**ČESKÁ SPOLEČNOST PRO JAKOST**
Novotného lávka 5, 116 68 Praha 1

# PŘÍPADOVÉ STUDIE REALIZACE PROJEKTŮ SPOLEHLIVOSTI

MATERIÁLY K SETKÁNÍ ODBORNÉ SKUPINY
PRO SPOLEHLIVOST

21. února 2012
Praha 1, Novotného lávka 5

# OBSAH

ŠKODA ELECTRIC a.s.

# Přínosy a úskalí sběru provozních dat RAMS ve ŠKODA ELECTRIC a.s.

Miroslav Šmiřák, dipl. tech., Řízení jakosti a environmentu ŠKODA ELECTRIC a.s.
tel. +420 603 884 652, e-mail: miroslav.smirak@skoda.cz

## 1. Úvod

Jedním z významných požadavků na funkční systém RAMS podle ČSN EN 50 126 „Drážní zařízení - stanovení a prokázání bezporuchovosti, pohotovosti, udržovatelnosti a bezpečnosti (RAMS)“ je datová základna spolehlivosti a bezpečnosti výrobků. Vytváří se sběrem, ukládáním, tříděním a zpracováním dat získaných během uvádění do provozu a během provozu výrobků u uživatele, tedy v etapě životního cyklu 11 Provoz a údržba a v etapě 12 Sledování výkonnosti. V tomto příspěvku bych chtěl představit aktuální stav datové základny spolehlivosti výrobků ŠKODA ELECTRIC a.s., její přínosy i problémy, na které při tvorbě a správě databáze narážíme.

Získávání informací z provozu výrobků společnosti je už v záručním provozu často nesnadná záležitost, v pozáručním provozu ještě mnohem obtížnější, někdy téměř nemožné. Protože jsem si ale vědomi, že bez kvalitní datové základny se neobejdeme, využíváme všech možností, jak potřebná data získávat. Nejjednodušší je situace v případech, kdy servisní zásahy na výrobcích (údržbu po poruše) provádí přímo zaměstnanci společnosti, i když ani v těchto případech to není bez problémů. Zasahující technik totiž často musí preferovat rychlost zásahu k obnově pohotovosti přímo v místě provozu před získáním úplných a pokud možno podrobných dat. Údaje potřebné pro záznam o poruše a obnově, např. bližší specifikace porouchané součásti, kilometrický proběh v době poruchy apod. se pak získávají a zaznamenávají dodatečně.

Tyto problémy jsou ale řešitelné v rámci naší interní organizace a rozdělení odpovědností. Složitější jsou případy, kdy servisní činnosti vykonává smluvní partner (zákazník, uživatel nebo třetí strana). V těchto případech se ukazuje jako nezbytné mít smluvně zakotvenou vzájemnou spolupráci výrobce (ŠKODA ELECTRIC a.s.) a zákazníka, resp. provozovatele nebo jiného subjektu provádějícího servisní činnosti) a předávání dat o provozu, poruchách a údržbě výrobku v provozu. Částečně je to řešitelné během záručního provozu, ale velmi obtížné po ukončení záručního provozu. Přitom doba záručního provozu je často pouze desetinou celkové délky provozu (užitečného života) výrobku, takže data z pozáručního provozu by byla pro výrobce nesmírně důležitá pro vytváření vlastních databází spolehlivosti a zlepšila by i predikce parametrů RAMS poskytovaných v rámci tendrů.

### 1.1 Výklad pojmů

Obecná poznámka k terminologii: v praxi se občas setkáváme s tím, že jsou nesprávně používané pojmy a zkratky, a to i v obchodních nebo v technických dokumentech, které jsou součástí smluvních vztahů. To s sebou přináší problémy například při identifikaci a přezkoumání požadavků zákazníků na produkt v oblasti RAMS nebo při jednáních s partnery. Dochází k tomu i v případech, kdy je ve stejných dokumentech uváděn odkaz na normy z oblasti RAMS. Některé případy jsou uvedeny v příspěvku Ing. J. Krause.

V příspěvku budou nejčastěji používány pojmy:

Pohotovost – „schopnost výrobku provádět požadovanou funkci v daných podmínkách, v daném časovém okamžiku nebo v daném časovém intervalu, za předpokladu, že jsou zajištěny požadované externí prostředky[1].“

Bezporuchovost (součást pohotovosti) vyjádřená např. ukazateli „intenzita poruch“, „střední doba/proběh do poruchy MTTF/MDTF“ nebo „střední doba/proběh mezi poruchami MTBF/MDBF“ (vyjadřuje „jak často se výrobek porouchá“ a co má na poruchovost největší vliv).

Udržovatelnost a Zajištěnost údržby, skládající se z plánovaných prostojů z důvodu předepsané preventivní údržby a z neplánovaných prostojů z důvodu údržby po poruše tj. prostoj nutný k obnově stavu pohotovosti (odstranění poruchového stavu).

Výrobek – je používán záměrně namísto pojmu produkt, který podle definice v EN ISO 9000 zahrnuje i nehmotný produkt, jako je např. služba nebo software apod.

## 1.2 Aktuální stav v systému RAMS

Systém RAMS podle ČSN EN 50126 byl ve ŠKODA ELECTRIC a.s. zaveden v letech 2009 až 2010, implementace byla dokončena začátkem roku 2011 před auditem systému řízení kvality podle normy IRIS[2]. Přesto zjišťujeme jak při práci na projektech, tak při auditech, že činnosti nejsou ještě „usazené“ a nejsou běžnou součástí realizačních procesů. To má několik příčin, ne jednoduchých, pokud je mohu shrnout jsou to hlavně:

* nedostatečné pochopení přínosů pro zvyšování bezporuchovosti a snižování nákladů (výsledky se neprojeví okamžitě, ale až za delší dobu);
* personální zajištění oblasti RAMS/LCC a kvalifikace personálu;
* kapacitní vytížení pracovníků odborných útvarů;
* obava alokovat požadavky na RAMS/LCC na dodavatele;
* obava vyjednávat se zákazníky nebo uživateli např. o nejasnostech v požadavcích na RAMS nebo o poskytování dat o provozu a poruchách výrobků ŠKODA ELECTRIC a.s.[3];
* nevyjasněné role a odpovědnosti útvarů a osob;
* nedostatečná zpětná vazba výstupů z databáze RAMS do technických útvarů.

Naopak jsme získali významné přínosy:

* schopnost komunikovat rovnocenně se všemi partnery v oblasti RAMS/LCC;

---

[1] Zjednodušeně ji lze vyjádřit jako poměr součtu dob vozidla v provozuschopném stavu ku součtu dob vozidla v provozuschopném stavu a v neprovozuschopném stavu, přičemž do součtu dob vozidla v neprovozuschopném stavu se uvažují jen doby z vnitřních příčin, tj. doby poruch a preventivní údržby.

[2] IRIS – „International Railways Industry Standard“, vydaná sdružením UNIFE. Vychází z požadavků normy EN ISO 9001, je proti ní obsáhlejší a podrobnější, zahrnuje mj. také povinnost zavedení systému řízení podle EN 50126 včetně řízení nákladů (LCC). V drážním průmyslu může nahrazovat normu ISO 9001 pro systémy managementu kvality.

[3] Měli bychom vždy usilovat o vypracování oboustranného „ujednání o RAMS“, zahrnujícího vyjasnění terminologie a použitých norem, parametrů RAMS, systém předávání dat o provozu, poruchách a údržbě výrobků včetně FRACAS (Failure Reporting And Corrective Action System), obsahujícího vzorce a výpočty pro hodnocení parametrů atd.): takový dokument by měl být součástí smluvních ujednání.

- máme zvládnuté techniky predikce charakteristik RAMS/LCC a máme praktické zkušenosti v konkrétních projektech;
- máme hotovou velkou část prací na vytvoření datové základny pro RAMS;
- začínáme do oblasti RAMS zapojovat některé dodavatele.

# 2. Účel a požadavky na datovou základnu

## 2.1 Historie

Data o provozu a údržbě trolejbusů byla shromažďována již v dřívějším systému INCAD používaném v tehdejší ŠKODA OSTROV. Tato základna měla definovanou vcelku dobrou strukturu dat o poruchách, s možností exportu do formátu .xls (Excel) k analýzám. Problémem bylo to, že neměla žádnou návaznost na jakoukoliv databázi finálních výrobků, nutnou pro výpočty parametrů bezporuchovosti.

