivosti – Část 3-15: Pokyn k použití – Inženýrství spolehlivosti systémů
IEC 60706-2, Ed. 2	Maintainability of equipment – Part 2: Maintainability requirements and studies during the design and development phase
ČSN EN 60706-2	Udržovatelnost zařízení – Část 2: Požadavky na udržovatelnost a studie udržovatelnosti v etapě návrhu a vývoje

IEC 60706-5, Ed. 2	Maintainability of equipment – Part 5: Testability and diagnostic testing
ČSN EN 60706-5	Udržovatelnost zařízení – Část 5: Testovatelnost a diagnostické zkoušení
IEC 62628, Ed. 1	Guidance on software aspects of dependability
ČSN EN 62628	Návod pro softwarová hlediska spolehlivosti
ISO/IEC 25000:2005[1]	Software Engineering – Software Product Quality Requirements and Evaluation (SQuaRE) – Guide to SQuaRE
ISO/IEC 25010:2011	Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – System and software quality models
ADMP-02, Ed. B	Guidance for Dependability In-Service Pokyny pro řízení spolehlivosti
AAP-20, Ed. C	NATO Programme Management Framework (NATO Life Cycle Model)
ČOS 051662, 3. vydání, Změna 1	Systém managementu programu NATO (NATO model životního cyklu)
AAP-48, Ed. B	NATO System Life Cycle Processes
ČOS 051655, 2. vydání	Procesy životního cyklu systémů v NATO
IEC 60050-192:2015	International Electrotechnical Vocabulary (IEV) – Part: 192: Dependability
ČSN IEC 60050-192	Mezinárodní elektrotechnický slovník – Část 192: Spolehlivost

Zpracovatel ČOS

Vojenský výzkumný ústav, s. p., RNDr. Milan Čepera, Ph.D. Změnu 1 a 2 zpracoval RNDr. Milan Čepera, Ph.D.

[1] Norma ISO/IEC 25000:2005 byla zrušena a nahrazena normou ISO/IEC 25000:2014.

Použité zkratky, značky a definice

Zkratky

Zkratka	Český název	Název v originálu
ATR	aktivní doba opravy	Active Repair Time
BIT	zabudovaný test	Built-In Test
COTS	komerčně nakupovaný materiál, komerčně pořizovaný majetek	Commercial Off The Shelf
FMECA	analýza způsobů, důsledků a kritičnosti poruch	Failure Modes Effect and Criticality Analysis
FTA	analýza stromu poruchových stavů	Fault Tree Analysis
GSN	strukturovaný zápis cílů	Goal Structuring Notation
IEC	Mezinárodní elektrotechnická komise	International Electrotechnical Commission
IT	informační technologie	Information Technology
MART	střední doba aktivní opravy	Mean Active Repair Time
MTBF	střední doba mezi poruchami	Mean Time Between Failure
MTTF	střední doba do poruchy	Mean Time To Failure
MTTR	střední doba do opravy	Mean Time To Repair
NATO	Organizace severoatlantické smlouvy	North Atlantic Treaty Organization
PAPS	Příručka pro postupné plánování vyzbrojování	Phased Armaments Programming System
TTR	doba do opravy	Time To Repair

Definice

Není využito. Not utilized.

1 Úvod

1.1 Všeobecně

1. Spolehlivost je klíčovou charakteristikou všech položek[3] mající přímý dopad na provedení úkolu, a takto i na úspěch úkolu. Charakteristiky spolehlivosti jakékoli položky[2] jsou neoddělitelně spjaty s jejím návrhem, jinými slovy spolehlivost má být uvažována od úplného počátku předkoncepční etapy a má pokračovat disciplinovaným způsobem během celého životního cyklu zavedením pravidel pro spolehlivost, jak je popsáno v řadě norem IEC 60300, na které se odvolává kapitola 1.4 tohoto standardu.

2. Spolehlivost je souhrnný pojem charakterizující nepřetržitý a bezpečný provoz jakékoli jednoduché nebo složité položky. Faktory, které ovlivňují provedení spolehlivosti jakékoli položky, jsou bezporuchovost, udržovatelnost, pohotovost, testovatelnost, údržba a bezpečnost. U mnoha položek je bezporuchovost a udržovatelnost klíčovou charakteristikou provedení, neboť mají přímý dopad na úspěch úkolu a na náklady životního cyklu. Strategie logistiky a udržovatelnosti položky jsou obvykle navrženy externě, ale mohou mít významný dopad na provedení jejich pohotovosti, neboť zobrazují způsobilost poskytovat nezbytné zdroje k zavedení optimalizovaných postupů údržby vytvořených a zlepšovaných v průběhu životního cyklu položky.

3. Stejně jako všechny ostatní charakteristiky provedení definované pro pořizování, je potřebné ty, které se vztahují ke spolehlivosti, řádně prozkoumat a promyslet, aby mohly být logicky specifiko-

1 INTRODUCTION

1.1 General

1. Dependability is a key characteristic of all items[3], having a direct impact on mission performance and thus mission success. The dependability characteristics of any item are inherent in its design, thus dependability should be considered from the very beginning of the pre-concept stage and be continued, in a disciplined manner, throughout the whole life cycle by the implementation of dependability disciplines as described in the IEC 60300 series standards referenced at Section 1.4 in this document.

2. Dependability is the collective term describing the continued and safe operation of any simple or complex item. The factors that influence the dependability performance of any item are reliability, maintainability, availability, testability, maintenance, and safety. In most items reliability and maintainability are the key performance characteristics of interest as they have a direct impact on mission success and life cycle cost. The logistic and maintenance strategy of the item are mainly external, but can have significant impact on its availability performance, as it reflects the ability to provide the necessary resources to implement optimised maintenance procedures developed and refined through the life cycle of the item.

3. In the same way as all other performance characteristics defined in procurements, those relating to dependability need to be properly researched and considered in order that

[2] Výraz „item“ je v příslušných ČSN překládán jako „objekt“. V ČOS řady 0516 je překládán vždy jako „položka“. Oba pojmy jsou v této souvislosti ekvivalentní.

[3] Položka zahrnuje systémy a vybavení, ať už hardwarové nebo softwarové, a služby.
Item includes systems, equipment, be it hardware or software based, and services.

vány, aby dodávaly požadované úrovně. Toho se dociluje pomocí specifikování přesné pohotovosti, bezporuchovosti, udržovatelnosti nebo dalších souvisejících požadavků a uvědomění si, že změna jakéhokoli jednoho může mít významný dopad na jakoukoli nebo všechny ostatní výše uvedené a na celkovou spolehlivost položky. Tyto požadavky potřebují být reálné pro typ položky, který je uveden ve smlouvě, specifické a měřitelné způsobem, kterého lze dosáhnout v dostupném čase a bez nepříznivého dopadu na celkovou cenovou dostupnost projektu. Je důležité zajistit, aby se požadavky rozpadaly na dílčí komponenty položek logickým a vyváženým způsobem tak, aby bylo možné odvodit plné porozumění všem charakteristikám spolehlivosti. I když si plně uvědomujeme, že životy vojenského personálu mohou být závislé na položce úspěšně pokračující v práci, je důležité zajistit, že tyto požadavky nejsou předimenzovány. Nastavení požadavků na 98% bezporuchovost nebo 99% pravděpodobnost přežití 48 hodinového úkolu asi významně vyžene ceny do výše a může se stát, že nižší čísla budou mít malý reálný dopad na provozní tempo a mohla by být mnohem lépe dosažitelná a cenově dostupná.

4. Je důležité si uvědomit rozdíl mezi požadavkem a záměrem nebo cílem, což jsou pojmy, mající velmi různé významy, a přesto se často používají, bez očividného rozpoznání následků. Požadavek je něco, co je nezbytné ke zdárnému provozu položky a nemá být zaměňováno bez plného uvážení následků a souhlasu všech zainteresovaných stran. Bude zapotřebí, aby dodavatel poskytl důkaz se zdůvodněním, že požadavky byly splněny, nebo tam, kde nemohou být splněny, důkaz na podporu zmírnění požadavku a proč se nyní dodavatel nedomnívá, že odsouhlasená specifikace nemůže být dodržena. Záměr nebo cíl je něco, co je

they can be specified in a coherent way to deliver the required levels. This is achieved through specifying specific availability, reliability, maintainability or other related requirements and recognising that a change to any one can have significant knock on effects on any or all of the others and the overall dependability of the item. These requirements need to be realistic for the type of item that is under contract, specific and measurable in a way that can be achieved within the time available and without adversely impacting the overall affordability of the project. It is important to ensure that requirements are flowed down to sub-components of the item in a coherent and balanced way so that a full understanding of the dependability characteristics can be derived. Whilst it is fully recognised that the lives of military personnel may be reliant on the item continuing to work successfully, it is important to ensure that these requirements are not over specified. Setting requirements for 98% reliability or 99% probability of surviving a 48 hour mission is likely to drive up costs significantly and it may be that a lower figure will have little real impact on the operational tempo and could be much more achievable and affordable.

4. It is important to recognise the difference between a requirement and a target or goal, terms which have very different meanings yet are often used in specifications without apparent recognition of the consequences. A requirement is something that is essential to successful operation of the item and should not be traded without full consideration of the consequences and agreement of all stakeholders. The supplier will need to provide evidence to substantiate that the requirement has been met, or where it can not be met, evidence in support of the request for a relaxation and why it is not now felt that the agreed specification cannot be met.

považováno za dobré mít, ale není to nezbytné a často je to zaměňováno za jiný záměr nebo cíl, pokud náklady rostou a jsou činěny pokusy zachovat pořizování v původním odsouhlaseném profilu nákladů.

5. Úrovně pohotovosti, bezporuchovosti a udržovatelnosti a tudíž i spolehlivosti, které byly dosaženy položkou, jsou velmi závislé na podmínkách, za nichž je tato položka využívána, často je popisována jako její profil mise nebo profil užití, ale v dokumentech NATO je odkazována jako Profil prostředí životního cyklu (LCEP). Jako příklad slouží položka v antivibračních uloženích v klimatizované místnosti udržovaná při 25 °C bude mnohem pravděpodobněji provozovaná bez incidentu než identická položka uložená na dřevěné paletě pod plachtou v prašném prostředí, kde okolní teplota může kolísat od -5 do +45 °C. Ve zbytku tohoto dokumentu bude používán termín Profil prostředí životního cyklu (LCEP).

6. Proto pokud se specifikují požadavky pro jakoukoli charakteristiku spolehlivosti, je nezbytné definovat podmínky pro skladování, přepravu, instalaci a používání, jimž bude položka vystavena. Je také nezbytné počítat s předpokládanými zásadami pro údržbu, a s oblastí, ve které bude tato údržba probíhat a s úrovněmi dovedností osob, které ji budou provádět. Zásah údržby, který je relativně jednoduchý v zařízení pro tento účel vybudovaném, se může stát extrémně obtížným za provozních podmínek.

7. Je také zapotřebí brát v úvahu dopad lidského faktoru a položky mají být navrhovány tak, aby minimalizovaly příležitosti k lidským chybám, které mají dopad na provedení spolehlivosti. Všude, kde je to možné, mají být úlohy automatizovány, aby se eliminovala rizika lidské chyby a tam, kde je požadován vstup uživatele, má být zajištěno, že pokud se vyskytnou chyby, nemají mít významný

A target or goal is something that is considered nice to have but not essential and often traded out when costs are rising and attempts are being made to keep the procurement within the original agreed cost profile.

5. The levels of availability, reliability, maintainability and hence dependability that are achieved by an item are very dependent on the conditions under which that item is utilised, often described as its Mission or Usage profile, but referred to in NATO documents as the Life Cycle Environment Profile (LCEP). As an example, item on anti-vibration mounts in an air-conditioned room maintained at 25 Celsius is much more likely to operate without incident than an identical one mounted on a wooden pallet under canvas in a dusty environment where the ambient temperature can fluctuate from -5 to +45 Celsius. For the remainder of this document the NATO term of Life Cycle Environment Profile (LCEP) will be used.

6. Therefore when specifying requirements for any of the dependability characteristics, it is necessary to define the conditions of storage, transportation, installation and use that will be encountered by that item. It may also be necessary to take account of the anticipated maintenance policy, the area in which that maintenance will be undertaken and the skill levels of the persons undertaking it. A maintenance action that is relatively simple in a purpose-built facility can become extremely difficult under operational conditions.

7. The human impact also needs to be considered and items should be designed to minimise the chances of human errors impacting on dependability performance. Wherever possible tasks that can be automated should be in order to eliminate the risk of human error and where the user is required to provide input care should be taken to ensure that if mistakes do occur they do not have a significant

vliv na provedení úkolu. Se vzrůstající složitostí položek mají být činnosti, které je potřeba provést v případě poruchy v provádění požadované funkce, jasně identifikované, aby se zajistilo, že uživatel nebude problém zhoršovat.

8. Všechny položky budou vykazovat určitou úroveň spolehlivosti, ale je pravděpodobné, že ty, které jsou vyráběny organizacemi, které aktivně neřídí spolehlivost, nedosáhnou úrovní, které jsou požadovány armádou. Pro zabezpečení spolehlivosti položky je nezbytné, aby se činnosti bezporuchovosti a udržovatelnosti plánovaly a prováděly tak, že návrh položky je pozitivně ovlivňován a že je toto v jakékoli etapě procesu návrhu a výroby verifikováno. Je zapotřebí věnovat včasnou pozornost plánům spolehlivosti a rozvržení příslušných zdrojů, aby se dosáhlo chtěných požadavků. Včasné investování do návrhu a realizace spolehlivosti pomocí programu spolehlivosti, jak je podrobně uvedeno v IEC 60300-1, se vždy samo vrátí ve formě provozních nákladů na položku, ve způsobu, jak vojenský personál důvěřuje položce, kterou používá a závisí na ní, v její schopnosti úspěšně projít plněním úkolu a tedy v její celkové pohotovosti vůči pracovním příkazům.

1.2 Účel

1. Účelem tohoto dokumentu je poskytnout instrukce k vytváření požadavků na spolehlivost. Vysvětluje, jaké potřeby mají být uvažovány pro spolehlivostní část specifikace pro akvizici a proč je důležitá.

2. Funkční analýza a proces klasifikace poruch jsou popsány v přiřazeném ADMP (ADPM-03). Těchto procesů je rozhodně zapotřebí ke stanovení požadavků na spolehlivost během provozního života. ADMP-03 doplňuje jak ADMP-01, tak ADMP02.

effect on mission performance. With the increasing complexity of items action that needs to be taken in the event of a failure to perform the required function should be clearly identified to ensure the user does not exacerbate the problem.

8. All items will exhibit some level of dependability but it is likely that those produced by organisations that do not actively manage dependability will not achieve the levels that are required by the military. To ensure the dependability of an item, it is essential that reliability and maintainability activities are planned and undertaken such that the item design is positively influenced and that this is verified at every stage of the design and production process. Early attention to dependability plans and allocation of appropriate resources is needed to achieve the desired requirements. An upfront investment in dependability design and construction through a dependability programme as detailed in IEC 60300-1 will always repay itself in terms of the operating costs for the item, in the way it is trusted by military personnel who use and depend upon it, its ability to successfully undertake a mission and thus its overall availability to operational command.