Ve ŠKODA TRANSPORTATION byla data shromažďována již v 80. letech, tehdy ve formě papírových Záznamníků poruch, ze kterých byla data přepisována do formy vhodné pro zpracování. Později byly využívané xls formuláře, které práci s daty usnadnily. Z těchto zkušeností vycházela i základní představa vytvoření jednotné struktury dat ve ŠKODA. Jako nejvhodnější prostředí byl zvolen Baan ERP, obsahující modul Servis, s možností vkládat do něj data o finálních výrobcích. Postupně byla zpracovány tzv. „customizované“ (vytvořené dodatečně podle požadavků uživatele) nástroje a úlohy, které jednak doplnily možnosti v databázi finálních výrobků a jednak zcela nově umožnily zaznamenávat data o provozních poruchách a údržbě výrobků formou Hlášenky servisního zásahu (HSZ). Tuto funkcionalitu standardní Baan ERP nemá. Struktura dat v HSZ plně odpovídá požadavkům na vytvoření a správu databáze záznamů o poruchách a údržbě.

## 2.2 Požadavky na data

Aby byla databáze opravdu účinným nástrojem pro řízení spolehlivosti výrobků, musí data splňovat základní podmínky:

- Úplnost – do databáze by měla být zaznamenána každá provozní porucha výrobku; v některých případech náhodně zjišťujeme, že některé poruchy zaznamenány nejsou. Tyto případy jsou ale postupně eliminovány. Dalším problémem úplnosti dat je, že v záznamu jsou v počátku jen nejnutnější data, která technik získá při servisním zásahu. Protože často odstraňuje několik poruch najednou a je preferována rychlost obnovy (Time to Restore), je pak nutné dodatečně data doplňovat a upřesňovat. Toto dodatečné upřesnění je pak velmi obtížné u dat, které nám poskytují jiné subjekty, hlavně v případech, kdy nejsme dodavatelem finálního vozidla, ale pouze jeho částí.

- Správnost – zde se ukazuje problém s nejednotným přístupem techniků, například při klasifikaci poruchy z hlediska závažnosti dopadu na provoz a na bezpečnost. Proto je nezbytná neustálá osvěta pracovníků provádějících servisní zásahy, případně vypracování manuálu pro práci s datovou základnou.

- Věrohodnost – data pokládáme za věrohodná, pokud je sbírají a zaznamenávají zaměstnanci ŠKODA ELECTRIC a.s. Pokud je sbírají jiné subjekty a předávají nám je k záznamu do

databáze, nezbývá, než datům důvěřovat, protože máme velmi slabé nástroje pro ověřování jejich správnosti a věrohodnosti. Pochyby o správnosti a věrohodnosti dat se objevily také v případech, kdy byly výsledné hodnoty parametrů spolehlivosti vypočtené z dat v databázi, stanoveny jako motivační ukazatele vázané na odměňování těch zaměstnanců, kteří databázi plní.

### 2.3 Využití datové základny v etapách životního cyklu výrobku

Datová základna a výstupy z ní jsou nezastupitelné v některých etapách životního cyklu výrobku, pro které poskytuje významné informace:

- V etapách 1 až 5 životního cyklu výrobku, tj. v etapách Koncepce, Definice systému, Analýzy rizika, Požadavků na systém a Rozdělení požadavků na systém (tedy ve fázi „Tendr“) je zdrojem dat pro vypracování podkladů pro zákazníka v rámci nabídek / tendrů, smlouvy a pro přípravu podkladů pro objednání subsystémů a dílů u dodavatelů, a to pro:
  - stanovení hodnot bezporuchovosti nebo ověření dosažitelnosti hodnot bezporuchovosti požadovaných zákazníkem, a to před podpisem smlouvy;
  - stanovení systému preventivní údržby a údržby po poruše;
  - odhady části nákladů životního cyklu (LCC) a specifikace náhradních dílů;
  - specifikaci požadavků na nakupované subsystémy nebo díly.
- V etapě 6 Návrh a zavedení je zdrojem dat pro:
  - podrobnější analýzy bezporuchovosti, udržovatelnosti, bezpečnosti pro identifikaci a návrhů řešení „slabých míst“ návrhu výrobku;
  - optimalizaci systému preventivní údržby s cílem udržet požadovanou provozní spolehlivosti (pohotovost) výrobku, včetně plánování dostupnosti potřebných ND;
  - specifikaci nákladů životního cyklu;
  - stanovení postupů a nástrojů pro zjišťování poruch a jejich příčin a optimalizaci jejich odstraňování (diagnostika provozních stavů a poruch apod.).
- V etapě 13 Modifikace a regenerace je zdrojem dat pro:
  - ověření správnosti predikovaných parametrů RAMS;
  - hodnocení provozní spolehlivost výrobku (pohotovosti, bezporuchovosti), formou zpětné vazby ze záručního a pozáručního provozu;
  - zjišťování příčin provozních poruch;
  - stanovení a zavádění opatření v technickém řešení výrobku a v systému jeho údržby k eliminaci zjištěných příčin.

## 3. Struktura datové základny

Struktura datové základny spolehlivosti ŠKODA ELECTRIC a.s. obsahuje:

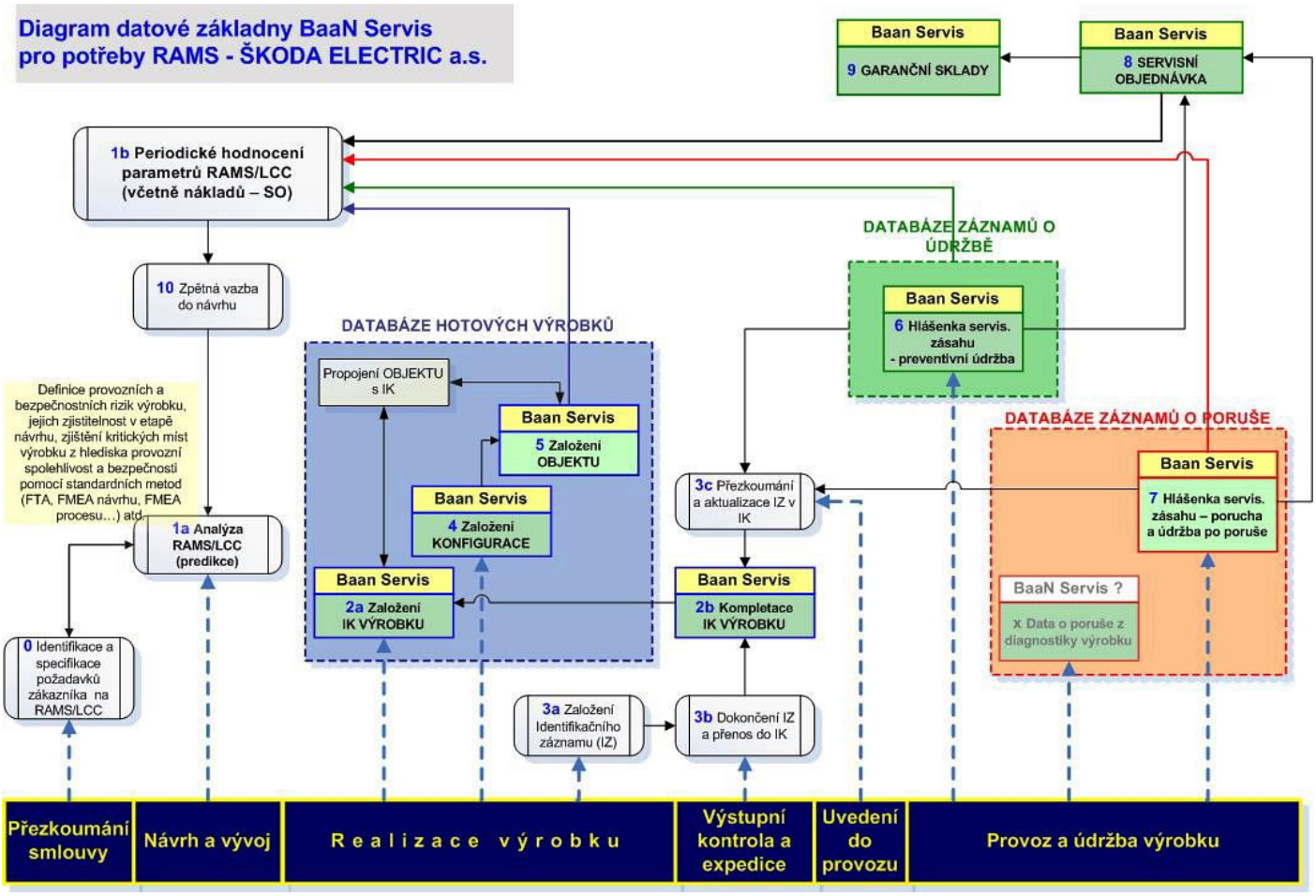
- databázi finálních výrobků a jejich specifikaci,
- funkčně orientovanou dekompozici výrobků,
- databázi záznamů o poruchách,
- databázi záznamů o údržbě po poruše.