1.2 Purpose

1. The purpose of this document is to provide guidance on developing dependability requirements. It will explain what needs to be considered for the dependability section of the acquisition specification and why it is important.

2. The functional analysis and the failure classification process are described in a dedicated ADMP (ADMP-03). Indeed, those processes are needed to establish dependability requirements as well as to assess dependability during in-service life. ADMP-03 supports both ADMP-01 and ADMP-02.

3. Budou určeny běžné koncepce a faktory související se všemi požadavky na spolehlivost a poté se budou brát v úvahu jednotlivé charakteristiky, které jsou uvedeny níže, postupně se bude zvažovat jejich využitelnost v každé etapě životního cyklu položky, jak je definováno v Systému postupného plánování vyzbrojování v NATO (PAPS):

a. Pohotovost
b. Bezporuchovost
c. Udržovatelnost
d. Testovatelnost
e. Údržba
f. Bezpečnost
g. Software

4. Není zamýšleno, že tento dokument bude poskytovat vzor, ze kterého mohou být jednoduše vybrány všechny nové požadavky, ani že mohou dát po krocích návod, jak pokrýt všechny eventuality, ale bude brát v úvahu koncepce, problémy a faktory, které ovlivní, jak jsou nastaveny požadavky, dá příklady různých druhů požadavků a vysvětlí výhody a úskalí každého z nich.

1.3 Použití

1. Informace obsažené v tomto standardu se vztahují na všechny položky, kdykoli existuje potřeba vytvořit a nastavit požadavky v jakékoli etapě jejich životního cyklu, ať už jsou to nové požadavky, přírůstková aktualizace, aktualizace během střední doby života, přepracování návrhu z důvodu zastarávání nebo části šroubovicového akvizičního plánu.

2. V průběhu jakékoli změny položky, hardwarové, softwarové nebo ve způsobu, jak je nasazena a užívána, je povinné zajistit, že atributy spolehlivosti jsou určeny nebo znovu přehodnoceny. To má být využito všemi členy projektů a provozních organizací, včetně různých agentur NATO, které jsou odpovědné za spolehlivost.

3. It will address the common concepts and factors relating to all dependability requirements and then look at the individual characteristics detailed below in turn considering their applicability at each stage of the item life cycle as defined in the NATO Phased Armament Programming System (PAPS):

a. Availability
b. Reliability
c. Maintainability
d. Testability
e. Maintenance
f. Safety
g. Software

4. It is not intended that this document will provide a template from which all new requirements can simply be selected, nor can it give a step by step guide to cover every eventuality, but it will consider the concepts, issues and factors that influence how a requirement is set, give examples of the differing types of requirement and explain the benefits and pitfalls of each.

1.3 Applicability

1. The information in this document applies to all items whenever there is a need to develop and set a requirement at whatever stage it is in its life cycle, be it a brand new requirement, an incremental update, a mid life update, a re-design due to obsolescence or part of a spiral acquisition plan.

2. During any change to the item, be that hardware, software or in the way its is deployed and used, it is imperative to ensure that the dependability attributes are addressed or re-addressed. It should be used by all members of projects and in service organisations including the various NATO agencies who are responsible for dependability.

1.4 Související dokumenty

Viz kapitolu Související dokumenty.

1.4 Related documents

See Chapter Související dokumenty.

2 KONCEPCE A FAKTORY

2.1 Profil prostředí životního cyklu

1. Charakteristiky spolehlivosti, kterých je dosahováno kteroukoli položkou, velmi závisí na tom, jakým způsobem se používají. To je definováno v Profilu prostředí životního cyklu, který znamená buď uvažovaný scénář založený na aktuální nebo předchozí zkušenosti, nebo předpovězený model založený na předpovědi budoucích požadavků na užití. Ať je profil vytvořen jakkoli, je důležité vzít v úvahu následující:

a. Požadovaný časový interval – jak dlouho je pro položku požadováno být v plně provozním stavu, jak dlouho je požadováno být v nějaké formě nízkého provozního nebo pohotovostního stavu, jak dlouho se očekává, že bude položka během zvolené doby používání vypnutá včetně libovolné přepravy, která může být vyžádána.

b. Počet opakování – může se stát, že LCEP pokrývá pouze jediné nasazení, což může být 2 hodinový let ve vzdušném prostředí, 7 hodinová trasa v pozemním prostředí, 30 denní nalodění v námořním prostředí nebo 8 hodinový pracovní den ve výcvikovém/kancelářském prostředí. U jiných, než zařízení na jedno použití (řízené střely, munice atd.), je velmi zřídkavé, aby u položky bylo požadováno dosažení pouze jednoho nasazení, je tedy nezbytné uvažovat, kolika opakování při dané délce trvání je zapotřebí, jaká je přípustná doba nepoužitelného stavu mezi nasazeními a jaká údržba nebo činnosti opravy jsou přípustné, aby se položka navrátila zpět do stavu připravenosti, včetně existujících bezpečnostních požadavků.

2 CONCEPTS AND FACTORS

2.1 Life Cycle Environment Profile

1. The dependability characteristics that are achieved by any item are very dependent on how it is used. This is defined in a Life Cycle Environment Profile (LCEP) that is either an envisaged scenario based on current or previous experience, or a predicted pattern based on what the future usage requirements are expected to be. However the profile is constructed, it is important to consider the following:

a. Period of time required – How long the item is required to be in a fully operational state, how long it is required to be in some sort of low operational or stand by state, how long it is expected to be switched off during the chosen period of interest including any transportation that may be required.

b. Number of repetitions – It may be that the LCEP covers only a single deployment, be that a 2 hour flight in the air environment, a 7 hour journey in the land environment, a 30 day embarkation in the maritime environment or an 8 hour working day in a training / office based environment. Other than for single use devices (missiles, ammunition etc) it is very rare that an item is only required to achieve a single deployment, thus it is necessary to consider how many times it needs to be repeated over a given duration, what the allowable down time is between deployments and what maintenance and or repair activity is allowable to bring the item back to a ready state, including any extant safety requirements.

c. Zatěžování – má se vzít v úvahu, jak moc a jak často bude položka zatěžována. Zatímco část specifikace týkající se provedení je obvykle dobře zpracovaná, pokud jde o maximální zatížení, často se přehlíží skutečnost, jak často se bude toto zatížení vyskytovat a jaká bude mezi jednotlivými výskyty „perioda zotavení“.

d. Nouzové režimy – mnoho současných položek má v sobě zabudováno zálohování, takže porucha jednotlivé trasy nebo funkce nezabrání položce v pokračujícím poskytování schopnosti, která je od ní požadována. To se nesmí plést s nouzovými režimy, které jsou často zabudovávány, aby poskytly uživateli poslední východisko při střetu s katastrofickou poruchou. Možnost manuálně provádět činnost, když automatický systém selže, je něco, co by mělo být použito pouze při ojedinělých příležitostech a zatímco může pro položku klidně existovat požadavek mít manuální nouzový režim, nemělo by být bráno v úvahu, když je vytvářen LCEP.

e. Údržba – Všechny položky bude někdy potřebné nevyhnutelně demontovat pro účely činností údržby a toto má být bráno v úvahu tak časně, jak je to jen v procesu specifikace možné, aby se zajistilo, že požadovaná schopnost může být poskytována položkou, která je specifikována. Vzhledem k požadované údržbě, je důležité vzít v úvahu, kde se bude údržba provádět, podmínky, za kterých se bude provádět, jaké informace, nástroje a zkušební zařízení budou k jejímu provádění zapotřebí, jaký výcvik bude požadován a praktičnost provádění takové údržby, zejména požaduje-li se její provádění za provozních podmínek. Mají být také brány ohledy na potřebu údržby během nebo po dlouhodobém skladování nebo přepravě. Odstavec

c. Loading - Consideration should be given to how heavily the item will be loaded and how often. Whilst the performance part of the specification is usually well covered in terms of maximum loading, what is often overlooked is how often that load will occur and what ‘recovery periods’ there will be between each occurrence.

d. Fall Back Modes – Many items these days have redundancy built in, such that failure of a single path or function does not prevent the item from continuing to provide the capability that is required of it. This must not be confused with fallback modes which are often built in to provide the user with a last resort should a catastrophic failure be encountered. The ability to manually carry out an activity when the automatic system has failed is something that should only be used on rare occasions and whilst there may well be a requirement for the item to have a manual fall back mode it should not be considered when the LCEP is being generated.

e. Maintenance – All items will inevitably need to be taken down at some point for maintenance activity and this should be considered as early as possible in the specification process to ensure that the required capability can be provided by the item that is being specified. When considering the maintenance that will be required it is important to take into account where the maintenance is to be performed, the conditions in which maintenance may have to be performed, what information, tools and test equipment will need to be provided, what training will be required and the practicality of undertaking that maintenance particularly if it is required to be performed under operational conditions. Consideration should also be given to the need for maintenance during or after

3.5 tohoto standardu poskytuje detailněji informace o specifikování údržby.

f. Očekávaná velikost strojového parku – když se provádí posouzení velikosti strojového parku, je důležité zvážit bezporuchovost a pohotovost každé položky. Předpoklad, že jakákoli položka bude mít 100% pohotovost, povede ke špatnému předpokladu o celkovém počtu požadovaném pro poskytnutí schopnosti, a povede to k časovým intervalům, kdy tato schopnost nebude v pohotovosti. Jak bylo diskutováno v předchozím odstavci, je-li schopnost skutečně požadována 24 hodin denně, 7 dní v týdnu, 52 týdnů v roce, musí kalkulace o velikosti strojového parku počítat i s majetkem, který není v pohotovosti.

2.2 Rozhraní

1. Jestliže se nastavují požadavky na spolehlivost, je důležité mít na paměti, že uvažovaná položka bude pravděpodobně tvořit část většího systému nebo bude odkázána na nějakou formu vnějšího stimulu, aby mohla být provedena podle své specifikace. Je pravděpodobné, že dodání takových vnějších stimulů nebude tvořit část smlouvy na položku a že bude předpoklad, aby bylo k dispozici, bude-li požadováno. Z těchto důvodů je důležité zajistit, aby rozhraní uvažované položky bylo jasně definováno a veškeré vnější stimuly, u nichž je vyžadována přítomnost, jsou identifikovány v dokumentaci, zejména je-li položka částí platby vzhledem ke smlouvě na provedení. Tyto vnější stimuly mohou nabývat mnoho forem a mohou zahrnovat vnější napájení, data od ostatních položek, pohotovost externě řízených a poskytovaných položek nebo položek existujících v majetku resortu, s nimiž je požadováno, aby uvažovaná položka spolupracovala. Může to být složitá oblast jak

long term storage or transportation. Section 3.5 of this document gives more details on maintenance specification.

f. Anticipated Fleet Size – When conducting fleet size assessments it is important to consider the reliability and availability of each item. Assuming that any item will be 100% available will lead to wrong assumptions about the total number required to provide the capability and will lead to periods of time when the capability is not available. As discussed in the previous paragraph if a capability is truly required 24 hours a day, 7 days a week, 52 weeks a year the fleet sizing calculations must take account of non availability of assets.

2.2 Boundary

1. When setting dependability requirements it is important to remember that it is likely the item being considered will form part of a bigger system or be reliant upon some form of external stimulus in order for it to perform according to its specification. It is likely that the supply of these external stimuli will not form part of the contract for the item and that they will be assumed to be present when required. For this reason it is important to ensure that the boundaries of the item that is being considered are clearly defined and all external stimuli that are required to be present are identified in the documentation, particularly if the item is part of a payment in respect of performance contract. These external stimuli can take many forms and may include external power, data from other items, the availability of externally managed and provided items or even existing items within the inventory which the item of interest will be required to work with. This can be a complex area to both understand and describe in such

pro porozumění, tak pro popis takovéhoto chování způsobem, že nebudou existovat nejednoznačnosti.

a manner that no ambiguity exists.

2. Aby fungovaly, vyžaduje většina položek nějakou formu vnější energie, jejíž dodání není často zahrnuto ve specifikaci položky. V těchto případech budeme předpokládat, že požadovaná energie na specifikovaných úrovních bude vždy v pohotovosti a nebude se započítávat pro účely všech činností spojených se spolehlivostí. Pokud by se vyskytla ztráta ukazatele, u kterého se ukáže, že jej lze přímo přisuzovat vnější dodávce energie, ať již nad nebo pod hodnotami danými specifikací, pak v nejjednodušší situaci ony události nebudou přisuzovány uvažované položce a jakákoli platba spojená s pohotovostí by nebyla odmítnuta. Do smlouvy se však běžně zahrnují požadavky, zajišťující ochranu položky proti poškození v případě, kdy je dodávána energie pod nebo nad specifikovanou hodnotou nebo dokonce požadavek, aby položka měla zabudovaný zdroj energie pro zajištění pokračujícího chodu po jistou dobu, nebo aby byla řádně odstavena z provozu v případě ztráty vnější dodávky energie. V těchto případech může být ztráta ukazatele přisuzována položce a může být zapotřebí snížení nebo odmítnutí jakékoli související platby.

2. In order to function, most items require some form of external energy, the supply of which is often not included in its specification. In these cases it will be assumed that the required energy, within specified levels, will always be available and for the purposes of all dependability activity they will be excluded. Should any loss of performance occur which it can be shown was directly attributable to the external energy supply, be it over or under specification, then in the simplest situation those events will not be attributed to the item under consideration and any payment associated with its availability would not be withheld. However, it is common for the contract to include the requirement for the item to be protected from damage in the event of over or under specification energy being supplied or even the requirement for the item to have a built in energy source to ensure its continued performance for a period of time or orderly shutdown in the event of loss of the external energy supply. In these cases the loss of any performance may be attributable to the item and any associated payment may need to be reduced or withheld.

3. Jak dokazuje příklad uvedený výše, zajištění, že rozhraní jsou jasně identifikována na základě dílčích komponent a provedení, se může stát velmi složitou úlohou, ale nejasná definice může vést k dlouhým a protahovaným diskusím při pokusu o dohodu, zda událost může být událost přisuzovaná nebo ne, zejména tam, kde je zahrnuta platba.

3. As the example above demonstrates, ensuring that the boundaries are clearly identified in terms of sub-components and performance can be become a very complex task but the lack of a clear definition can lead to long and protracted discussions when trying to agree if an event is attributable or not, particularly where a payment is involved.