Výhledově bude obsahovat:

* databázi záznamů o preventivní údržbě,
* databázi záznamů o zkouškách,
* databázi diagnostických záznamů.

Struktura je patrná z následujícího obrázku 1.

Obrázek 1. Struktura datové základny spolehlivosti ŠKODA ELECTRIC a.s.

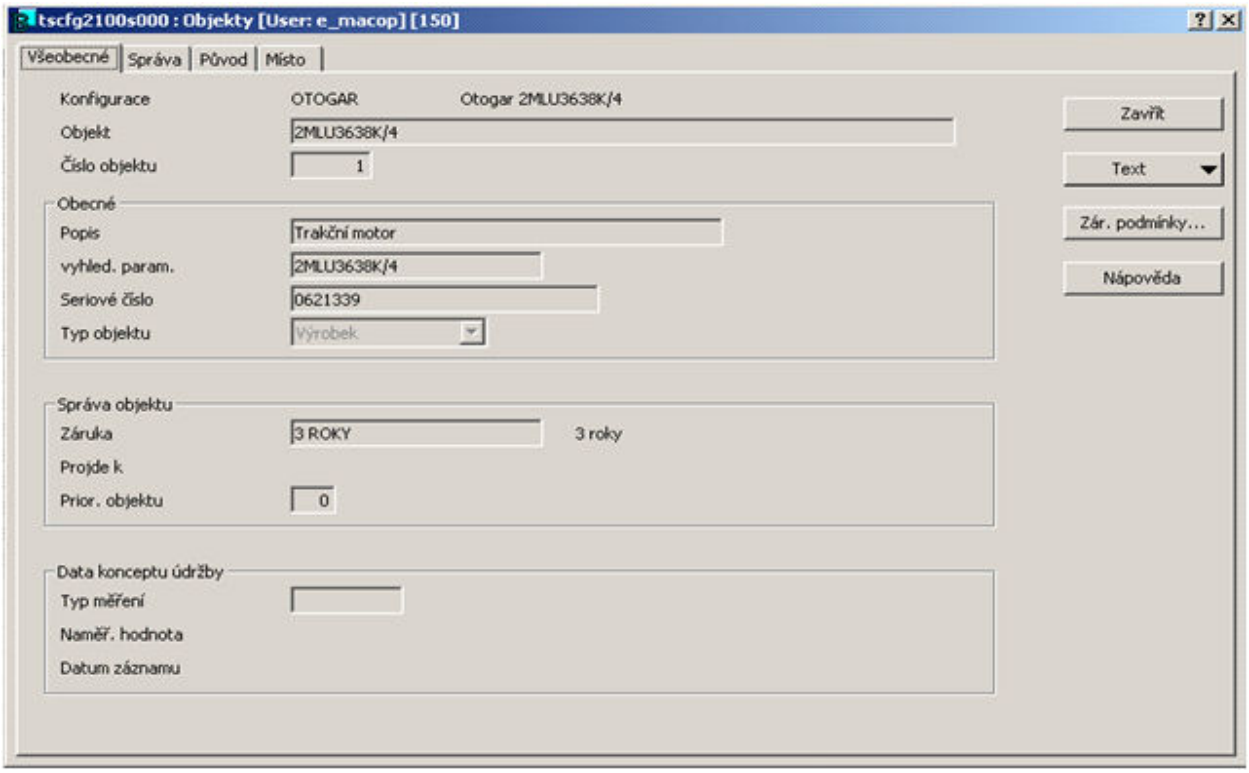



## 3.1 Databáze finálních produktů

Databáze finálních výrobků je tvořena jednak daty ve standardních nástrojích Baan ERP, modulu Servis, v tzv. Konfiguracích[4] a Objektech, a jednak v „customizovaném“ nástroji navrženém ŠKODA ELECTRIC a.s. – v Identifikačních kartách výrobků (IKV). Tyto nástroje obsahují základní data o finálních produktech společnosti potřebná pro výpočty charakteristik spolehlivosti – viz následující obrázky.

[4] Tento pojem používá systém Baan ERP v jiném smyslu, než je standardně používán pro management konfigurace

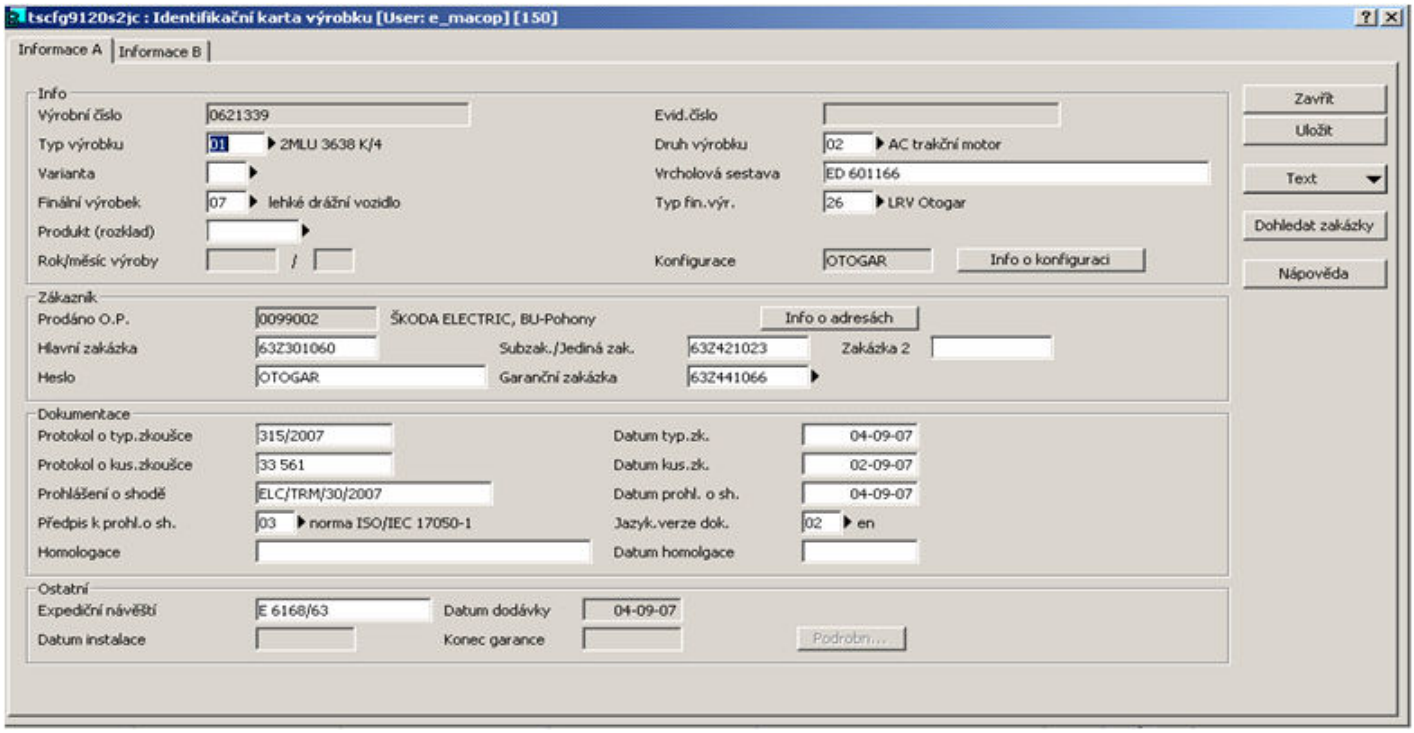
Obrázek 2. Ukázka dat – databáze finálních výrobků: Objekty konfigurace