2.3 Ohledy na prostředí

2.3 Environment Consideration

1. Charakteristiky spolehlivosti, kterých dosahuje položka, jsou velmi závislé na provozním prostředí, v němž se položka používá. Faktory prostředí jsou často specifikovány jako minimální a maxi-

1. The dependability characteristics that are achieved by an item are very dependent on the operational environment in which it is used. Environmental factors are often specified as minimum

mální hodnoty potřebné pro provoz s rozšířenými limity pro přežití. Jakkoli je to specifikováno, je třeba uvážit následující:

a. Prostředí – je nezbytné definovat podmínky, za kterých se předpokládá, že bude položka provozována. Teplota je normálně specifikována jako rozsah, ale často nejsou dány žádné údaje, jak dlouho se očekává, že bude položka provozována na každém konci tohoto spektra, nebo co se očekává pod pojmem normální podmínky. Měla by se rovněž zvážit specifikace extrémů, při nichž se očekává přežití položky v neprovozních podmínkách. Další faktory, např. vlhkost, slanost a znečištění prachem, mohou mít také významný vliv na charakteristiky spolehlivosti položky, a pokud se mají vyskytnout, mají být specifikovány.

b. Terén – je také důležité brát v úvahu terén, v němž bude pravděpodobně položka provozována, protože to na ni může klást významnou zátěž a namáhání. V pozemním prostředí to bude pravděpodobně vysvětlení typu povrchu, s nímž bude položka v kontaktu, rychlost, při které se toho má dosáhnout a doba, kterou bude položka v kontaktu s jednotlivými povrchy. V námořním prostředí je pravděpodobné, že to bude pokrývat specifikace stavů moře, zatímco ve vzdušném prostředí to bude pravděpodobně pokryto nadmořskou výškou nad hladinou moře během letu.

c. Přístup k údržbě – předpokládá-li se, že bude požadována jakákoli forma údržby během provozu, pak je nezbytné zahrnout požadavky, které jasně specifikují, o jaké údržbě se uvažuje, aby bylo zajištěno poskytování přístupu, který umožní provádění údržby a poskytování jakýchkoli nezbytných nástrojů.

and maximum values for operation with extended limits for survival. However it is specified, it is important to consider the following:

a. Environment – It is necessary to define the conditions the item is expected to operate in. Temperature is normally specified as a range but often no indication is given on how long the item is expected to operate at each end of that spectrum, or what the normal condition is anticipated to be. Consideration should also be given to specifying the extremes at which an item will be expected to survive in a non operational condition. Other factors, e.g. humidity, salinity, and dust contamination can also have significant effect on the dependability characteristics of the item and should be specified if they are to be encountered.

b. Terrain – It is also important to consider the terrain over which the item is likely to operate as this can place significant stress and strain on it. In the land environment this is likely to be an explanation the type of surface that will be encountered, the speed at which it should be accomplished and the amount of time it will spend on any particular surface. In the maritime environment it is likely that this will be covered by the specification of sea states whilst in the air environment it is likely this will be covered by height above sea level whilst flying.

c. Access For Maintenance – If it is anticipated that any form of maintenance will be required during operation, then it is necessary to include a requirement that clearly articulates what maintenance is envisaged, to ensure the provision of access to allow that maintenance to be carried out and the provision of any necessary tools.

2.4 Úspěch a porucha

1. Když se specifikuje bezporuchovost, je běžnou a dobrou praktikou zahrnout pravděpodobnost úspěchu úkolu nebo pravděpodobnost dosažení dané časové periody bez výskytu selhání úkolu. To předpokládá, že existuje soulad v tom, co tvoří úspěch a takto i kdy se porucha projeví, tj. kdy položka už nadále nepracuje způsobem, který je pro uživatele pokládán za přijatelný. Zatímco většina garantů položky, kteří formulují požadavky, bude snadno schopna definovat úspěch, je mnohem těžší definovat poruchu. Nastavení jasných a odsouhlasených definic poruchy je důležitý krok, který je často během specifikování požadavků na spolehlivost přehlížen.

2. V časných etapách, kdy je výsledný návrh pochybný, budou definice poruch vymezeny na funkční úrovni. Pro jejich uzpůsobení bude nezbytné identifikovat funkce, které jsou nepostradatelné, aby položka vykonávala požadovaný úkol, a které budou normálně zaznamenávány do seznamu základních funkcí úkolu, jimiž jsou jízda vozidla, let letounu, komunikování, ochrana atd. Následný krok by měl vzít v úvahu, jaká úroveň degradace dá vzniknout poruše každé této funkce a tudíž schopnost položky úspěšně dokončit úkol. V závislosti na typu a složitosti položky se může počet hlavních funkcí lišit a může být tedy nezbytné vzít v úvahu, jaké definice funkčních poruch budou vytvořeny.

3. Jak postupuje návrh a ze způsobu definice architektury, která bude určovat každou funkci, by se měly odvodit definice poruch tak, aby mohla být příčina každé funkční poruchy připsána jednotlivým komponentám hardwaru nebo softwaru v rámci takové architektury. Další informace vztahující se k vytváření definic poruch, funkčnímu

2.4 Success and Failure

1. When specifying reliability it is common and good practice, to include requirements such as probability of mission success or probability of achieving a given period of time without encountering a mission failure. This presupposes that there is an understanding of what constitutes success and thus when failure has occurred i.e. when an item is no longer performing in a manner that is considered acceptable to the user. Whilst most item sponsors who are formulating the requirements will readily be able to define success it is much more difficult to define failure. Setting clear and agreed definitions of failure is an important step that is often overlooked during the specification of dependability requirements.

2. In the early stages, as the final design is unlikely to be known, failure definitions will be defined at a functional level. To enable this, it will be necessary to identify the functions that are essential for the item to perform its required mission, which will normally be recorded in a mission essential function list, typical examples being Move, Fight, Communicate, Protect etc. The next step would be to consider what level of degradation constitutes failure of each of those functions and thus the items ability to successfully complete its mission. Depending on the type and complexity of the item, the number of essential functions can differ, thus it may be necessary to consider which functions failure definitions will be developed for.

3. As the design progresses and the architecture that will provide each function is defined, the failure definitions should evolve such that the cause of each functional failure can be attributed to individual hardware or software components within the architecture. Further information relating to the development of failure definitions, the

rozpadu položky a klasifikaci spolehlivosti vztažené k událostem lze najít v ADMP-03.

4. Zatímco je snadné porozumět koncepci definování poruchy, realita jejího odvozování a odsouhlasení je velmi odlišná, obzvlášť tam, kde není porucha zřejmá. Ať jsou definice jakékoli, musí být odsouhlaseny všemi, kterých se to týká a musí být řízeny v průběhu všech diskusí, jež jsou s uvažovanou položkou spojeny. Následující příklady se pokusí to ukázat:

a. Pro vozidlo je dán požadavek, že má být schopno podniknout 200 km cestu bez přerušení a má být schopno dosáhnout rychlosti 150 km/h v čase, kdy se nachází na jakékoli hlavní silnici. Jestliže se vozidlo stane z jakéhokoli důvodu nepohyblivé, pak se důvodně předpokládá, že mělo poruchu; ale pokud, díky špatné funkci uvnitř vozidla, je schopné dosáhnout jen rychlosti 145 km/h, mělo potom vozidlo poruchu? Jestli ne, pak při jaké rychlosti je vozidlo považováno za nevhodné ke svému účelu a mělo poruchu? Podobně, jestliže vozidlo má píchlou pneumatiku, která může být opravena do 10 minut, bylo by to považováno za poruchu?

b. Od systému obsahujícího informační technologie (IT) je požadováno, aby poskytoval kancelářské služby pro 1000 pracovníků, kteří jsou umístěni přes 5 podlaží v jedné budově. Systém je poskytován na základě smlouvy o pohotovosti s měsíčním placením, v závislosti na počtu poruch, které se projeví u uživatelů. Jestliže jeden uživatel na jednom patře nemá přístup do sítě, znamená to poruchu systému IT, nebo znamená to poruchu, když skupina 10 nebo více uživatelů nemá přístup, nebo se to za výskyt poruchy nepovažuje, dokud celé patro nemá přístup? Zda jde o poruchu, by šlo zvažovat na základě

functional breakdown of an item, and the classification of dependability related events can be found in ADMP-03.

4. Whilst the concept of defining failure is easy to understand the reality of deriving and agreeing them is very different, particularly where failure is not clear cut. Whatever the definitions are, they have to be agreed by all concerned and adhered to throughout all discussions associated with the item concerned. The following examples will attempt to show this:

a. A vehicle has a requirement to be able to undertake a 200 km journey, without interruption, and be capable of achieving 150Km/hr for the time it is on any major road. If the vehicle becomes immobilised for any reason then it is reasonable to assume that it has failed; but if, due to a malfunction within the vehicle, it is only capable of achieving 145Km/hr then has the vehicle failed? If not then at what speed is it considered that the vehicle is not fit for purpose and has failed? Similarly if the vehicle suffers from a flat tyre which can be repaired within 10 minutes would this be considered a failure?

b. An Information Technology (IT) system is required to provide office services for 1000 members of staff located across 5 floors in one building. The system is being provided under an availability contract with monthly payment depending on the number of failures the users experience. If a single user on one floor cannot access the network does this constitute failure of the IT system, or does a group of 10 or more users not having access constitute failure, or is failure not considered to have occurred until a whole floor does not have access? The failure could also be considered in terms of how long it

toho, jak dlouho trvá uživatelům obnovit soubor ze sítě, přihlásit se do systému, spustit aplikaci, dosáhnout přístupu na internet nebo kombinace těchto událostí.

takes users to recover a file from the network, to log on to the system, to launch an application, to access the internet or any combination of these events.

2.5 Verifikace a validace (dosažení) požadavků

1. Jak je stanoveno v úvodu, je důležité zajistit, aby pro všechny požadavky, které jsou pro položku nastavovány, bylo možno prokázat, že byly dosaženy. Stejným způsobem jako u ostatních požadavků na provedení může být spolehlivost dokládána zkouškami, ale na rozdíl od mnoha požadavků na provedení je jedna zkouška často nedostatečná k prokázání, že bylo dosaženo spolehlivosti, a jejich statistická podstata vyžaduje pro poskytnutí požadované konfidenční úrovně uskutečnit větší množství zkoušek. Toho se dosahuje pomocí poskytnutí objektivního důkazu, který podpoří tvrzení, že specifikované požadavky byly splněny (ověření)[4] nebo který podpoří tvrzení, že specifikované zamýšlené použití bylo splněno (validace)[5].

2.5 Requirements Verification and Validation

1. As stated in the introduction it is important to ensure that all requirements which are set for the item can be shown to have been achieved. In the same way as for other performance requirements, dependability can be proven by test, but unlike many performance requirements a single test is often not enough to show that dependability has been achieved and their statistical nature requires many tests to be carried out to deliver the required level of confidence. This is generated through the provision of objective evidence in support of the claim that specified requirements have been fulfilled (verification)[4] or in support of the claim that a specific intended use has been fulfilled (validation)[5].

2. Počet nebo délka požadovaných zkoušek budou záviset na statistické konfidenční úrovni, která je uvažována jako přijatelná, čím je požadována vyšší míra důvěra v ukazatele, tím více testů nebo delší čas pro testování bude zapotřebí, musí být tedy vytvořen robustní plán testů a musí být zahrnut do programu spolehlivosti a hlavního vývojovému programu pro položku. Má se připustit, že plán testů spolehlivosti bude pravděpodobně vyžadovat spoustu kalendářního času a může se stát hlavním faktorem ve smyslu celkové doby potřebné pro vývoj. Má se tudíž využít

2. The number of, or length of tests required will depend on the level of statistical confidence that is considered acceptable, the higher the confidence required the more tests or the longer the test time that will be required, thus a robust test plan must be developed and included within the dependability programme and the main development programme for the item. It should be recognised that the dependability test plan is likely to require a lot of calendar time and can be a major driver in terms of overall development time. Thus every opportunity to use other development

[4] Definice ověření je vzata z IEC 60050-192 a odvozena z ISO 9000.
The definition of verification is taken from IEC 60050-192 derived from ISO 9000.

[5] Definice validace je vzata z IEC 60050-192 a odvozena z ISO 9000.
The definition of validation is taken from IEC 60050-192 derived from ISO 9000.

každá příležitost vykonat další vývojové zkoušky, aby se získaly informace o úlohách spolehlivosti.

tests to inform the dependability tasks should be taken.

3. Testování k prokázání, že bylo dosaženo požadavků na spolehlivost, vyžaduje, aby standardní výrobní položka byla provozována během časového období, během kterého je každá porucha zaznamenána a je posouzen její význam. Dosažená úroveň bezporuchovosti je funkcí úplné doby zkoušky kombinované s počtem závažných poruch, které se vyskytly. To ukazují následující příklady:

3. Testing to prove that a reliability requirement has been achieved requires the production standard item to be run for a period of time, during which each failure is recorded and assessed for relevance. The achieved level of reliability is a function of the trial time completed combined with the number of relevant failures that occurred. The following examples demonstrate this:

a. Položka byla provozována 1000 hodin, během této doby se vyskytlo 10 závažných poruch. Statistická analýza založená na modelu testu dobré shody (jinak Pearsonův chí-kvadrát test)*) ukazuje, že to signalizuje, že bylo dosaženo střední doby mezi poruchami (MTBF) 94 hodin na 50% konfidenční úrovni, MTBF 80 hodin bylo dosaženo na 70% konfidenční úrovni a MPBF 65 hodin na 90% konfidenční úrovni. Viz IEC 61124[6] pro veškeré podrobnosti o testu dobré shody a dalších statistických modelech, vhodných pro testování spolehlivosti.

   *) Národní poznámka: Pearsonův chí-kvadrát test (test dobré shody) je metoda matematické statistiky, která umožňuje ověřit, zda má náhodná veličina určité předem dané rozdělení pravděpodobnosti. Test je založen na tom, že náhodnou veličinu s polynomickým rozdělením lze transformovat na veličinu mající přibližně rozdělení chí kvadrát.

a. An item has been operated for 1000 hours during which time 10 relevant failures have occurred. Statistical analysis based on the chi-squared model shows that this indicates a Mean Time Between Failure (MTBF) of 94 hours has been achieved to a 50% level of confidence, an MTBF of 80 hours has been achieved to a 70% level of confidence and an MTBF of 65 hours to a 90% level of confidence. See IEC 61124 for full details of chi-squared and other statistical models appropriate to reliability testing.

b. Byla přijata smlouva za účelem nákupu 50 položek na jedno použití, s požadavkem, že každá položka má dosáhnout 99% úroveň bezporuchovosti na 80% konfidenční úrovni. Aby se to prokázalo, je nezbytné provést 161 testů bez toho, aby se vyskytla

b. A contract has been let for the purchase of 50 single use items with a requirement that each item should achieve a 99% level of reliability to an 80% level of confidence. In order to prove this it is necessary to complete 161 tests without a relevant failure

[6] Norma ČSN IEC 61124:1998 byla zrušena 1.3.2007, existuje norma IEC 61124:2012, nikoli však jako harmonizovaná ČSN.

závažná porucha. Jinými slovy, aby se prokázala bezporuchovost, bylo by zapotřebí objednat více než trojnásobné množství položek. Tento požadavek je nepřijatelný a bylo by nezbytné buď změnit požadavek na něco, co se může brát v úvahu jako přijatelné díky snížení úrovně bezporuchovosti její přiřazené konfidenční úrovni, nebo odsouhlasením jiných metod prokazování, že návrh je během vývoje a výroby položky robustní a bezporuchový.

4. Za důkaz můžeme pokládat mnoho forem, od výsledku testů, jejichž podrobnosti jsou výše, tvořících pouze jednu část celkového důkazu, požadovaného k prokázání, že bylo dosaženo požadavků. Je nejpravděpodobnější, že program spolehlivosti bude vyžadovat, aby důkazy byly prezentovány ve formě zaručených fakt vytvářených v průběhu života položky a postupně dodávaných záruk, že bude položka spolehlivá. Je důležité poznat, že fakta nejsou jen studnicí pro výsledky, ale jsou nositelem, připouštějícím tvorbu odůvodněných a auditovatelných tvrzení a argumentů o spolehlivosti položky.