Tabulka 1. Ukázka exportu dat z části databáze finálních výrobků – Objekty konfigurací

| Konfigurace | Objekt | Sér.číslo | Záruka (měsíc) | Projde k | Dat. dodání | Dat. instalace | Rok/Měs. výr. | Adresa lokality |
|---|---|---|---|---|---|---|---|---|
| TR_HRADE | TM9CTAJ6VBASE3624 | 13624 | 48 | 22.11.2015 | 23.11.2011 | 23.11.2011 | 2011/11 | AP2340100 |
| TR_HRADE | TM9CTAJ6VBASE3625 | 13625 | 48 | 22.11.2015 | 23.11.2011 | 23.11.2011 | 2011/11 | AP2340100 |
| TR_HRADE | TM9CTAJ6VBASE3626 | 13626 | 48 | 22.11.2015 | 23.11.2011 | 23.11.2011 | 2011/11 | AP2340100 |
| TR_HRADE | TM9CTAJ6VBASE3627 | 13627 | 48 | 22.11.2015 | 23.11.2011 | 23.11.2011 | 2011/11 | AP2340100 |
| TR_HRADE | TM9CTAJ6VBASE3628 | 13628 | 48 | 22.11.2015 | 23.11.2011 | 23.11.2011 | 2011/11 | AP2340100 |
| TR_HRADE | TM9CTAJ6VBASE3629 | 13629 | 48 | 22.11.2015 | 23.11.2011 | 23.11.2011 | 2011/11 | AP2340100 |
| TR_PARDU | TM9ATAJ6VBASE3630 | 13630 | 42 | 28.2.2015 | 1.9.2011 | 1.9.2011 | 2011/7 | AP2857300 |
| TR_PARDU | TM9ATAJ6VBASE3631 | 13631 | 42 | 28.2.2015 | 1.9.2011 | 1.9.2011 | 2011/7 | AP2857300 |
| TR_JIHLA | TM98TAJ6VBASE3609 | 13609 | 48 | 29.8.2015 | 30.8.2011 | 30.8.2011 | 2011/8 | AP2353500 |
| TR_JIHLA | TM98TAJ6VBASE3610 | 13610 | 48 | 29.8.2015 | 30.8.2011 | 30.8.2011 | 2011/8 | AP2353500 |
| TR_JIHLA | TM98TAJ6VBASE3611 | 13611 | 48 | 29.8.2015 | 30.8.2011 | 30.8.2011 | 2011/8 | AP2353500 |
| TR_JIHLA | TM98TAJ6VBASE3612 | 13612 | 48 | 29.8.2015 | 30.8.2011 | 30.8.2011 | 2011/8 | AP2353500 |
| TR_JIHLA | TM98TAJ6VBASE3613 | 13613 | 48 | 29.8.2015 | 30.8.2011 | 30.8.2011 | 2011/8 | AP2353500 |
| TR_JIHLA | TM98TAJ6VBASE3614 | 13614 | 48 | 29.8.2015 | 30.8.2011 | 30.8.2011 | 2011/8 | AP2353500 |
| TR_JIHLA | TM98TAJ6VBASE3615 | 13615 | 48 | 29.8.2015 | 30.8.2011 | 30.8.2011 | 2011/8 | AP2353500 |
| TR_JIHLA | TM98TAJ6VBASE3616 | 13616 | 48 | 29.8.2015 | 30.8.2011 | 30.8.2011 | 2011/8 | AP2353500 |
| TR_JIHLA | TM98TAJ6VBASE3617 | 13617 | 48 | 29.8.2015 | 30.8.2011 | 30.8.2011 | 2011/8 | AP2353500 |
| TR_JIHLA | TM98TAJ6VBASE3618 | 13618 | 48 | 29.8.2015 | 30.8.2011 | 30.8.2011 | 2011/8 | AP2353500 |
| T_WROCLA | 19T-WROCLAW-SADA-31 | 19T-WROCLAW-SADA-31 | 40 | 25.12.2014 | 26.8.2011 | 26.8.2011 | 2011/8 | AP2624900 |
| T_WROCLA | 19T-WROCLAW-SADA-30 | 19T-WROCLAW-SADA-30 | 40 | 21.12.2014 | 22.8.2011 | 22.8.2011 | 2011/8 | AP2624900 |
| T_WROCLA | 19T-WROCLAW-SADA-29 | 19T-WROCLAW-SADA-29 | 40 | 14.12.2014 | 15.8.2011 | 15.8.2011 | 2011/8 | AP2624900 |
| TR_PRESO | TM9DTAJ6CBASE3635 | 13635 | 24 | 3.8.2013 | 4.8.2011 | 4.8.2011 | 2011/8 | AP3420500 |
| LK_ZSR | LOKO 109E2 - SADA 02 | LOKO 109E2 - SADA 02 | 36 | 6.7.2014 | 7.7.2011 | 7.7.2011 | 2011/7 | AP2624900 |
| T_WROCLA | 19T-WROCLAW-SADA-28 | 19T-WROCLAW-SADA-28 | 40 | 28.10.2014 | 29.6.2011 | 29.6.2011 | 2011/6 | AP2624900 |
| T_WROCLA | 19T-WROCLAW-SADA-27 | 19T-WROCLAW-SADA-27 | 40 | 21.10.2014 | 22.6.2011 | 22.6.2011 | 2011/6 | AP2624900 |

Obrázek 3. Ukázka dat – databáze finálních výrobků: Identifikační karta výrobku




Tabulka 2. Ukázka exportu dat z části databáze finálních výrobků – Identifikační karty výrobků

| Výr.číslo | Konfigurace | Typ výrobku | Druh výrobku | Typ finálního výrobku | Datum dodání | Datum instalace | Garance do | Předpokládaný proběh | Skutečný proběh |
|---|---|---|---|---|---|---|---|---|---|
| 06T-CAGLIARI-SADA-01 | T_CAGLIA | 06T el. výzbroj | elektrovýzbroj | 06T Cagliari | 25.8.2005 | 25.8.2005 | | 0 | 0 |
| 06T-CAGLIARI-SADA-02 | T_CAGLIA | 06T el. výzbroj | elektrovýzbroj | 06T Cagliari | 25.8.2005 | 25.8.2005 | | 0 | 0 |
| 06T-CAGLIARI-SADA-03 | T_CAGLIA | 06T el. výzbroj | elektrovýzbroj | 06T Cagliari | 25.8.2005 | 25.8.2005 | | 0 | 0 |
| 06T-CAGLIARI-SADA-04 | T_CAGLIA | 06T el. výzbroj | elektrovýzbroj | 06T Cagliari | 26.8.2005 | 26.8.2005 | | 0 | 0 |
| 06T-CAGLIARI-SADA-05 | T_CAGLIA | 06T el. výzbroj | elektrovýzbroj | 06T Cagliari | 15.9.2005 | 15.9.2005 | | 0 | 0 |
| 06T-CAGLIARI-SADA-06 | T_CAGLIA | 06T el. výzbroj | elektrovýzbroj | 06T Cagliari | 7.4.2006 | 7.4.2006 | | 0 | 0 |
| 06T-CAGLIARI-SADA-07 | T_CAGLIA | 06T el. výzbroj | elektrovýzbroj | 06T Cagliari | 11.5.2007 | 11.5.2007 | | 0 | 0 |
| 06T-CAGLIARI-SADA-08 | T_CAGLIA | 06T el. výzbroj | elektrovýzbroj | 06T Cagliari | 11.5.2007 | 11.5.2007 | | 0 | 0 |
| 06T-CAGLIARI-SADA-09 | T_CAGLIA | 06T el. výzbroj | elektrovýzbroj | 06T Cagliari | 17.5.2007 | 17.5.2007 | | 0 | 0 |
| 10T3-PORT-SADA-01 | T_PORTLA | 10T3 el. výzbroj | elektrovýzbroj | 10T3 Portland | | | | 0 | 0 |
| 13145 | TR_MRLAZ | 24Tr AGORA | trolejbus | 24Tr AGORA | 25.11.2004 | 25.11.2004 | | 0 | 0 |
| 13146 | TR_ZLIN | 25Tr AGORA | trolejbus | 25Tr AGORA | 30.4.2005 | 30.4.2005 | | 0 | 0 |
| 13147 | TR_ZLIN | 24Tr AGORA | trolejbus | 24Tr AGORA | 4.11.2004 | 4.11.2004 | | 0 | 0 |
| 13148 | TR_ZLIN | 24Tr AGORA | trolejbus | 24Tr AGORA | 24.11.2004 | 24.11.2004 | | 0 | 0 |
| 13149 | TR_ZLIN | 24Tr AGORA | trolejbus | 24Tr AGORA | 4.11.2004 | 4.11.2004 | | 0 | 0 |
| 13150 | TR_ZLIN | 24Tr AGORA | trolejbus | 24Tr AGORA | 5.12.2004 | 5.12.2004 | | 0 | 0 |
| 13151 | TR_MRLAZ | 24Tr AGORA | trolejbus | 24Tr AGORA | 27.10.2005 | 27.10.2005 | | 0 | 0 |
| 13152 | TR_ZLIN | 24Tr AGORA | trolejbus | 24Tr AGORA | 20.12.2004 | 20.12.2004 | | 0 | 0 |
| 13153 | TR_PLZEN | 24Tr AGORA | trolejbus | 24Tr AGORA | 1.12.2004 | 1.12.2004 | | 0 | 0 |
| 13154 | TR_PLZEN | 24Tr AGORA | trolejbus | 24Tr AGORA | 15.7.2005 | 15.7.2005 | | 0 | 0 |
| 13155 | TR_PLZEN | 24Tr AGORA | trolejbus | 24Tr AGORA | 22.8.2005 | 22.8.2005 | | 0 | 0 |