5. Povaha charakteristik spolehlivosti je taková, že mnohé z nich jsou často souborem kvantitativních hodnot, kde zkouška požadavku je zajišťována hodnotami měřenými během testů, tak jako ty, nastíněné výše. Tento typ požadavku sebou nezbytně nese strukturovaný matematický proces, pomocí něhož jsou hodnoty počítány a jsou vynášena tvrzení, založená na jejich citaci. Ne všechny požadavky musí být kvantitativní a tam, kde nemohou být měřeny, budou nastaveny jako kvalitativní. Takové druhy požadavků závisí mnohem více na utvořeném argumentu, že poskytnutý důkaz splňuje požadavek, než na výsledcích testu samotného a mohou být často lépe vyjádřeny použitím formalizované metody, jako je

occurring. Put another way, in excess of 3 times the number of items that are being purchased would need to be used to prove the reliability. This requirement is unacceptable and it would be necessary to either change the requirement to something that could be considered acceptable, by reducing the level of reliability its associated confidence, or by agreeing other methods of proving that the design is robust and reliable during the development and manufacture of the item.

4. Evidence can take many forms with the test results detailed above forming only one part of the overall evidence required to show that the requirements have been met. It is most likely that the dependability programme will require the evidence to be presented in the form of an assurance case which builds over the life of the item, progressively delivering assurance that the item will be dependable. It is important to recognise that the case is not only a repository for results but is a vehicle to allow reasoned and auditable claims and arguments to be made about the dependability of the item.

5. The nature of dependability characteristics are such that many of them are often set as quantitative values where the proof of the requirement is provided by values measured during tests such as those outlined above. This type of requirement necessarily brings with it a structured mathematical process by which values are calculated and claims made based on them. Not all requirements have to be quantitative and where they can not be measured will be set as qualitative. These types of requirements depend much more on the argument made that the evidence provided meets the requirement than the results of the tests themselves and can often be better expressed using formalised methods such as Goal Structuring Notation (GSN).

Goal Structuring Notation (GSN – strukturovaný zápis cílů).

2.6 Strategie pořizování

1. Je důležité zajistit, aby jakékoli požadavky na spolehlivost byly nastaveny takovým způsobem, že odráží strategii pořizování.

2. Očekává-li se od položky, že bude zabezpečována základními metodami v rámci vojenských metod, pak bude nezbytné vzít v úvahu nastavení požadavků, které zajistí, že je organizacím zabezpečujícím skladování poskytnut dostatek náhradních dílů a že výcvik osob provádějících údržbu zahrnuje plné pokrytí diagnostiky poruch a oprav, včetně seznámení s jakýmikoli speciálními druhy nástrojů nebo testovacího zařízení.

3. Je-li položka zabezpečována smluvním dodavatelem pomocí smlouvy založené na ukazatelích, pak bude nezbytné zajistit, aby byly zahrnuty instrukce/požadavky související s časovou odezvou, klauzule spojené s penále a dohody o tom, co je a co není předmětem smlouvy. Má se připustit, že máme-li pouze celkový požadavek na pohotovost položky, nemusí být dostatečný, aby zajistil, že je položka v pohotovosti, když se to požaduje. Je-li vyžadováno, aby položka dosáhla 99% pohotovosti během roku (8760 hodin), pak může položka během roku nebýt v pohotovosti 87,6 hodin. Zatímco u položky mohou být přijatelné prostoje 1,5 hodiny týdně, prostoj 48 hodin v jakémkoli jednom čase (v roce) nemusí být přijatelný, přestože oba příklady by překročily požadavek na 99% pohotovost, pokud by šlo o jedinou dobu nepoužitelného stavu.

2.7 Technologická omezení

1. Je nezbytné zajistit, že jakékoli nastavené požadavky na spolehlivost, odpovídají technologii, o níž se předpokládá, že bude použita pro návrh. Nejvyspělejší

2.6 Procurement Strategy

1. It is important to ensure that any dependability requirements that are set reflect the procurement strategy.

2. If the item is expected to be supported using organic methods internal to the military, then it will be necessary to consider setting requirements that ensure enough spares are provided to the stores organisation and that maintainer training includes full coverage of failure diagnosis and repairs, including familiarisation with any special to type tools or test equipment.

3. If the item is to be supported by the contractor using a performance based contract then it will be necessary to ensure that statements / requirements relating to response times, penalty clauses and agreements on what is and is not within the scope of the contract are included. It should be recognised that just having an overarching item availability requirement may not be enough to ensure that the item is available when it is required. If an item is required to achieve 99% availability over a year (8760 hours) then it can be unavailable for 87.6 hours during the year. Whilst it may be acceptable for the item to be non operational for 1.5 hours a week, having it non operational for 48 hours at any one time may not be, even though both examples would exceed the requirement of 99% availability over the year if they were the only downtime.

2.7 Technology Constraints

1. It is necessary to ensure that any dependability requirements that are set are consistent with the technology that it is anticipated will be used in the design.

technologie je často méně spolehlivá, než technologie, která byla po jistou dobu používána.

2. Jestliže je očekávání takové, že položka bude silně softwarová, potom nastavení požadavku pro střední dobu do opravy (MTTR) na 120 minut nemusí být vhodné, když převládající způsob poruchy je pravděpodobně zablokování softwaru, jehož odstranění vyžaduje 5 minut trvající restart systému.

3. Je-li u položky očekáváno, že bude mít speciální povlak, jehož vytvrdnutí po aplikaci trvá 240 minut, a jenž by bylo třeba opětovně aplikovat po každém odstranění upevnění za účelem údržby, pak nastavení MTTR na 20 minut by bylo nejpravděpodobněji nevhodné, ledaže by čas na vytvrdnutí byl specificky z měření času vyloučen.

4. Podobně, jestliže má technologie, u níž se očekává, že bude použita v položce, historii, která ukazuje, že MTBF je pouze 1000 hodin, a pak se položka zabuduje do návrhu, kde je zásadní, aby MTBF dosáhla 2500 hodin, je vysoce pravděpodobné, že to povede k poruše. Ve vojenské a bezpečnostní oblasti je třeba, aby požadavky na provedení položky, byly před ostatními, použitá technologie je často nová a nevyzkoušená. V těchto případech je nezbytné přezkoumat, jestli může technologie dosáhnout úrovní spolehlivosti, které jsou definovány a rozpoznat, že méně bezporuchová položka může být výhodnější, než vůbec žádná.

Cutting edge technology is often less dependable than technology that has been in use for a period of time.

2. If expectation is that the item will be software intensive, then setting a requirement for a Mean Time To Repair (MTTR) of 120 minutes may not be appropriate when the predominant failure mode is likely to be a software lock up which requires a 5 minute reboot to fix.

3. If an item is anticipated to have a special coating that takes 240 minutes to cure after application and which would need to be re-applied each time a fastening was removed for maintenance, then setting an MTTR of 20 minutes would most likely be inappropriate unless the cure time was specifically excluded from the time measurement.

4. Similarly, if the technology which it is anticipated will be used in the item has a history that shows it only achieves 1000 hours MTBF, then incorporating it into a design where it is vital it achieves 2500 hours MTBF is highly likely to lead to failure. In the military and security fields the performance requirements of the item need to be ahead of others, the technology that is being used is often new and unproven. In these cases it is necessary to review if the technology can achieve the levels of dependability being specified, recognising that a less reliable item may be more beneficial than no item at all.

2.8 Vnější vliv

1. Charakteristiky spolehlivosti položky pro zajištění obrany mohou být významně ovlivněny rozhodnutími a změnami v ostatních oblastech, z nichž některé jsou mimo vliv pracovníků pro pořizování. V minulosti byly výhody technologie velmi často ovlivněny potřebami obrany, ale v poslední době bylo tohle změněno a pokroky v technologii jsou nyní velmi stimulovány komerčním

2.8 External Influence

1. The dependability characteristics of a defence item can be significantly affected by decisions and changes in other areas, some of which are out with the control of the procurement staff. In the past, advances in technology were often influenced by the needs of defence but recently this has changed and technology advances are now very much driven by the commercial world.

světem. Aspekty životního prostředí mají také vliv, jaký materiál může být použit v konstrukci obranných položek a tohle může mít významný vliv na možné charakteristiky spolehlivosti.

Environmental concerns also have an effect on what materials can be used in the construction of defence items and this can have significant effect on the eventual dependability characteristics.

2. Současné změny v zásadách ochrany prostředí požadovaly, aby se zastavilo používání olova v položkách. Tak, jak bylo olovo používáno po mnoho let v konstrukci karet elektronických obvodů a bylo zaváděno do procesu pro potlačení dalších problémů, se kterými jsme se setkávali, poslední legislativní prostředky říkají, že jsou nyní požadovány jiné metody, aby bojovaly s těmito problémy a že vlastnosti elektroniky, které pozitivně přispívají ke spolehlivosti a byly dobře známé, nyní potřebují, aby byly zkoumány a posouzeny. V mezidobí je nezbytné, aby se zajistilo, že existují vhodné metody, kterými se výstupy bez olova řídí.

2. Recent changes in environmental policy have required that the use of lead in items is stopped. As lead has been used in the construction of electronic circuit cards for many years, and was introduced into the process to suppress other issues that had been encountered, the latest legislation means other methods are now required to combat these issues and that the properties of electronics that contribute positively to dependability and were well known, now need to be researched and reviewed. In the interim it is necessary to ensure that methods are in place to control lead free issues.

3. Jak je uváděno výše, komerční průmysl je poháněn změnami v elektronice, což znamená, že mnoho obranných položek trápí problémy zastarávání, ještě před tím, než začnou sloužit svému účelu. To vyžaduje, aby bylo předem vykonáno značné množství plánovací práce, aby se zajistilo, že problémy s náhradními díly nezpůsobí nepohotovost položky. Opakem této situace je ta, kde má obrana problémy s technologií, zde je nepravděpodobné, že by průmysl byl ochoten posunout věci dopředu, neboť celkový počet ovlivněných položek je významně menší, než jaká je zkušenost v jakémkoli komerčním chodu elektronické položky.

3. As referenced above, commercial industry is driving the change in electronics at a pace which means that many defence items are suffering from obsolescence issues before they even enter service. This requires considerable planning work to be done up front to ensure that spares issues do not cause unavailability of item. The reverse of this situation is that where defence has issues with technology, it is unlikely that industry will be willing to move things forward as the total number of items affected is significantly less than that experienced in any commercial run of an electronic item.

4. Problémy identifikované výše jsou obzvlášť závažné, pokud uvažujeme komerčně nakupovaný materiál, který také přináší problémy, jako je nemožnost ovlivnit návrh a nedostatek v porozumění charakteristikám spolehlivosti, jež se spíše projeví ve vojenském prostředí, ve srovnání s komerčním prostředím.

4. The issues identified above are particularly relevant when considering Commercial Off The Shelf (COTS) items which also bring issues such as lack of design influence and a lack of understanding of the dependability characteristics that are likely to be exhibited in a military environment when compared to the commercial environment.

5. V některých případech budou existující vojenské položky integrální částí návrhu nebo budou spolupracovat s nově navrhovanými položkami. V těchto případech budou charakteristiky spolehlivosti konečné položky ovlivněny charakteristikami těchto existujících částí. Jestliže má existující položka pouze 90% bezporuchovost, pak jakýkoli vývoj, který ji zahrnuje, může pak dosáhnout maximálně 90% bezporuchovosti, pokud nebude v návrhu obsažena nějaká forma zálohování.

5. In some cases existing military items will be an integral part of the design or will need to interface with the new design items. In these cases the dependability characteristics of the final item will be influenced by the characteristics of those existing parts. If an existing item only has 90% reliability then any development that incorporates it can only ever achieve 90% reliability unless some form of redundancy is included in the design.

6. V případě komunikačních systémů se lze spolehnout na komerční položky pro zorientování se nebo pro jiné nakládání, často na základě ceny za hodinovou sazbu. Za těchto okolností armáda velmi málo ovlivní, jak a kde bude prováděna údržba nebo celková pohotovost služby. V těchto případech budou požadavky na spolehlivost vojenské položky vyžadovat, aby byly brány v úvahu i části, které jsou mimo vojenský vliv nebo řízení.

6. Communication Systems can rely on commercial items to provide ‘routeing’ or other handling, often on a cost by the hour basis. In these circumstances the military have very little influence over how and when maintenance is conducted or the overall availability of the service. In these cases the dependability requirements of the military item will need to take account of the parts that are outside of military influence or control.

2.9 Omezení nákladů

1. Vždy je nezbytné brát v úvahu, že jakékoli požadavky na spolehlivost bude třeba přezkoumat ve vztahu k celkovému rozpočtu na položku. Dosáhnout vysoké úrovně spolehlivosti může být nákladné a pravděpodobně bude muset být nalezena rovnováha mezi náklady a spolehlivostí.

2.9 Cost Constraints

1. It is always necessary to consider that any dependability requirements may need to be reviewed against the overall budget for the item. To achieve high levels of dependability can be costly, and it is likely that a balance between cost and dependability will have to be made.

2. Položka, která dosáhne vyšší úrovně bezporuchovosti, bude intuitivně vyžadovat méně údržby a menší množství náhradních dílů během svého života; a tedy větší investování během etapy návrhu za účelem zlepšení bezporuchovosti může vést k nižším nákladům životního cyklu, avšak toho může být velmi obtížné dosáhnout a prokázat. Je si třeba rovněž uvědomit, že náklady na dosažení bezporuchovosti často rostou exponenciálně a tedy dosažení několika posledních procentních bodů z požadavku nemusí poskytnout dobrou

2. An item that achieves higher levels of reliability will intuitively require less maintenance and less spares through its life; thus investing more during the design stage to improve reliability can lead to lower life cycle costs, however this can be very difficult to achieve and prove. It should also be recognised that the cost of achieving reliability often increases in an exponential way thus achieving the last few percentage points of a requirement may not provide good value for money.

hodnotou za danou cenu.

3. Jednou z potvrzených cest zvyšování bezporuchovosti je zvýšit zálohování navyšováním počtu dílčích komponent obsažených v položce. Přestože to zredukuje počet poruch během úkolu, počet poruch dílčích komponent takto navýší počet náhradních dílů, rozsah požadované údržby a rovněž porostou i náklady životního cyklu.

3. One of the acknowledged ways of increasing reliability is to add redundancy by increasing the number of sub-components contained within an item. Although this will reduce the number of mission failures, the number of sub-component failures will increase thus the number of spare parts, the amount of maintenance required and the life cycle costs will also increase.

3 CHARAKTERISTIKY SPOLEHLIVOSTI

3.1 Pohotovost

1. Pohotovost je definována[7] jako „schopnost být ve stavu schopném pracovat tak, jak je požadováno“ a je udávána dobou, kdy je položka v provozním stavu ve srovnání s uplynulým kalendářním časem, takže nejjednodušším způsobem může být vyjádřena matematicky pomocí vzorce

$$\frac{doba\ použitelného\ stavu}{celková\ doba}$$

nebo

$$\frac{doba\ použitelného\ stavu}{doba\ použitelného+nepoužitelného\ stavu}$$

2. Jak se uzavírání smluv posouvá od tradičního přístupu s využitím organického zabezpečení smluv založených na ukazatelích, stává se pohotovost nejběžněji používanou charakteristikou při definování požadavků na spolehlivost. Jak bude uvedeno dále, jsou různé druhy pohotovosti, z nichž některé lze snadno definovat a vypočítat hodnotu a další, u nichž je možno je jednoduše definovat, ale je mnohem těžší je vypočítat nebo změřit jejich hodnotu. Existuje tedy mnoho způsobů jak rozepsat a specifikovat pohotovost, ať už se jedná

3 DEPENDABILITY CHARACTERISTICS

3.1 Availability

1. Availability is defined[7] as ‘ability to be in a state to perform as required’ and is a measure of the time the item is in an operable state when compared to elapsed calendar time so in its simplest form can be represented mathematically by the formula

$$\frac{Uptime}{Totaltime}$$

or

$$\frac{Uptime}{Uptime+Downtime}$$

2. As defence contracting moves from the traditional approach using organic support towards performance based contracts, Availability is becoming the most commonly used characteristic when defining dependability requirements. As will be shown later on there are differing types of availability, some of which are easy to define and calculate values for and others which, whilst easy to define, are much harder to calculate or measure values for. There are also many ways to break down and specify availability be it for an individual part within an item, the

[7] Definice pohotovosti je převzata z IEC 60050-192. The definition of availability is taken from IEC 60050-192.

o jednotlivou část položky, celou položku nebo několik položek buď na úrovni strojového parku, nebo na jisté úrovni provozní jednotky.

whole item or a number of items either at the fleet level or at some operational unit level.

3. Jak je popsáno dříve v tomto standardu v části „Strategie pořizování“, musí se věnovat pozornost specifikování pohotovosti, aby se zajistilo, že dosažená úroveň pohotovosti skutečně dodává schopnost, kterou uživatel očekával. Vůbec nelze požadovat pohotovost 100 %, protože v určitém bodě v čase se vždy vyskytne porucha a zatímco návrh může být takový, že většina poruch může být snížena pomocí zálohování nebo alternativními metodami poskytnutí služby, náklady na snížení oproti nákladům na 1 ze 100 000 případů brzy dosáhnou nepřijatelných úrovní, je tedy normální muset akceptovat určitou dobu nepoužitelného stavu, jakkoli malá může být. Aby se zajistilo, že se během těchto výpadků nesleví ze způsobilosti na nepřijatelnou úroveň, doba nepoužitelného stavu má být ohraničena uvedením délky času, kdy může způsobilost nebýt v pohotovosti a jak často může způsobilost nebýt v pohotovosti během kalendářního období.

3. As described earlier in the document under the procurement strategy heading, care must be taken when specifying availability to ensure that the achieved level of availability actually delivers the capability that the user anticipated. No availability requirement can ever be 100% as failure will always occur at some point in time and whilst the design can be such that most failures can be mitigated through redundancy or alternate methods of service provision, the cost of mitigating against those 1 in 100,000 events soon rises to unacceptable levels, thus it is normal to have to accept some downtime, however small that may be. To ensure that capability is not compromised to an unacceptable level during these outages, the down time should be bounded by specifying the length of time the capability can be unavailable for and how often the capability can be unavailable in a calendar period.

4. Vzal-li poskytnutí „sítě“ jako příklad, uživatel specifikoval, že musí být v pohotovosti po 99,8 % času. Za kalendářní rok (365 dnů) to umožňuje síti nebýt v pohotovosti až 17,5 hodiny, ale požadavek, jak je postaven, nedává žádná omezení, jakým způsobem narůstá doba nepoužitelného stavu. Jedním z extrémů je, že tato doba může nabýt hodnot 17,5 hodin jednou během kalendářního roku, což by mělo mít pro komunikační síť vážné následky. Dalším extrémem může být, že nebude v pohotovosti okolo tří minut každý den, což může narušit důvěru uživatele v dobré fungování sítě mnohem víc, než jediný výpadek zmíněný výše. V obou případech je prokazovaná úroveň pohotovosti stejná a vyhovuje požadavku na 99,8 %, jak bylo specifikováno. Aby se tomu

4. Taking the provision of a ‘network’ as an example, the user has specified that it has to be available for 99.8% of the time. In a calendar year of 365 days this allows for the network to be unavailable for 17.5 hours but the requirement as it stands puts no constraints around how that down time is accrued. At one extreme the network could be down for 17.5 hours once during the calendar year which for a communication network would have serious consequences. At the other extreme it could be unavailable for close to 3 minutes every day, which could erode user confidence in the network far more than the one off occurrence previously referred to. In either case the demonstrated level of availability is the same and meets the 99.8% requirement as specified. To get around this it is

vyhnulo, je doporučeno, aby uživatel definoval, kolikrát maximálně je přijatelné mít nějakou dobu nepoužitelného stavu během jednoho roku, a jak dlouho může maximálně trvat uvést síť z nepoužitelného stavu zpět do stavu on-line. Toho by se typicky dosáhlo nastavením požadavků na bezporuchovost a udržovatelnost, které jsou souměřitelné s požadavkem na pohotovost.

5. Vezmeme-li v úvahu obecný pojem pohotovosti, existuje několik standardních definic, které jsou používány v závislosti na tom, co je obsaženo v měřené době nepoužitelného stavu:

a. **Inherentní pohotovost** je ukazatel pohotovosti položky za ideálních podmínek, tj. za předpokladu, že vycvičená osoba provádějící údržbu, náhradní díly, nástroje a zkušební zařízení požadované k provedení údržbářského zásahu po poruše jsou všechny ihned k dispozici. Je to nejběžnější metrika*), která je zahrnuta do smlouvy, protože jediná obsahuje dobu nepoužitelného stavu spojenou s prováděním zásahu údržby po poruše, která je řízena orgánem pro návrh[8] a je zaměřena na zajišťování, že doba nepoužitelného stavu způsobená návrhem je optimalizovaná. Je-li v rámci specifikací použita inherentní pohotovost, musí se dát pozor na řízení očekávání, neboť je velmi nepravděpodobné, že jí může být v provozu dosaženo, neboť zde vždy existují nějaká logistická zpoždění, která budou muset být zahrnuta.

*) Národní poznámka: Slovo **metrika** může mít několik významů:
– pojem z matematické analýzy a teorie metrických prostorů, zobecňující vzdálenost,
– měřitelný údaj procesu, činnosti nebo ukazatele,

recommended that the user defines the maximum number of times it is acceptable to have any down time during the year, and when the network is down the maximum time it can take before it is back on line. This would typically be done by setting reliability and maintainability requirements that are commensurate with the availability requirement.

5. Having considered the generic concept of availability there are a number of standard definitions that are used depending on what is included within the measured downtime:

a. **Inherent availability** is a measure of the availability of the item under ideal conditions, i.e. assuming that a trained maintainer, the spare parts, the tools and test equipment required to undertake corrective maintenance action are all to hand immediately. It is the most common metric that is included in a contract as it only includes the down time associated with carrying out corrective maintenance action activity which is within the control of the design authority and it focuses attention on ensuring that down time due to design is optimised. If inherent availability is used within a specification, care must be taken to manage expectations as it is very unlikely that it can be achieved in service because there will always be some logistic delays that will need to be included.

[8] **Orgán pro návrh** je organizační celek MO nebo organizace mimo rezort, která je beze zbytku odpovědná za návrh a vývoj produktu.

– sada údajů o komunikační cestě v síti.

b. **Provozní pohotovost** dává mnohem realističtější pohled na úrovně pohotovosti, které mohou být dosaženy v provozu, neboť zahrnuje logistická zpoždění, ale je obtížnější je měřit a tím dosáhnout podoby, se kterou všichni souhlasí. Co všechno tvoří logistické zpoždění je velmi diskutované téma s ne zcela jasnou odpovědí a s nejasnými pravidly, která mohou být použita na každý údržbářský zásah po poruše. Pokud část zkušebního zařízení nebo nástroje, který je vyžadován, nebyla vrácena na jeho „správné místo“ po předchozí činnosti a trvá to 30 minut, než se najde, může být toto počítáno do logistického zpoždění vůči položce? Uvedení požadavků na provozní pohotovost do smlouvy zdůrazní tento typ problémů a vyžaduje napsání mnoha pravidel, aby se zajistilo, že požadavky jsou jasné a jednoznačné.

b. **Operational availability** gives a more realistic view of the levels of availability that can be achieved in service because it includes logistic delays but it is more difficult to measure and thus gain a figure that is agreeable to everyone. What truly constitutes logistic delay is a much debated topic with no clear answer and no clear rules that can be applied to every corrective maintenance action. If the piece of test equipment or tool that is required has not been returned to its ‘correct location’ following a previous activity and it takes 30 minutes to locate it, can this be counted as logistic delay against the item? Putting an operational availability requirement into a contract highlights this type of issue and requires many rules to be written to ensure the requirement is clear and unambiguous.

6. Požadavky na pohotovost položky mohou být specifikovány počtem úrovní, v závislosti na tom, co je požadováno. Je-li položka částí strojového parku, může být vhodné nastavit požadavek na pohotovost pro celý strojový park nebo pro jeho různé části, například vozidla se často rozdělují na provozní a výcvikový park, přičemž provozní park mívá vyšší požadavek na pohotovost než výcvikový park. Může se stát, že položka sama má požadavek na pohotovost nebo může být výhodné nastavit požadavek na pohotovost pro část položky, například dieselové generátory na lodi mohou mít požadavek na pohotovost, stejně jako loď samotná. Je třeba dbát opatrnosti pro zajištění, aby požadavky byly navzájem souměřitelné tak, aby úroveň pohotovosti požadované pro vyšší sestavu nepřesáhla úroveň, která je eventuálně stanovena pro pohotovosti nižší úrovně.

6. Availability requirements for an item can be specified at a number of levels depending on what is required. If the item is part of a fleet it may be appropriate to set an availability requirement for the whole fleet or for different parts of the fleet, for example vehicles are often split into operational and training fleets with the operational fleet having a higher availability requirement than the training fleet. It may be that the item itself has an availability requirement or it may be beneficial to set an availability requirement for a part of the item, for example the diesel generators in a ship may have an availability requirement as well as the ship itself. Care needs to be taken to ensure that the requirements are commensurate with each other such that the level of availability requested for the higher assembly is not in excess of that which is possible given the lower level availabilities.

7. Metody uzavírání smluv se v některých letech posouvají od tradičních

7. Contracting methods have for some years been moving away from the tradi-

řešení organického zabezpečení směrem ke smlouvám založeným na ukazatelích, kde jsou zahrnuty specifikované úrovně pohotovosti nebo schopnosti. V takových situacích je nezbytné zajistit, aby byla specifikována data potřebná k měření úspěchu, nebo jinak, aby byla specifikována metrika a aby byla zahrnuta metoda sběru. Může být nezbytné nebo vhodnější, aby sebraná data byla zadána do schváleného modelu posuzování oproti požadavkům, zejména je-li pořizování rozsáhlé nebo se týká velkého počtu položek majetku.

tional organic support solutions towards performance based contracts where specified levels of availability or capability are included. In such situations it is necessary to ensure that the data needed to measure the success, or otherwise, of the metrics is specified and a method of collecting it is included. It may be necessary, or preferable, for the collected data to be fed into an agreed model for the assessment against the requirements particularly if provision is wide spread or against a large number of assets.

8. Při každém požadavku, je naprosto nutné zajistit, že to, co je nabízeno /nasmlouváno, je plně pochopeno a je souměřitelné s tím, co je požadováno. Není neobvyklé, že se ve smlouvách založených na ukazatelích objevuje množství/rozsah vyloučení, která, pokud nejsou plně pochopena, mohou mít významný vliv na to, co uživatel očekává. Například, při uzavírání smlouvy na letadlo jsou motory často částí samostatné smlouvy, která může znít na takové věci, jako kola a pneumatiky, některé elektronické položky a dokonce i náhradní díly, které nebyly požadovány v několika předešlých letech. Podobně způsoby a mechanismy poruch, které nejsou nebo nemohou být předpovězeny, jako je koroze nebo proražení pneumatiky, se nachází mimo smluvní podmínky a budou vyžadovat samostatné nacenění a uzavření smlouvy.

8. Whatever the requirement, it is imperative to ensure that what is offered / contracted for is fully understood and commensurate with what is required. It is not uncommon in a performance based contract for there to be a number / range of exclusions which, if not fully understood, can have significant impact on what the user is expecting. As an example, when contracting for an air vehicle, the engines are often part of a separate contract as can be such things as wheels and tyres, certain electronic items and even spare parts which have not been demanded in the preceding few years. Similarly failure modes and mechanisms that have not, or can not be, predicted such as corrosion or tyre puncture are often outside of the contractual terms and will require to be costed and contracted for separately.

9. Pohotovost může být dobrým parametrem pro definici v jakékoli etapě pořizování, od počátku předkoncepční etapy, až do etapy využívání a zabezpečení včetně. Jak bylo uvedeno v předchozích odstavcích, má se věnovat pozornost zajištění, aby charakteristiky, které mají největší dopad na pohotovost, byly také mnohem podrobněji definovány v průběhu vyzrávání položky. V předkoncepční etapě a etapě koncepce může být přijatelné specifikovat pouze požadavek na nejvyšší úroveň pohotovosti, aby se

9. Availability can be a good parameter to define at any stage of procurement from early pre-concept up to and including utilisation and support. As has been shown in the preceding paragraphs care should be taken to ensure that the characteristics which have the greatest impact on availability are also more closely defined as the item matures. In pre-concept and concept stages it may be reasonable to only specify a top level availability requirement to ensure that operational needs can be met, but as the

zajistilo, že bude dosaženo provozních potřeb, ale jak návrh vyzrává a požadavky na použití se stávají jasnějšími, je mnohem a mnohem důležitější zajistit, aby doba nepoužitelného stavu byla ohraničena tak, aby neměla významný dopad na provozní požadavky.

3.2 Bezporuchovost

1. Bezporuchovost je buď definována[9] jako charakteristika položky nebo jako míra ukazatele. Jako definice charakteristiky položky je to schopnost plnit požadovanou funkci v daných podmínkách a v daném časovém intervalu, zatímco jako míra ukazatele je to pravděpodobnost být schopen plnit funkci jak je požadováno v daných podmínkách v daném časovém intervalu.

2. Pro položku mohou být definovány různé úrovně bezporuchovosti, aby pokryly odlišné úrovně zhoršení ukazatele, nejběžnější jsou porucha úkolu a základní poruchy, jak je ukázáno níže:

a) Bezporuchovost úkolu – je mírou bezporuchovosti položky a zahrnuje pouze takové poruchy, které učiní položku neschopnou provozu nebo nezpůsobilou provést úkol.

b) Základní bezporuchovost – je mírou bezporuchovosti položky odrážející celkovou intenzitu poruch položky.

3. Aby se to dostalo do kontextu, porucha vnitřního osvětlení v rodinném automobilu může být uživatelem považována za méně důležitou nepříjemnost, zejména když nastupujeme nebo vystupujeme z auta ve tmě, ale neučinila by automobil neprovozuschopným a byla by nejspíš považována za základní poruchu. Avšak porucha na čerpadle paliva nebo vody by učinila automobil neprovozuschopným a nejspíš by byla

design matures, and the usage requirements become clearer, it becomes more and more important to ensure that downtime is bounded so that it does not have a significant impact on operational requirements.

3.2 Reliability

1. Reliability can either be defined[9] as a characteristic for an item or as a performance measure. As a definition of a characteristic for an item it is the ability to perform under given conditions for a given time interval whilst as a performance measure it is the probability of being able to perform as required under given conditions for the time interval.