Hlavním problémem databáze finálních výrobků je to, že data jsou uložena v různých částech, které systém Baan ERP neumí integrovat do jednoho souboru. To je možné pouze přes postupný export dat do souborů formátu xls a následnou integraci s pomocí identifikátoru, zajišťujícího

jednoznačnou vazbu na ostatní interní datové zdroje (např. na databázi záznamů o údržbě). Takovým identifikátorem je výrobní (sériové) číslo výrobku. Na této možnosti integrací aktuálně pracujeme. Problém by ovšem vyřešilo nasazení aplikačního software, který by zpracovával data z databáze finálních produktů a data z databáze záznamů o poruše a údržbě, jak bude uvedeno dále. Dalším problémem je úplnost dat – chybí jejich křížová kontrola, tzn. porovnání počtu záznamů v Objektech, počtu záznamů v IKV a počtu skutečně vyrobených a expedovaných výrobků.

## 3.2 Databáze záznamů o poruchách

Jediným zdrojem dat pro vytvoření databáze záznamů o poruchách a údržbě je „customizovaná“ aplikace „Hlášenka servisního zásahu (HSZ) v Baan ERP, modul Servis. Jak už bylo řečeno, žádná taková úloha ve standardním Baan ERP neexistuje. Aplikace vychází z prvotního vzoru papírového Záznamu o poruše, ze kterého byly převzaty číselníky i struktura dat, přičemž některé z nich byly přizpůsobené pravidlům používaným v Baan ERP a doplněné podle požadavků na data v systému RAMS.

V této aplikaci je možné vystavit HSZ přímo ve společnosti na základě dat získaných o poruše a údržbě, ale existuje také možnost načtení HSZ z textového souboru, zasílaného jednotlivými servisními místy do centra (e-mailem). Aplikace se skládá z jedné hlavní úlohy (vlastní hlášenky), podpůrných úloh (pro načítaní externího souboru s hlášenkou a pro vytvoření struktury uzlů výrobku) a úloh pro obsluhu příslušných číselníků včetně funkčně orientovaných dekompozic výrobků (funkčních rozpadů).

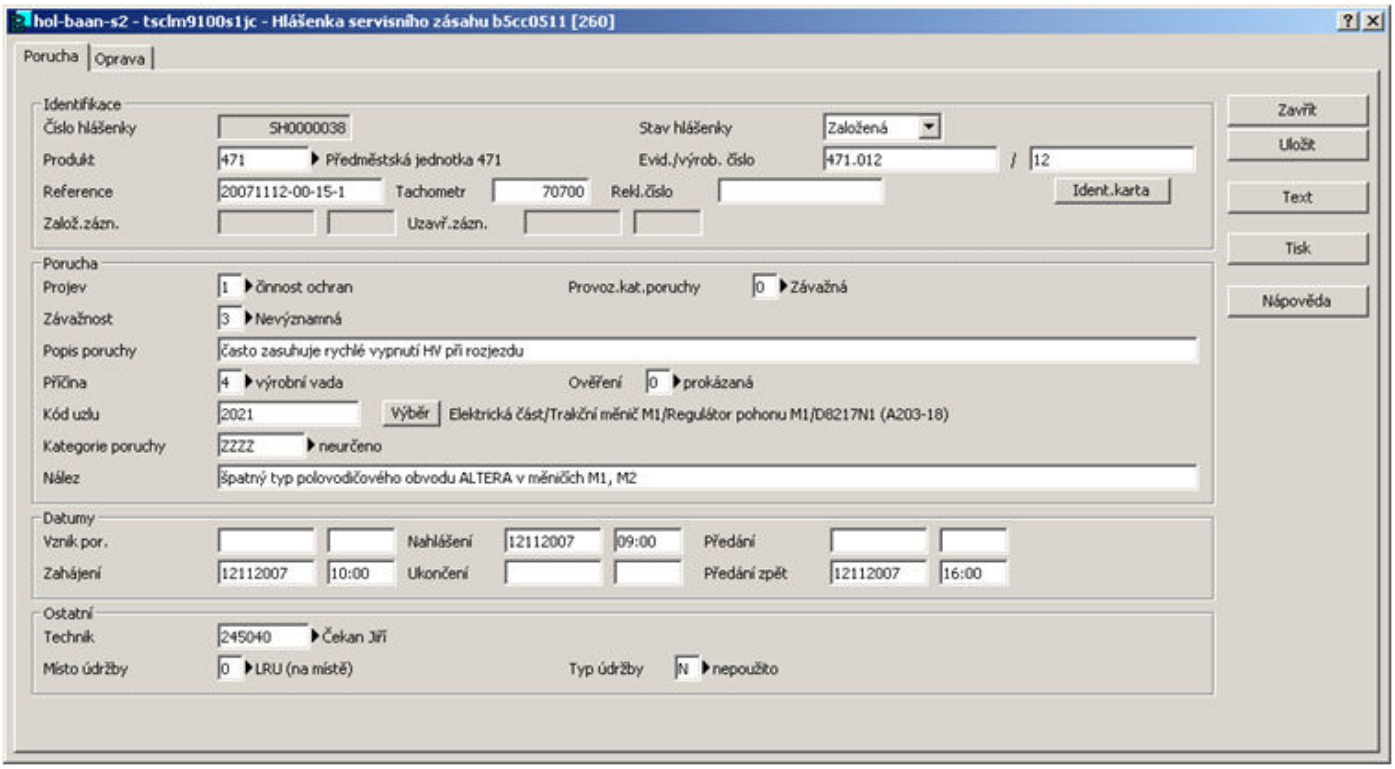
Na první záložce HSZ jsou popisné události, na druhé záložce jsou informace o způsobu provedení opravy (servisního zásahu). Většina polí je v tomto formuláři na první záložce povinná, některá pole na obou záložkách jsou navázaná na číselníky. Při zápisu kódu uzlu je možné jej zapsat rovnou nebo provést výběr z číselníku funkčního rozpadu.

Tlačítko „Identifikační karta“ v sekci „Identifikace“ umožňuje zobrazit přiřazenou IKV, spojenou přes výrobní číslo výrobku. Tlačítko „Text“ umožňuje zápis libovolného textu k Hlášence servisního zásahu.

Součástí HSZ je i informace o propojení na příslušnou Servisní objednávku Baan ERP, která umožňuje zobrazit přiřazenou Servisní objednávku a její položky (resp. její aktivity)[5] a příslušné podrobnosti.

[5] Servisní objednávky jsou základem pro sledování nákladů na servisní zásahy spojené s konkrétní poruchou a příslušnou HSZ.

Obrázek 4. Ukázka dat – databáze záznamů o poruše: Hlášenka servisního zásahu




Ukázku exportovaných dat z HSZ zde neuvádím, je příliš obsáhlá a bude součástí prezentace.

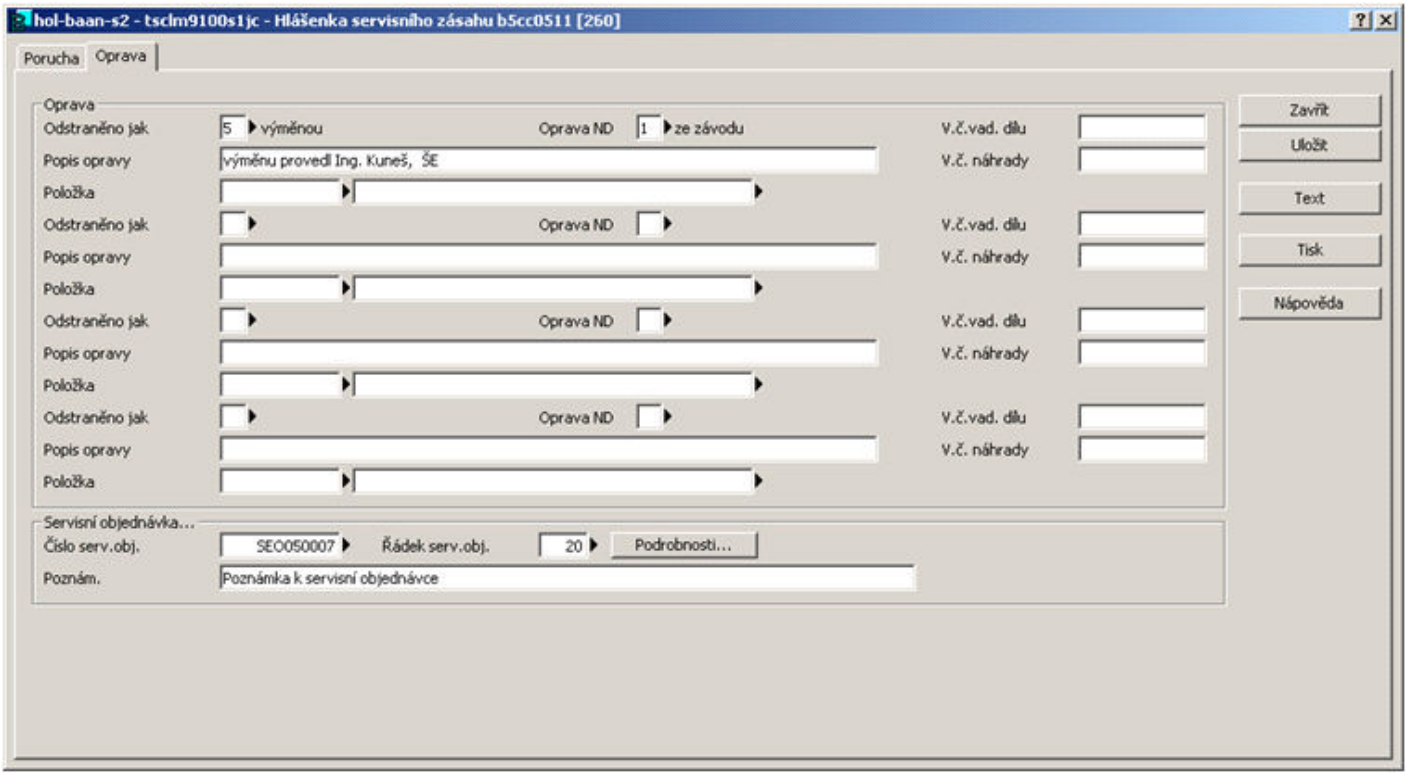
### 3.3 Databáze záznamů o údržbě po poruše (obnově)

Aktuálním problémem při naplňování této databáze je velké množství chybějících dat. Často se nedaří získat výrobní čísla vadných a nových dílů, zejména v případech, kdy servisní zásah nedělají pracovníci společnosti. I když z hlediska RAMS není nutné přesné přiřazení dílu k identifikačnímu číslu položky a k sériovému číslu položky (dílu), je to velmi významné pro management konfigurace. V této oblasti momentálně ve ŠKODA ELECTRIC a.s. zavádíme nová pravidla, umožňující lépe sledovat aktuální konfiguraci finálního výrobku a jeho subsystémů. I v nových pravidlech bude mít záznam výrobních čísel vadného a nového dílu nenahraditelný význam.

Data pro tvorbu databáze o údržbě[6] jsou také součástí HSZ – viz obrázek č. 5.

[6] Aktuálně pouze o údržbě po poruše, zatím se HSZ nevyužívají pro záznamy o preventivní údržbě

Obrázek 5. Ukázka dat – databáze záznamů o údržbě: Hlášenka servisního zásahu




## 3.4 Databáze záznamů o preventivní údržbě

Tato možnost zatím není využívána, i když to HSZ umožňuje. Pro výpočty hodnot pohotovosti finálních výrobků (trolejbusů) proto využíváme pouze data o prostojích vlivem poruchy (MTTR), nikoliv data o prostojích vlivem preventivní údržby.

## 3.5 Databáze nákladů

Ke sledování nákladů na servisní zásahy je v Baan Servis standardní úloha, tzv. Servisní objednávky. Ty umožňují zaznamenávat a sledovat jak činnosti spojené se servisním zásahem, včetně např. nákladů na dopravu (cestovní náklady), tak materiál potřebný pro obnovu vydaný z garančního skladu atd. Ideální by byl stav, kdyby se ke každé HSZ vystavila servisní objednávka, jenže často vyjíždí servisní technik k zásahu do nějaké lokality a tam pracuje na několika výrobcích, resp. odstraňuje poruchy uvedené v několika HSZ, takže zásadu „jedna HSZ = jedna Servisní objednávka“ není možné vždy dodržet.

Dalším problémem při sledování nákladů na servisní činnosti jsou případy, kdy kvůli rychlosti obnovy je vyměněn celý vyměnitelný blok, který byl zdrojem poruchy. Přes Servisní objednávku se do nákladů započte celá hodnota vyměněného bloku. Ten je ale dodatečně podroben kontrole, často je příčinou provozní poruchy selhání jednoho komponentu z bloku. Po opravě bloku (která je výrazně levnější) je blok znovu přijat na garanční sklad jako použitelný. To ale často s odstupem týdnů, někdy měsíců, proto se velmi obtížně sledují skutečné náklady na servisní zásah.

## 3.6 Práce s datovou základnou

Aby byla data v datové základně co nejúplnější a nejsprávnější, musí být nutně jasně definované odpovědnosti za jednotlivé činnosti. Rozdělení povinností a odpovědností není zatím zcela jasně definováno, původně měla na přelomu let 2010 a 2011 vzniknout interní směrnice „Datová základna RAMS/LCC“, která by popisovala všechny činnosti a stanovila odpovědnosti při tvorbě, správě a využití datové základny spolehlivosti. Její součástí měl být podrobný Manuál k datové základně v Baan Servis. Bohužel se z různých důvodů nepodařilo tuto směrnici dokončit a vydat, je proto připravováno její vydání na 1. polovinu roku 2012, přestože stále přetrvávají spory mezi odbornými útvary o rozdělení odpovědností, zejména při naplňování databáze finálních výrobků.

V databázi záznamů o poruchách je situace mnohem lepší, i když jsou znatelné rozdíly mezi oběma divizemi (každá má své vlastní oddělené databáze v Baan Servis). Hlavní odpovědnost za záznamy o poruchách a údržbě leží na pracovnících úseků Poprodejní služby, pod které spadají i technici vykonávající servisní zásahy.

Nejméně problémů je v záznamech o poruchách trolejbusů, protože ŠKODA ELECTRIC a.s. je finálním dodavatelem trolejbusů přímým uživatelům a v drtivé většině případů zajišťuje servisní služby vlastními zaměstnanci. Mnohem více problému je se záznamy o poruchách elektrických výzbrojí, dodávaných jiným výrobcům finálních vozidel, nejvíce problémů je se záznamy o poruchách trakčních motorů.

Problémem, který stojí za zmínku, je také průběžná aktualizace záznamů o poruchách uvedených v HSZ. Jak už bylo řečeno, při servisním zásahu je často vyměňován celý blok, který byl zdrojem poruchy. Proto servisní technik vybere v HSZ v poli Kód uzlu příslušnou úroveň funkčního rozpadu výrobku[7]. S odstupem času po provedené analýze a zjištění konkrétního porouchaného dílu by měl být údaj v HSZ konkretizován podle skutečnosti, ale v mnoha případech se to právě pro delší časový odstup neděje. Tím je omezována možnost podrobnějších analýz příčin poruch a stanovení cílenějších opatření k jejich eliminaci.