2. Various levels of reliability can be defined for an item to cover differing levels of degradation in performance, the most common being Mission Failure and basic failure as shown below:

a. Mission Reliability – A measure of item reliability including only those failures, which render the item inoperable or non-mission worthy.

b. Basic Reliability – A measure of item reliability reflecting the overall failure rate of the item.

3. To put this into context, the failure of an interior light on a family motor car may be considered a minor nuisance by the user, particularly when getting in and out of the car in the dark but would not render the car inoperable and would most likely be considered a basic failure. However failure of the fuel or water pump would render the car inoperable and would thus most likely be considered as a mission failure.

[9] Definice bezporuchovosti je převzata z IEC 60050-192.
The definitions of reliability are taken from IEC 60050-192.

považována za poruchu úkolu.

4. Nechť je poznamenáno, že základní bezporuchovost zahrnuje všechny úrovně poruch, včetně poruchy úkolu, aby řádně odrážela úhrnnou frekvenci poruch položky.

4. It should be noted that Basic reliability includes all levels of failure, including mission failures, to properly reflect the total failure frequency of the item.

5. Bezporuchovost úkolu a základní bezporuchovost jsou dva popisovače, které mohou být použity, ale existuje i mnoho dalších, které zahrnují (ale nejsou omezeny pouze na tyto) skladovací, latentní, hlavní a kritickou. Ať je vybrán jakýkoli popis, který má být použit pro uvažovanou položku, je povinností, aby popisovače úrovně zhoršení nebo definice této poruchy byly obsaženy ve specifikaci, aby se zajistilo, že každý člověk spojený s touto položkou porozumí jasně a jednoznačně této smluvní podmínce.

5. Mission and Basic are two of the descriptors that can be applied to reliability, but many others exist too, including, but not limited to Storage, Dormant, Major, and Critical. Whatever descriptors are chosen to be applied for the item that is under consideration it is imperative that the level of degradation or definition(s) of those failure descriptors are included within the specification to ensure everyone associated with that item has a clear and unambiguous understanding of the term.

6. Bezporuchovost může být specifikována několika různými způsoby, a když ani jeden způsob nemůže být považován za nejlepší k pokrytí každé okolnosti, některé metody mohou být za jistých okolností méně vhodné, než jiné.

6. Reliability can be specified in a number of different ways and whilst no one way can be considered as best to cover any circumstance, some methods can be less appropriate than others under certain conditions.

7. Nejběžnější a pravděpodobně nejuznávanější metodou specifikování bezporuchovosti je uvádění střední hodnoty pomocí termínů, jako je Střední doba mezi poruchami (MTBF) pro opravitelné položky nebo Střední doba do poruchy (MTTF) pro neopravitelné položky. Specifikované hodnoty mají být takové, které dosáhnou minimálních provozních požadavků uživatele a mají být souměřitelné s libovolným požadavkem na pohotovost, který byl definován. Je důležité si uvědomit, že jakýkoli požadavek specifikovaný touto cestou je pouze střední hodnotou a má se předpokládat, že významná množství z populace selžou ještě před tím, než bude dosaženo střední doby, tedy specifikování 200 hodin MTBF pro zabezpečení provozního požadavku 200 hodin, bude mít za následek poruchu. Měli bychom si povšimnout, že specifikování střední hodnoty bez některých doplňují-

7. The most common, and probably most recognised, method of specifying reliability is to quote it as a mean value using a term such as Mean Time Between Failure (MTBF) for a repairable item or Mean Time To Failure (MTTF) for a non repairable item. The values specified should be those that achieve the users' minimum operating requirement and should be commensurate with any availability requirement that has been defined. It is important to recognise that any requirement specified in this way is only a mean value and it should be expected that significant numbers of the population will fail before the mean time is reached, thus specifying a 200 hour MTBF to support an operating requirement of 200 hours will result in failure. It should also be noted that that specifying a mean value without any supporting information is of no benefit to the items being purchased. Consideration must be

cích informací není pro nakupovanou položku přínosem. Musí být uváženo, zda „doba“ je založena na hodinách provozu, kalendářním čase nebo nějaké transformaci založené na známých faktorech, jako jsou počty vzletů a přistání letadel, vzdálenost pro automobily nebo počet výstřelů pro zbraň. Je také nezbytné zajistit, aby byla každá střední hodnota jasně doložen LCEP.

given to whether the ‘time’ is based on hours of operation, calendar time or some transformation based on known factors such as take offs and landings for an aircraft, distance for a vehicle or number of firings for a gun. It is also necessary to ensure that any mean value is clearly supported by a LCEP.

8. Bezporuchovost může být také definována jako pravděpodobnost úspěchu s nebo bez přiřazené provozní doby. Požadavek pro jednorázové zařízení (typicky je to řízená střela) by byl specifikován jako pravděpodobnost úspěchu bez vymezení času, neboť uživatel chce záruku, že když bude tato položka použita, bude úspěšně pracovat ve vztahu ke svému předem definovanému LCEP. Položka, u níž by se očekávalo, že by měla opakovat podobné nebo různé LCEP vícekrát, například automobil, by byla specifikována vymezením času, kde toto vymezení času je rovno délce úkolu.

8. Reliability can also be specified as a probability of success, with or without an associated specified operating time. The requirement for a one shot device, typically a missile, would be specified as a probability of success without a time qualification as the user wants assurance that when that item is used it will operate successfully against its predefined LCEP. An item that would be expected to repeat similar or differing LCEP many times, a vehicle for example, would be specified with a time qualification where the time qualification is equal to the length of the mission.

9. Všechny příklady požadavků uvedených výše mají kvantitativní podstatu, tj. mohou být specifikovány a měřeny numericky, ale je také možné specifikovat požadavky kvalitativně, tj. ve vztahu ke kvalitě položky. Tento typ požadavku na bezporuchovost často souvisí s návrhem položky, čehož příklady jsou uvedeny níže:

9. All of the example requirements above are of a quantitative nature, i.e. can be specified and measured in a numerical way, but it is also possible to specify requirements in a qualitative way, i.e. relating to the quality of the item. For reliability this type of requirement often relates to the design of the item, examples of which are below:

a. Jednobodová porucha – položka musí být navržena tak, aby žádný jednotlivý poruchový stav nemohl způsobit poruchu kritickou pro úkol nebo bezpečnost.

a. Single Point of Failure - The item shall be designed such that no single fault can cause a mission or safety critical failure within it.

b. Oddělené cesty – položka musí být navržena tak, aby byly záložní části položky drženy nezávisle zajištěním, že kabely, dodávka energie a cesty pro signály mají dobře definované oddělené cesty.

b. Path Separation – The item shall be designed such that redundant parts within the item are kept independent by ensuring that cables, power supplies and signal routes have well defined separate paths.

10. Ať je bezporuchovost specifikována jakkoli, je nutné zahrnout definice poruch odpovídající každé úrovni bezporuchovosti tak, jak je definováno v části 2.4 tohoto ČOS.

11. Jak je popsáno v části o pohotovosti, je důležité mít na paměti, že je-li uzavírána smlouva na poskytnutí pohotovosti nebo schopnosti, může být vyžadován samostatný požadavek na bezporuchovost.

12. Bezporuchovost jako parametr může být specifikována v jakékoli etapě pořizování, ale může být obtížnější definovat ji v předkoncepční etapě a etapě koncepce zejména tam, kde není známa technologie a řešení návrhu konečné položky. V těchto případech musí být věnována pozornost zajištění, že pokud jsou nastaveny požadavky na bezporuchovost, nepředepisují se řešení návrhu nebo omezení návrhu taková, že neuvažují inovace nebo využití výhod objevující se, ale neodzkoušené technologie.

3.3 Udržovatelnost

1. Udržovatelnost je buď definována[10] jako charakteristika položky nebo jako míra ukazatele. Jako definice charakteristiky položky je to schopnost setrvat ve stavu nebo vrátit se do stavu, v němž může plnit požadovanou funkci, za daných podmínek použití a údržby, zatímco jako míra ukazatele je to pravděpodobnost, že daný údržbářský zásah prováděný za daných podmínek a používající specifikované postupy, může být dokončen v časovém intervalu (t1, t2), jestliže je činnost zahájena v t = 0. Pro účely nastavení smysluplných požadavků je udržovatelnost brána jako míra ukazatele.

10. However reliability is specified, it is imperative that failure definitions relevant to each level of reliability are included as defined in section 2.4 of this document.

11. As described in the section on availability above, it is important to remember that a separate reliability requirement may be required when contracting for availability or capability.

12. Reliability as a parameter can be specified at any stage of procurement but can be more difficult to define in the preconcept and concept stages particularly where the technology and design solution of the final item are not known. In these instances care must be taken to ensure that if a reliability requirement is set it does not dictate the design solution or constrain the design such that innovation or taking advantage of emerging but unproven technology is not considered.

3.3 Maintainability

1. Maintainability can either be defined[10] as a characteristic for an item or as a performance measure. As a definition of a characteristic for an item it is the ability to be retained in, or restored to a state to perform as required, under given conditions of use and maintenance whilst as a performance measure it is the probability that a given maintenance action, performed under stated conditions and using specified procedures and resources, can be completed within the time interval (t1, t2) given that the action started at t = 0. For the purposes of setting meaningful requirements maintainability is taken to be a performance measure.

[10] Udržovatelnost je definována v IEC 60050-192. Maintainability is defined in IEC 60050-192.

2. Je v uživatelově zájmu porozumět, jak dlouho bude trvat navrácení položky zpět do plně provozních podmínek po jakémkoli incidentu. Doba bude závislá na dvou faktorech: fyzická doba, po kterou trvá diagnostika a provedení opravy a doby, za kterou obdržíme požadovaný náhradní díl, nástroje a osobu provádějící údržbu schopnou provést práci; tato druhá doba bývá uváděna jako logistické zpoždění a je většinou mimo vliv nebo řízení osoby navrhující položku. Aby se mohly rozlišit tyto dvě různé doby, je běžné uvádět dobu diagnostiky a opravy jako Aktivní dobu opravy (ART) a doba zahrnující logistické zpoždění bývá uváděna jako Doba do opravy (TTR).

2. The user is interested in understanding how long it will take to bring an item back to a fully operational condition following any incident. The time will be dependent on two factors: the physical time it takes to diagnose and undertake the repair and the time to obtain the required spares, tools and a maintainer capable of undertaking the work, this later time being referred to as logistic delay and which is mostly outside of the influence or control of the item designer. In order to differentiate between these two differing times it is normal for the diagnose and repair time to be referred to as Active Repair Time (ART) and the time including logistic delay to be referred to as Time To Repair (TTR).

3. Pokud by každá úloha zotavení použitelná pro položku byla vázána na dobu a byla plánována, pak by bylo vytvořeno jedinečné rozdělení, které by mohlo být definováno určitým počtem bodů. Pokud se nastavují požadavky na udržovatelnost, jsou to body na tomto rozdělení, u nichž je požadováno, aby je uživatel definoval, buď na základě historické znalosti podobných položek, na základě očekávání aktuální technologie, nebo na základě vnímané doby, kdy uživatel může akceptovat, že položka není ve stavu pohotovosti. Obvykle se na rozdělení specifikuje více než jeden bod, aby se ohraničil jeho tvar, typické míry jsou střední hodnota, medián nebo procentní bod.

3. If every recovery task applicable to the item was timed and plotted then a unique distribution would be generated which could then be defined by a fixed number of points. When setting maintainability requirements it is points on this distribution that the user is required to define, either based on historical knowledge of similar items, expectation of current technology or on the perceived time the user can accept the item not being available. It is usual to specify more than one point on the distribution in order to bound its shape, typical measures being the Mean, Median or percentage points.

4. Nejběžnější a pravděpodobně nejsnadněji přijímaná metoda specifikování udržovatelnosti je pomocí využití střední doby, buď jako Střední doba aktivní opravy (MART) nebo jako Střední doba do opravy (MTTR). Jak je uvedeno výše, specifikování pouze střední doby samotné má velmi malý vliv na návrh položky, a tak se za nejlepší postup považuje zahrnout alespoň jeden procentní bod navíc ke střední době.

4. The most common, and probably most readily recognised, method of specifying maintainability is through the use of a mean time, either as a Mean Active Repair Time (MART) or as a Mean Time To Repair (MTTR). As stated above, simply specifying a mean on its own has very little influence on the design of the item thus it is considered best practice to include at least one percentage point in addition to the mean.

5. Specifikování dvoj- nebo vícenásobných dob pomocí procentních bodů pro požadavky udržovatelnosti vyžaduje, aby osoba navrhující položku vzala v úvahu takové záležitosti, jako je přístup do skříní, snadné vymontování částí a schopnost diagnostikovat špatnou funkci položky, v rozumném čase. Obvykle se procentní bod specifikuje poblíž horního konce rozdělení tak, že buď 90 %, nebo 95 % všech oprav musí být ukončeno ve specifikovaném čase. Společně buď se Střední dobou, nebo eventuálně s dobou, kdy je hotovo 50 % všech oprav, toto definuje přibližný tvar rozdělení doby opravy. Je-li položka silně závislá na softwaru, pak může být užitečné nastavit dobu s nižšími procentními body, v níž musí být provedeny všechny restarty softwaru.

5. Specifying two or more percentage point times for maintainability requirements requires the item designers to consider such things as access to cabinets, ease of removal of parts and ability to diagnose a malfunctioning item in a reasonable time. It is normal to specify a percentage point towards the top end of the distribution such that either 90% or 95% of all repairs shall be completed by the specified time. In conjunction with either a Mean time, or possibly a time for 50% of all repairs to be complete this defines the approximate shape of the repair time distribution. If the item is heavily dependent on software then it may be applicable to set a lower percentage point time within which all software restarts shall be accomplished.

6. Existují události, zejména ve smlouvách založených na ukazatelích, kde může být užitečné nastavení maximální doby, v níž mají být dokončeny všechny akce nebo činnosti. Smluvní sankce mohou pak být použity na jakoukoli činnost, která není ukončena v požadovaném čase. Je třeba věnovat pozornost při nastavování takových limitů, které nejsou natolik široké, aby měly na provoz položky nepříznivý vliv, a které nejsou tak těsné, aby měl dodavatel velmi malou šanci dodržet čas.

6. There are occasions, particularly in a performance based contract, where it may be applicable to set a maximum time by which all actions or activities shall be completed. Contractual penalties may then be applied to any activity that is not completed by the required time. Care needs to be taken in setting such limits to ensure that it is not so wide that it has an adverse effect on operation of the item and that is not so narrow that the supplier has very little chance of meeting the time.

7. Jsou-li požadavky na udržovatelnost nastaveny během časných etap životního cyklu, mohou být používány pro ovlivnění návrhu ve smyslu jeho udržovatelnosti před tím, než jsou učiněna rozhodnutí o návrhu. To by bylo provedeno k zajištění, že rozdělení souvisící s jakoukoli střední hodnotou navrženou výše, není nepříznivě zkresleno jednou nebo skupinou činností opravy. To by se typicky provedlo nastavením maximálního času (M Max), o němž se předpokládá, že by jej za normálních okolností žádná oprava neměla překročit, jsou-li uvažovány jen ty faktory, které

7. Maintainability requirements if set during the early stages of the life cycle can be used to influence the design in terms of its maintainability before design decisions have been made. This would be done to ensure that that the distribution relating to any of the mean values outlined above are not adversely skewed by a single, or group of repair activities. This would typically be done by setting a maximum time (M Max) which no repair should be expected to exceed under normal circumstances taking account only of those factors which are under the control of the designer.

jsou pod kontrolou osoby navrhující položku.

8. Jako příklad uvažujme položku uzavřenou v kontejneru a namontovanou na větší konstrukci, do níž je zajištěn přístup odstraněním jednoho z krytů kontejneru. To, jak jsou kryty připevněny, může mít významný vliv na dobu, kterou trvá provedení jakékoli činnosti opravy, která je na položce vyžadována. Je-li položka držena 25 normálními šrouby, které mají být odšroubovány a zašroubovány pouze klíčem, čas potřebný k dosažení přístupu do kontejneru bude významně delší, než kdyby byla položka držena podobným počtem rychloupínacích šroubů nebo zámků pro rychlé uvolnění.

9. V těchto případech by měl mít požadavek na M Max vliv na volbu upevňovacích prvků, ačkoli může být brán v úvahu i požadavek na čas a může se porovnat s cenou upevňovacího nářadí a požadavkem na jakékoli speciální nástroje, s nimiž se bude pracovat.

10. Všechny požadavky definované výše jsou kvantitativní povahy, ale udržovatelnost může být také definována kvalitativním způsobem. Některé příklady kvalitativních požadavků jsou uvedeny níže:

a. Položka nesmí obsahovat jakýkoli upevňovací prostředek, který nemůže být odstraněn šroubovákem č. 2, který je dostupný v kterémkoli komerčním obchodě s nástroji.
b. Položka musí být navržena tak, aby jakýkoli pracovník mohl provést požadovanou pravidelnou kontrolu bez speciálních znalostí nebo výcviku.
c. Položka musí být taková, že všechny položky, u nichž je po uživateli požadována pravidelná prohlídka nebo doplnění, musí být ihned jasně viditelné.

11. Udržovatelnost jako parametr může být specifikována v jakékoli etapě pořizování, ale může být obtížnější definovat ji v před-koncepční etapě a etapě

8. As an example consider an item, housed in a container and mounted on a large structure, access to which is gained by removing one of the covers of that container. How the covers are attached can have a significant influence on the time it takes to carry out any repair activity that is required by the item. If it is held on by 25 non captive bolts that have to be removed and replaced using only a spanner, the time taken to gain access to the container will be significantly longer than if it is held on by a similar number of captive bolts or quick release fastenings.

9. In this instance an M Max requirement could influence the choice of fittings that are used, although the time requirement may have to considered and possibly traded off against the cost of the fastening devices and the requirement for any special tools to operate them.

10. The requirements defined above are all of a quantitative nature, but maintainability can also be defined in a qualitative way. Some examples of qualitative requirements are given below:

a. The item shall not contain any fixing device that can not be removed using a number 2 cross head screw driver available from any commercial tool stockist.
b. The item shall be designed such that any operator can conduct the regular checks required without specialist knowledge or training.
c. The item shall be such that all items the user is required to inspect or top up on a regular basis shall be immediately obvious.

11. Maintainability as a parameter can be specified at any stage of procurement but can be more difficult to define in the pre-concept and concept stages particularly

koncepce, zejména tam, kde není známa technologie a řešení návrhu konečné položky. V těchto případech musí být věnována pozornost zajištění, že pokud jsou nastaveny požadavky na udržovatelnost, nepředepisují se řešení návrhu nebo omezení návrhu taková, že neuvažují inovace nebo využití výhod objevující se, ale neodzkoušené technologie.

where the technology and design solution of the final item are not known. In these instances care must be taken to ensure that if a maintainability requirement is set it does not dictate the design such that innovation or taking advantage of emerging but unproven technology is not considered.

3.4 Testovatelnost

1. Testovatelnost je definována[11] jako míra, do jaké může být položka testována, a je klíčová pro zajištění, že může být identifikována příčina problému, pokud již položka dále nefunguje tak, jak se očekává. Testovatelnost je charakteristika, která musí být pro položku vyprojektována a nemůže být jednoduše dodána v kterékoli pozdější etapě.

2. Od týmu provádějícího vývoj je požadováno plné porozumění tomu, jak položka funguje, a tedy i jak může podle očekávání přestat fungovat, aby určil nejlepší místo k monitorování datových signálů tak, že lze ověřit/prokázat funkčnost a lze detekovat chybná nebo chybějící data a vhodně to oznámit obsluze.

3. Detekování poruch může být dosaženo pomocí různých typů rutin zabudovaných testů (BIT), z nich některé běží nepřetržitě na pozadí, další jsou zahajovány obsluhou. Normálně by se pro detekování ztráty funkce používaly zkušební rutiny, které běží nepřetržitě na pozadí. Je-li identifikována ztráta funkce, obsluha/údržbář by spustil rutinu obsluhou zahajovaného zabudovaného testu pro hlubší identifikování příčiny poruchy.

4. Jestliže je položka složitým systémem, který zahrnuje mnoho součástí, často

3.4 Testability

1. Testability is defined[11] as the degree to which an item can be tested and is key to ensuring that when an item is no longer functioning as expected the cause of the problem can be identified. Testability is a characteristic that must be designed into the item and can not simply be added at some later stage.

2. A full understanding of how the item functions, and thus how it can cease to function as expected, is required by the development team in order to determine the best place to monitor data signals so that the functionality can be proven and erroneous or missing data can be detected and reported to the operator as appropriate.

3. Fault detection can be achieved using different types of ‘Built In Test’ (BIT) routines, some of which run continuously in the background, others which are instigated by the operator. The test routines which run continuously in the background would normally be used to detect the loss of a function. When the loss of function is identified the operator / maintainer would run the instigated BIT routines to further identify the cause of the failure.

4. When the item is a complex system that incorporates many parts, often

[11] Definice testovatelnosti je přijata z IEC 60050-192. The definition of testability is taken from IEC60050-192.

navržených jinými organizacemi, je důležité porozumět datovým signálům, které jsou v těchto součástech monitorovány, aby se zajistilo, že jejich význam bude dostupný obsluze. Mnoho počítačových položek obsahuje udržovací baterii, která umožňuje zachovat základní informace o datu a čase, které jsou kritické pro schopnost položky fungovat správně. Skoro všechny tyto položky mají výstražný signál, aby oznámily, že baterie potřebuje výměnu, a je zásadní, aby tento signál byl dán na vědomí obsluze, takže ve vhodném čase může provést výměnu, radši, než by nechala položku selhat a možná by tím učinila složitý systém neschopný provozu.

designed by other organisations, it is important to understand the data signals that are monitored within those parts to ensure those of significance can be accessed by the operator. Many computer based items incorporate a 'keep alive' battery that maintains basic date and time information that are critical to its ability to function correctly. Almost all of these items have a 'warning signal' to say that battery needs changing and it is vital that this signal is brought to the attention of the operator so that replacement action can be taken at a convenient time rather than letting it fail and maybe rendering the complex system unserviceable.

5. Podobně mnoho současných automobilových motorů má složité systémy řízení, a tak když vezmeme komerční motor a začleníme jej do vojenského prostředí, je zásadní porozumět všem funkcím tohoto systému řízení. Režim „dostat se domů"[12], který omezuje otáčky motoru, aby byl ochráněn v případě potenciální poruchy, může být dokonale akceptován ve výcvikové roli, ale pod palbou v nepřátelském prostředí to nemusí být pro obsluhu akceptovatelné.

5. Similarly many vehicle engines have complex management systems these days, thus when taking a commercial engine and integrating it into a military environment it is vital to understand all of the functions of that management system. A 'get you home' mode that limits engine revolutions to protect it in the event of potential failure may be perfectly acceptable in a training role but when under fire in a hostile environment may not be something the operator is happy to accept.

6. Není snadné nastavit požadavky, které stimulují návrh a jsou měřitelné, protože poskytování důkazu o shodě může vyžadovat drahé a zdlouhavé testování nebo se musí vykonat „na papíře" za použití nástrojů, jako je Analýza způsobů, důsledků a kritičnosti poruch (FMECA) nebo Analýza stromu poruchových stavů (FTA), k určení způsobů poruchy. Typickými požadavky by mohly být:

6. Setting requirements that drive the design and are measurable is not easy since providing evidence of compliance can require expensive and lengthy testing or has to be done 'on paper' using such tools as the Failure Modes Effect and Criticality Analysis (FMECA) or Fault Tree Analysis (FTA) to show which failure modes have been addressed. Typical requirements could be:

a. Pokrytí zkouškou[13] –

a. Test Coverage[13] –

[12] **Režim „dostat se domů"** je soubor parametrů navržený u daného vozidla jako strategie pro návrat vozidla do domovské základny bez dalších poškození hnacího ústrojí.

[13] The definition of Test Coverage is taken from IEC 60706-5:2007.
Definice Pokrytí zkouškou je přejata z IEC 60706-5:2007.

Poměr počtu vadných funkcí, které jsou skutečně způsobilé k diagnóze podle daných instrukcí pro testy, k celkovému počtu funkcí. Pokrytí zkouškou může být také uvažováno na základě intenzity poruch místo počtu poruch. Intenzita pokrytí zkouškou (τ) je hodnota vážená intenzitou poruch (λ):

τ = ($\Sigma\lambda$ poruch detekovaných testem / $\Sigma\lambda$ všech poruch položky)

Tato druhá definice je vhodnější pro posuzování bezporuchovosti úkolu. Poruchy během úkolu mohou skutečně vyplývat z poruch objevujících se po testu nebo z poruch objevujících se před testem, ale nebyly detekovány. Bezporuchovost úkolu může být pak posuzováno přímo z intenzity poruch a pokrytí zkouškou. Může být vyžadováno ke specifikování požadovaného pokrytí oproti specifické funkci, tj. kritickým poruchám bezpečnosti nebo úkolu. Charakteristickým požadavkem může být: „92% všech možných poruchových podmínek musí být identifikováno rutinou zabudovaného testu. Dodatečně musí být identifikováno 100% poruchových podmínek, které mohou způsobit kritickou poruchu bezpečnosti nebo úkolu“.

b. Intenzita detekování poruchových stavů – Počet poruchových stavů na položce, které mohou být identifikovány a oznámeny obsluze buď pomocí vytvoření optického zobrazení na pracovním pultu, nebo pomocí vysvícení detekčních žárovek. Může být vyžadováno, aby se specifikovala intenzita detekování vůči specifickým funkcím, tj. poruchovým stavům, které mohou způsobit poruchy kritické pro bezpečnost nebo úkol. Typickým

The ratio of the number of faulty functions actually capable of diagnosis by the given test instruction to the total number of functions. Test Coverage can also be considered on the base of failure rates instead of failure numbers. The test coverage rate (τ) is weighted by the failure rate (λ):

τ = ($\Sigma\lambda$ failures detected by the test / $\Sigma\lambda$ All failures of the item)

This second definition is more appropriate for mission reliability assessments. Indeed, failures during mission may result from failures occurring after the test or from failures occurring before the test but undetected. The mission reliability can then be assessed directly from failure rates and test coverage. It may be required to specify the coverage required against specific function i.e. safety or mission critical failures. A typical requirement may be that “92% of all possible fault conditions shall be identified by the built in test routines. Additionally 100% of the fault conditions that could cause safety and mission critical failures shall be identified.”

b. Fault detection rate – The number of fault conditions that can be identified and reported to the operator by the item either through the generation of a visual display on the operating console or through the illumination of a detection lamp. It may be required to specify detection rates against specific functions i.e. fault conditions that could cause safety or mission critical failures. A typical requirement may be that 90% of all possible faults, and 100% of faults that could cause safety or mission critical failures shall be

požadavkem může být, že 90 % všech možných poruch a 100 % poruch, které mohou způsobit poruchy kritické pro bezpečnost nebo úkol, musí být detekováno a oznámeno obsluze.

detected and reported to the operator.

c. Intenzita izolování poruchových stavů – počet poruchových stavů, které když jsou detekovány mohou být izolovány na jednotlivou jednotku, která pak může být vyměněna obsluhou. Typickým požadavkem může být, že 87 % všech možných poruchových stavů může být izolováno na jednotlivé vyměnitelné jednotky a 95 % všech možných poruchových stavů na ne více než 2 vyměnitelné jednotky.

c. Fault isolation rate – The number of fault conditions that, once detected, can be isolated to a single unit that can then be changed by the operator. A typical requirement may be that 87% of all possible faults can be isolated to a single replaceable unit and 95% of all possible faults to no more than 2 replaceable units.

d. Intenzita falešných poplachů – počet varovných zpráv poskytovaných obsluze, kdy po následném prošetření není nalezen žádný problém (také uváděno – není možné opakovat), je obvykle omezen podmínkou vyjádřenou v procentech. Typickým požadavkem může být, že „počet zpráv o poruše zobrazených obsluze, kdy po následném prošetření není nalezena žádná porucha, nesmí být větší než 4 %“.

d. False Alarm Rate – The number of alert messages provided to the operator which on subsequent investigation result in no problem being found (also referred to as being unable to replicate) is limited normally in percentage terms. A typical requirement may be that ‘No more than 4% of the failure messages displayed to the operator shall subsequently result in no fault being found.’

7. Požadavky definované výše jsou všechny kvantitativní povahy, ale testovatelnost může být také definována kvalitativním způsobem. Některé příklady kvalitativních požadavků jsou uvedeny níže:

7. The requirements defined above are all of a quantitative nature, but testability can also be defined in a qualitative way. Some examples of qualitative requirements are given below:

a. Položka musí mít způsobilost pro test „projít/selhat“[14], který může být kdykoli spuštěn obsluhou, aby poskytl důvěru, že položka je plně provozuschopná a schopná nasazení.

a. The item shall have a go/ no go capability that can be run by the operator at any time to give confidence that it is fully operable and committable.

b. Položka musí obsahovat nepřetržitě běžící rutinu zabudovaného testu,

b. The item shall contain a continuously running built in test routine that identi-

[14] To odpovídá principu testu „projít/selhat“, využívajícího podmínky dvou stavů.

která identifikuje a oznamuje obsluze ztrátu hlavní funkce.

fies and reports the loss of major functions to the operator.

8. Testovatelnost jako parametr může být specifikována v jakékoli etapě pořizování, ale může být obtížnější ji definovat v předkoncepční etapě a etapě koncepce, zejména tam, kde není známa technologie a řešení návrhu položky. V těchto etapách jsou kvalitativní požadavky pravděpodobně mnohem vhodnější než kvantitativní, které by měly být vyvinuty pro zahrnutí v pozdějších etapách pořizování.

8. Testability as a parameter can be specified at any stage of procurement but can be more difficult to define in the preconcept and concept stages particularly where the technology and design solution of the final item are not known. In these stages qualitative requirements are likely to be more appropriate than quantitative ones which should be developed for inclusion in the later stages of the procurement.

3.5 Údržba

1. Údržba je definována[14] jako kombinace všech technických a manažerských opatření zaměřených na udržení položky ve stavu, nebo navrácení do stavu, v němž může podle požadavku vykonávat funkci. Způsob, kterým se na položce bude provádět údržba, je nutno vzít v úvahu velmi brzo v procesu návrhu, pro zajištění, že jakékoli požadované činnosti mohou být provedeny bez nutnosti dlouhých zpoždění při získávání vhodného přístupu k položce a bez uvedení údržbáře do rizika poranění.