## 3.7 Stav datové základny

V následujících tabulce je přehled počtu záznamů v databázi finálních výrobků a v databázi záznamů o poruše a údržbě. Z tabulky je patrné, že databáze finálních produktů není úplná, věrohodnější je údaj o počtu vystavených IKV, i když ani u nich není jistota, že jsou založeny pro všechny výrobky společnosti. Kontrola úplnosti záznamů začala probíhat v divizi Trakční motory, divize Pohony a trolejbusy bude následovat.

Součástí záznamů o poruchách v divizi Pohony a Trolejbusy jsou i záznamy (HSZ), které vznikly automatizovaně převodem dat z dřívější databáze vedené v systému INCAD do konce roku 2008, tj. do plné funkčnosti HSZ v Baan ERP. S těmito záznamy zatím nepracujeme, některá data nejsou plně kompatibilní s daty v HSZ, takže tyto záznamy tvoří jakýsi „datový sklad“. Je zpracován převodní klíč mezi některými číselníkovými daty INCAD a HSZ, problém je v tom, že změny dat nelze provést automatizovaně, ale musí se postupně dělat ručně.

[7] Funkčně orientovaná dekompozice výrobku má stromovou strukturu a je provedena do 4. až 5. úrovně

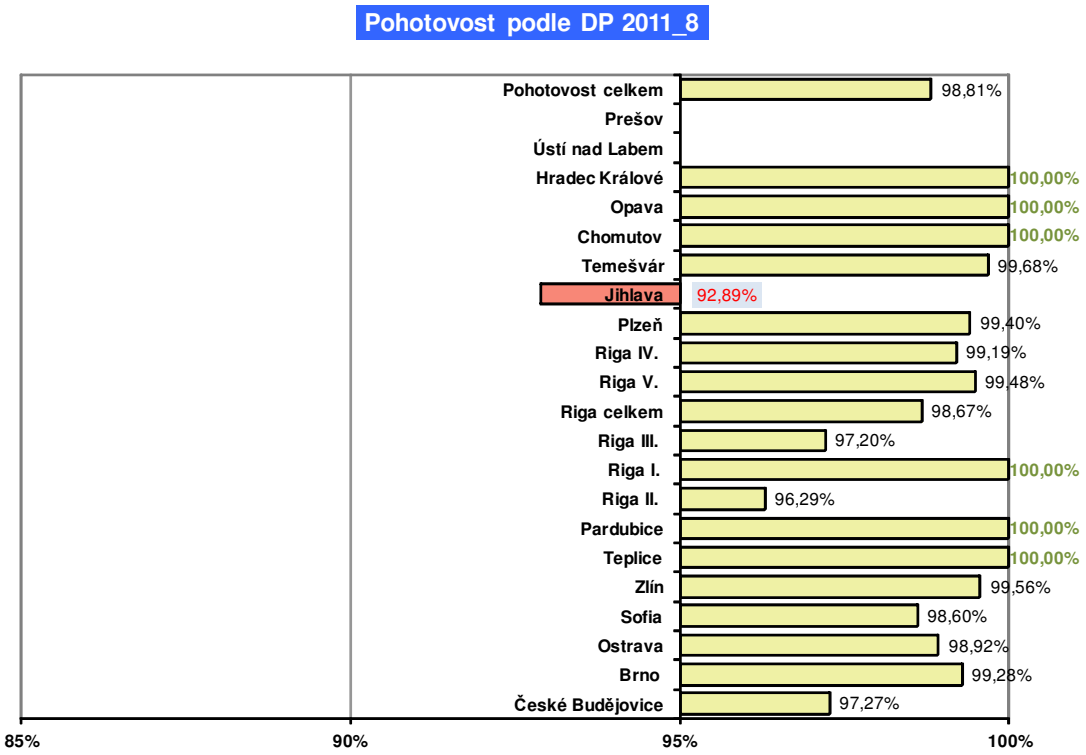
Tabulka 3. Celkový přehled záznamů

| | Divize Trakční motory | Divize Pohony a Trolejbusy |
|---|---|---|
| Počet založených Objektů v databázi finálních výrobků | 4 955 | 358 |
| Počet založených Identifikačních karet výrobků v databázi finálních výrobků | 6 979 | 1 155 |
| ROZDÍL (Objekty-IKV) | -2 024 | -797 |
| Počet založených HSZ v databázi záznamů o poruše a údržbě celkem | 7 350 | 10 301 |

# 4. Využívání výstupů z datové základny

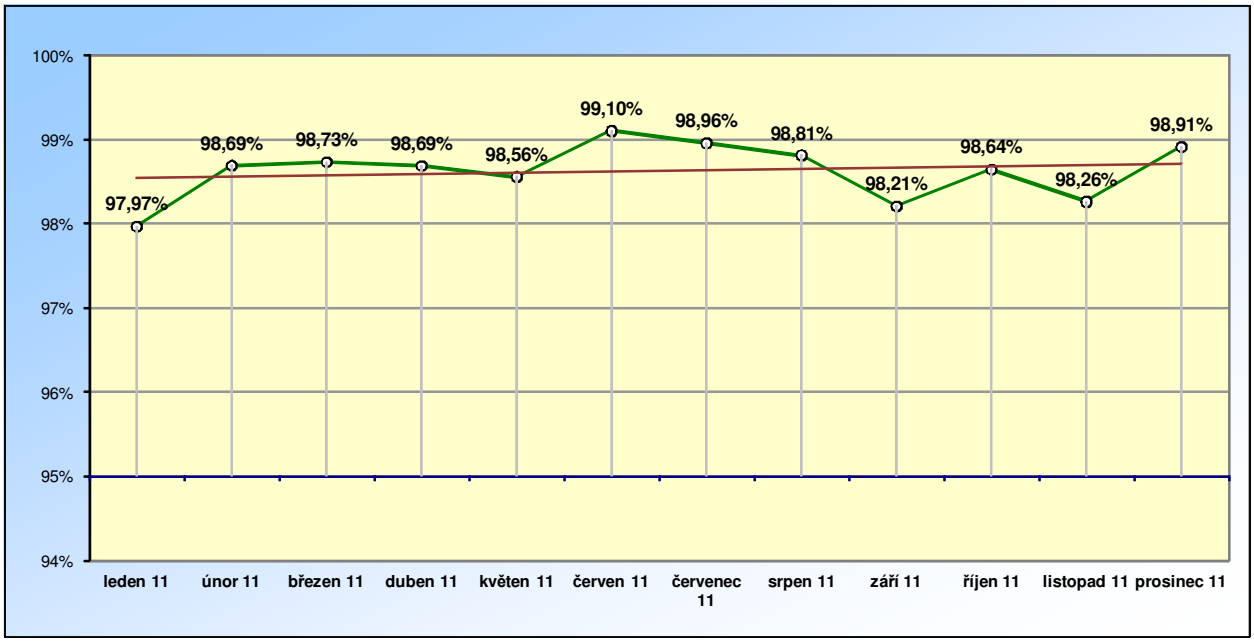
Aby datová základna nebyla jen samoúčelně shromažďovanými údaji bez dalšího využití, musí poskytovat různým útvarů a osobám požadované výstupy. Ty jsou zpracovávané zatím v omezeném množství, hlavně s ohledem na pracnost zpracování některých z nich, zejména jde-li o parametry bezporuchovosti, k jejichž výpočtům jsou potřebná data z databáze finálních produktů a provozní data finálních produktů (kilometrické proběhy atd.). Následující obrázky a tabulky jsou ukázkou některých výstupů (reportů) z databáze spolehlivosti. Některé údaje o poruchách (četnosti poruch, MDBF apod.) jsou citlivá a nejsou veřejná, proto jsou pro prezentaci upravená, tedy neodpovídají skutečnosti.