3.5 Maintenance

1. Maintenance is defined[15] as combination of all technical and management actions intended to retain an item in, or restore it to, a state in which it can perform as required. The way in which the maintenance will be undertaken on the item needs to be considered very early in the design process to ensure that any required actions can be performed without the need for lengthy delays whilst suitable access is gained to the item and without putting the maintainer at risk of harm.

2. Údržba normálně spadá do jedné ze dvou kategorií, preventivní nebo údržba po poruše, kde preventivní je definována[15] jako údržba prováděná za účelem zmírnění degradace a snížení pravděpodobnosti výskytu poruchy a údržba po poruše je definována[16] jako údržba prováděná po detekování poruchového stavu, jejímž účelem je obnovení.

2. Maintenance normally falls into one of two categories, preventive or corrective where preventive is defined[16] as maintenance carried out to mitigate degradation and reduce the probability of failure and corrective is defined[17] as maintenance carried out after fault detection to effect restoration.

[15] Definice údržby je převzata z IEC 60050-192. The definition of Maintenance is taken from IEC 60050-192.

[16] Definice preventivní údržby je převzata z IEC 60050-192. The definition of Preventive Maintenance is taken from IEC 60050-192.

[17] Definice údržby po poruše je převzata z IEC 60050-192. The definition of Corrective Maintenance is taken from IEC 60050-192.

3. Údržbu po poruše je třeba provádět ve vhodném čase brzy poté, co byl poruchový stav detekován a je jen málo, co lze udělat ve specifikaci pro její řízení. Avšak načasování a frekvence činností preventivní údržby jsou mnohem pružnější a mohou být ovlivňovány požadavky. Tyto požadavky mohou být kvantitativní i kvalitativní povahy, jak je uvedeno níže:

a. Preventivní údržba nesmí překročit dvě hodiny za týden.
b. Nasazuje-li se položka ve 30 denním úkolu, doba nepoužitelného stavu způsobená preventivní údržbou nesmí překročit 20 hodin s jednotlivou činností netrvající více než 90 minut.
c. Během požadovaných hodin provozu, které trvají od 9:00 do 17:00 od pondělí do pátku, nesmí být zapotřebí provádět žádnou preventivní údržbu.
d. Preventivní údržbu musí být možné vykonat jednou osobou za použití pouze minimální sady nástrojů, popsaných jinde ve specifikaci.
e. Všechny denní uživatelské kontroly musí být možné provést nekvalifikovanými uživateli

3. Corrective Maintenance needs to be carried out at a convenient point soon after the fault has been detected and there is little that can be done in a specification to control it. However the timing and frequency of Preventive Maintenance activity is much more flexible and can be influenced by requirements. These requirements can be of a quantitative or qualitative nature as shown below:

a. Preventive maintenance shall not exceed 2 hours per week.
b. When the item is deployed for a 30 day mission, down time due to Preventive Maintenance shall not exceed 20 hours, with no single activity taking more than 90 minutes.
c. No preventive maintenance shall need to be undertaken during the required hours of operation, these being 09:00 to 17:00, Monday to Friday.
d. Preventive Maintenance shall be capable of being undertaken by one person using only the minimum tool set described elsewhere in the specification.
e. All daily user checks shall be capable of being undertaken by unskilled users.

3.6 Bezpečnost

1. Tato část není určena k popisu obecných kritérií bezpečnosti, ale k pojednání o problémech obklopujících vzájemný vztah mezi požadavky na spolehlivost a bezpečnost a o tom, jak někdy může být nutné vyměnit spolehlivost za bezpečnost. To, že položka má dobré charakteristiky spolehlivosti, ještě neznamená, že bude bezpečná, a stejně položka, která je bezpečná, nemusí být spolehlivá, jak je požadováno.

2. Aby se zajistilo, že je položka bezpečná, může být nezbytné přidat další položky pro umožnění stálého monitorování určitých atributů a nějaká forma záznamového zařízení, kde

3.6 Safety

1. This section is not intended to describe general safety criteria, but to discuss the issues surrounding the interrelationship between dependability and safety requirements and how at times dependability may need to be traded for safety. Just because an item has good dependability characteristics does not mean it will be safe, and equally an item that is safe may not be as dependable as required.

2. In order to ensure that an item is safe it may be necessary to add additional items to enable constant monitoring of particular attributes and some form of recording device where the data can be

mohou být data ukládána. Ať jsou charakteristiky spolehlivosti takové položky jakékoli, bude to mít celkově negativní vliv na to, jak je celková položka bezporuchová, udržovatelná a tedy v pohotovosti.

stored. Whatever the dependability characteristics of this item are it will have an overall negative effect on how reliable, maintainable and thus available the overall item is.

3. Podobně požadavek, aby položka byla bezpečná, a tak se demonstrovala velmi nízká pravděpodobnost katastrofické poruchy, může stimulovat úroveň zálohování, která je vestavěna do položky. To může dostat bezporuchovost položky na mnohem vyšší úroveň, než může být normálně uvažováno za cenově efektivní.

3. Similarly the requirement for an item to be safe, thus demonstrating a very low probability of catastrophic failure may drive the levels of redundancy that are built into an item. This can drive up the level of reliability in an item to a much higher level than may normally be considered cost effective to include.

4. Požadavky na poskytnutí pracovního prostředí, které ochraňuje uživatele před některými vnějšími vlivy, může mít také dopad na charakteristiky spolehlivosti položky. Nedávné vojenské požadavky vyžadovaly, že vozidla, aby chránila uživatele před účinky výbušných zařízení, byla nevyhnutelně dovybavena pancéřováním. Přidání tohoto pancíře způsobilo nárůst celkové hmotnosti vozidel nad původní záměr návrhu, což mělo nepříznivý vliv na bezporuchovost podvozku, pérování, brzdové soustavy a výstupního výkonu. Navíc v mnoha případech bylo nezbytné sejmout pancéřování, aby se mohla provést údržba nebo oprava; tedy atributy jako je Střední doba do opravy a 95 percentil[18] dob opravy se prodloužily nad požadavek původního návrhu.

4. The requirement to provide an operational environment that protects the users of the item from some external influence may also have an impact on the dependability characteristics of an item. Recent military requirements have meant that vehicles have necessarily been up-armoured in order to protect the users from the blast effects of explosive devices. The addition of this armour has taken the all up mass of the vehicles over the original design intent which has had adverse effects on reliability of the under carriage, suspension, braking systems and power output. Additionally, in many instances it is necessary to remove the armour to undertake maintenance or repair; thus attributes such as Mean Time To Repair and the 95 percentile repair times have been extended beyond the original design requirement.

5. Požadavky na bezporuchovost často definují pravděpodobnost úspěchu úkolu, zatímco požadavky na bezpečnost často definují pravděpodobnost, že se nevyskytne nebezpečná událost. Proto, když se stanovují požadavky na bezporuchovost, mají se zohlednit i požadavky na bezpečnost. Požadavky na bezpečnost mohou ve skutečnosti vymezit

5. Reliability requirements often define the probability of mission success whilst safety requirements often define the probability of non-occurrence of a hazardous event. Therefore, when setting reliability requirements, the safety requirements should be taken into account. Indeed, safety requirements may determine the minimum acceptable

[18] **Percentil** je hodnota variační řady oddělující její stý díl.

minimální přijatelnou úroveň bezporuchovosti. Například bezpečnostní pojistka u výzbroje může mít přípustnou intenzitu poruch 1 na 106 letových hodin. Při návrhu a analýze bezporuchovosti pojistky má být proto tato intenzita poruch zohledněna.

level of reliability. For example, an armament safety switch may have an allowable hazard rate of 1 per 106 flying hours. The design and reliability analysis of the switch should, therefore, take this hazard rate into account.

6. Požadavky na spolehlivost jsou často kvalitativními požadavky, které souvisejí s bezpečností, včetně ustanovení jako „Produkce nebezpečného záření nebo energie, pokud nebyla přijata opatření k ochraně osob nebo citlivých dílčích komponent před poškozením nebo nepříznivým vlivem, je nepřijatelná“ nebo „Postupy a charakteristiky pro balení a manipulaci, které mohou způsobit neštěstí, jsou nepřijatelné“.

6. Dependability requirements often have qualitative requirements relating to safety included within them with statements such as “Generation of hazardous radiation or energy, when no provisions have been made to protect personnel or sensitive sub-components from damage or adverse effects is unacceptable” and “Packaging or handling procedures and characteristics that could cause a mishap is unacceptable.”

7. Řada způsobů používaných pro posuzování spolehlivosti položky je společných těm, které se používají pro posuzování položky z hlediska bezpečnosti, FMECA je obvyklý příklad. Ačkoli bude proces použitý při provádění FMECA pro bezpečnost i spolehlivost stejný, konečná analýza kritičnosti je pravděpodobně odlišná a má se věnovat pozornost zajištění, že výsledky z posouzení bezpečnosti nejsou přenášeny napříč přímo do posouzení spolehlivosti.

7. A number of the techniques used to assess the dependability of an item are common to those used when assessing the safety aspects of an item, FMECA being a common example. Although the process employed in conducting the FMECA for safety and dependability will be the same, the final analysis of the criticality is likely to be different and care should be taken to ensure that the results from a safety assessment are not read across directly into a dependability assessment.

3.7 Software

3.7 Software

1. Software se během nedávné minulosti stal rostoucím velkým podílem mnoha položek a nadále poskytuje stále rostoucí podíl jejich funkčností a je zcela integrální součástí nezbytnou pro jejich nepřetržitý každodenní provoz

1. Software has become an increasing large proportion of many items during the recent past and continues to provide an ever increasing proportion of their functionality, being a wholly integral part of the item vital for its continued day to day operation.

2. Na rozdíl od hardwaru, který trpí vlastnostmi opotřebování, což často předem varuje před poruchou, a když se porouchá, je nutné jej demontovat a fyzicky opravit, software se neopotřebovává, často selže bez předchozího varování, poskytujíc malou nebo žádnou indikaci, že se vyskytla porucha. Software však může být restartován nebo znovu spuštěn v relativně krátkém čase, což obnoví jeho plnou funkčnost. Fyzické změny softwaru mohou být mnohem flexibilnější, časově méně náročné a při zavádění méně nákladné než u hardwaru, ale u velkých systémů kritických na bezpečnost mohou být náklady na zkoušení, které prokáže zdárný provoz, vysoké.

2. Unlike hardware, which suffers from wear out properties that often give advance warning of failure and when it fails needs to be removed and physically repaired, software doesn't wear out, often fails without advance warning providing little or no indication that failure has occurred. Software can however be rebooted or re-initialised in a relatively short space of time returning it to full functionality. Physical changes to software can be more flexible, less time consuming and less costly to instigate than for hardware, but on large safety critical systems the cost of testing to prove successful operation can be high.

3. Opětovné použití softwaru se stává stále více samozřejmostí, ale jako u jakékoli integrace se musí věnovat pozornost zajištění, že všechny vstupy, výstupy a vzájemné závislosti jsou plně pochopeny. To, že byl softwarový modul spolehlivý v předchozí aplikaci, to automaticky neznamená, že bude spolehlivý v jakékoli nové aplikaci.

3. The reuse of software is becoming more commonplace but as with any integration care must be taken to ensure that all of the inputs, outputs and interdependencies are fully understood. Just because a software module was dependable in a previous application does not automatically mean it will be in any new one.

4. Z hlediska specifikování spolehlivosti mohou být všechny individuální charakteristiky, které jsou použity pro hardware, stejně použity i pro software. Požadavky na pohotovost mohou být nastaveny tak, aby pokryly připravenost softwaru pracovat; požadavky na bezporuchovost mohou být nastaveny tak, aby pokryly nepřetržitost softwarové služby; požadavky na udržovatelnost mohou být nastaveny tak, aby pokryly snadnost modifikování, upgradování a rozšiřování softwaru; a navíc, požadavky na zotavitelnost mohou být nastaveny tak, že pokryjí zotavení softwaru po poruše s nebo bez externích činností.

4. From the point of view of dependability specification, all of the individual characteristics that are used for hardware can equally be used for software. Availability requirements can be set to cover readiness of software operation; Reliability requirements can be set to cover the continuity of software service; Maintainability requirements can be set to cover the ease of software modification, upgrade and enhancement; In addition recoverability requirements can be set to cover software restoration following a failure, with or without external actions.

5. Za nejlepší praxi je v současnosti považováno nastavit požadavky na úrovni položky, včetně hardwaru a softwaru, nedělit požadavky na hardware a software, protože obsluhu

5. It is currently considered best practice to set the requirements at the item level including hardware and software, not breaking out the requirement in terms of hardware and software as the operator is

zvlášť nezajímá, co způsobilo, že položka řádně nefunguje, pouze, že se situace vyskytla. Pokud přijmeme tento přístup, je zásadní zajistit, aby definice poruch přímo zahrnovaly způsoby poruch vyvolané softwarem tak, aby byly spolehlivě vysvětleny během jakékoli statistické analýzy. Schopnost rychle se zotavit z poruchy způsobené softwarem nemá být důvodem pouze to přijmout a neprovést žádnou činnost k nápravě.

not particularly interested in what has caused the item not to function properly, merely that the situation has occurred. When adopting this approach it is critical to ensure that the failure definitions robustly account for software induced failure modes so that they are accounted for during any statistical analysis. The ability to recover quickly from a software induced failure should not be reason to just accept it and take no action to correct it.

6. Má-li být software specifikován nezávisle, může být za účelem posouzení příspěvku softwaru na systémové úrovni událostí/nebezpečí provedena počáteční analýza rizik, aby se stanovily úrovně softwarové integrity a takto aby se specifikovaly požadavky na návrh. Požadavky na návrh softwaru se soustředí na proces zabezpečování kvality softwaru a na metody specifické pro software.

6. If software is to be specified independently, an initial risk analysis can be undertaken to assesses the contribution of the software to system-level events/hazards in order to determine software integrity levels, and thus to specify design requirements. Software design requirements focus on the software quality assurance process and on software specific methods.

(VOLNÁ STRANA)

(VOLNÁ STRANA)

(VOLNÁ STRANA)

Účinnost českého obranného standardu od: **12. dubna 2016**

Změny::

Změna číslo	Účinnost od	Změnu zapracoval	Datum zapracování	Poznámka
1	20. 5. 2019	Úř OSK SOJ / Odbor obranné standardizace	21. 5. 2019	
2	21. 12. 2022	Úř OSK SOJ / Odbor obranné standardizace	21. 12. 2022	

Upozornění: Oznámení o českých obranných standardech jsou uveřejňována měsíčně ve Věstníku Úřadu pro technickou normalizaci, metrologii a státní zkušebnictví v oddíle „Ostatní oznámení“ a Věstníku MO.

V případě zjištění nesrovnalostí v textu tohoto ČOS zasílejte připomínky na adresu distributora.

Rok vydání: 2022, obsahuje 26 listů
Distribuce: Odbor obranné standardizace Úř OSK SOJ, nám. Svobody 471/4, 160 01 Praha 6
Vydal: Úřad pro obrannou standardizaci, katalogizaci a státní ověřování jakosti
oos.army.cz
NEPRODEJNÉ