Obrázek 6. Pohotovost trolejbusů podle lokace (dopravního podniku)

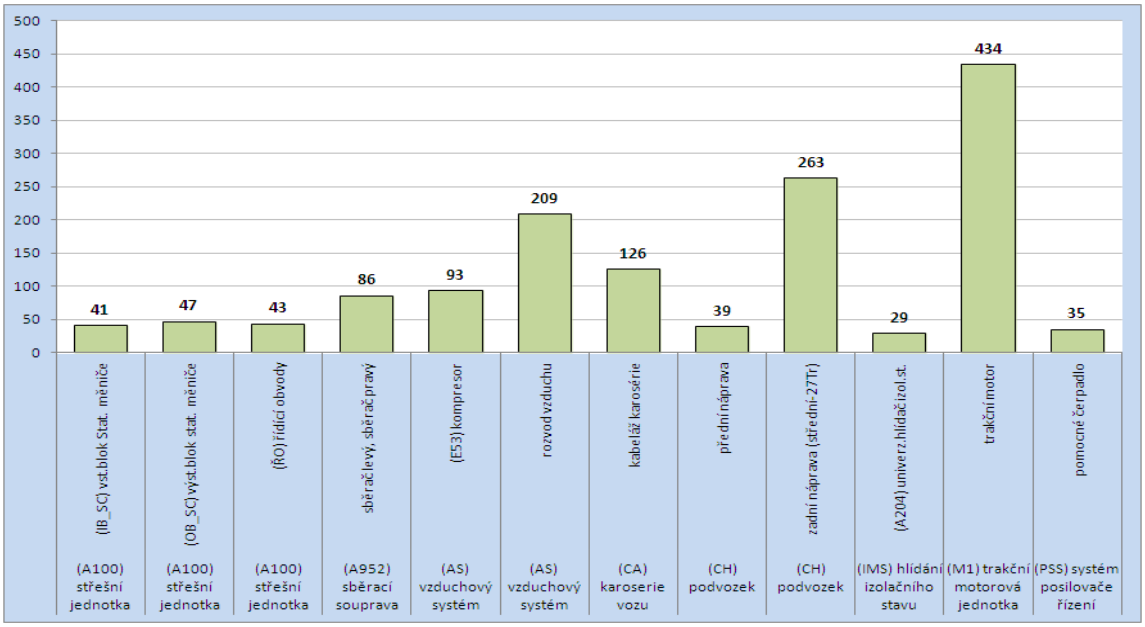



V případě, že pohotovost klesne pod 95%, jsou analyzovány příčiny prostojů.

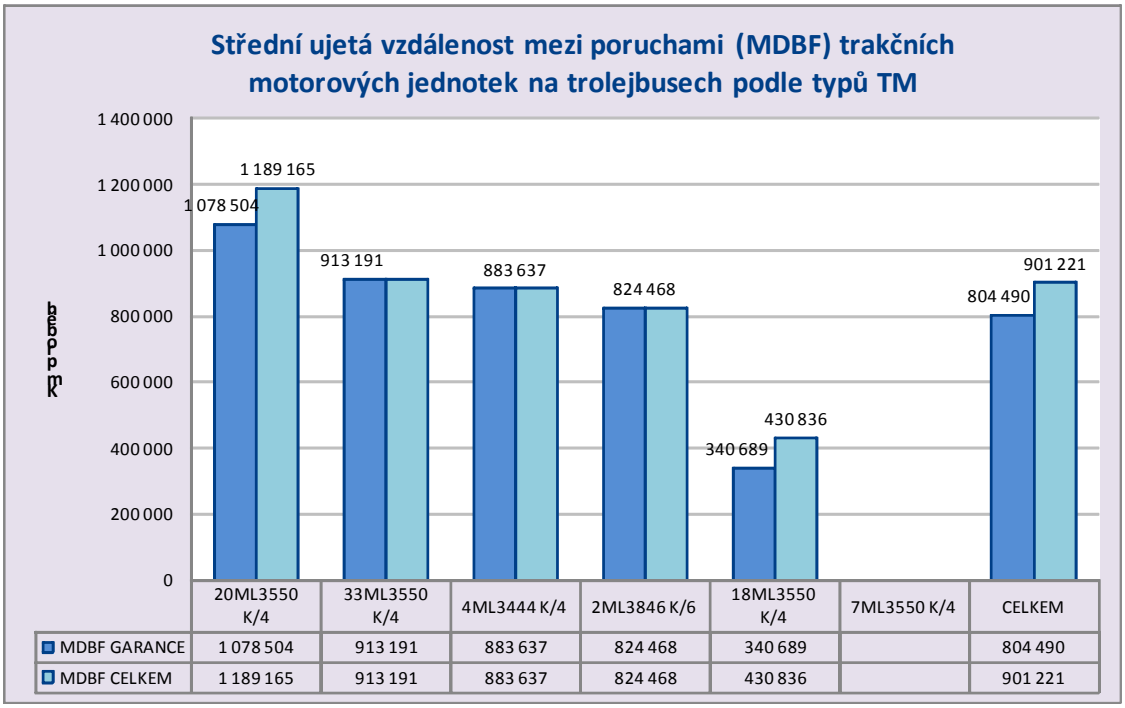
Obrázek 7. Vývoj pohotovosti trolejbusů - 2011



Obrázek 8. Součet prostojů trolejbusů v roce 2011 podle poruch uzlů vozidla (dny); *zobrazené hodnoty jsou fiktivní, slouží jen pro názornost*




Obrázek 9. Ukázka výpočtu střední ujeté vzdálenosti mezi poruchami trakčních motorových jednotek v trolejbusech; *zobrazené hodnoty jsou fiktivní, slouží jen pro názornost*



# 5. Shrnutí přínosů, úskalí a problémů

## 5.1 Přínosy

- Máme vytvořenou rozsáhlou datovou základnu k využití, za předpokladu doplnění potřebných dat a jejích aktualizace.
- Máme úplná a věrohodná data o provozu, poruchách a údržbě po poruše trolejbusů v záruční době, která začínají být využívána pro výpočty parametrů spolehlivosti – standardně pro výpočty pohotovosti, což je parametr nejvíce sledovaný a požadovaný provozovateli trolejbusů a bývá stále častěji zahrnut do tendrových podmínek.
- Sledujeme dlouhodobě vývoj pohotovosti, ale i střední ujeté vzdálenosti mezi poruchami trolejbusů, s možností určit komponenty, které nejvýznamněji ovlivňují tyto parametry.
- Máme k dispozici data pro vyhodnocování a sledování vývoje středních dob/vzdáleností mezi poruchami komponentů trolejbusů včetně nakupovaných dílů.

## 5.2 Úskalí a problémy

- Nepochopení účelu datové základny RAMS – objevují se požadavky, které jdou nad rámec účelu datové základny, např. požadavky na:
  - sledování poruchovosti konkrétních komponentů podle identifikačních a výrobních čísel,
  - vyhodnocování dopadů změn dílů na dosahované parametry RAMS,
  - provádění analytické práce přímo v datové základně a tedy na „zpodrobnění“ údajů v databázi až na úroveň nejnižších komponentů, např. polovodičových prvků apod.
- V databázi chybí zatím data o preventivní údržbě, která společně s daty o údržbě po poruše lze využívat pro optimalizaci udržovatelnost výrobku a optimalizaci zajištěnosti údržby výrobku.
- Máme velké objemy dat v různých aplikacích, ale nemáme žádnou nadstavbu pro jejich efektivní zpracování do požadovaných výstupů. Aktuální představa ve skupině ŠKODA TRANSPORTATION (kterou nesdílím) je, že nad jednotným datovým úložištěm společným pro všechny společnosti skupiny bude vytvořena nadstavba v prostředí MS Excel, která potřebné výstupy zajistí. Od prvního návrhu na toto řešení uplynul již rok a nijak se v řešení nepokročilo.
- Špatná dostupnost a nižší věrohodnost dat o provozu, poruchách a údržbě částí elektrických výzbrojí vozidel dodávaných ze ŠKODA ELECTRIC a.s. výrobcům finálních vozidel. V rámci skupiny dochází ke zlepšení, byla vypracována jednotná pravidla pro uzavírání smluv mezi společnostmi skupiny, jejich součástí jsou i povinná ujednání o poskytování potřebných provozních dat.
- Téměř nedostupná jsou provozní data v období pozáručního provozu, která by pro výrobce byla velmi významná s ohledem na poměr délky záručního a pozáručního provozu v celkové délce technického života výrobku. Zatím se nedaří zapracovávat do smluv ujednání o poskytování takových dat uživatelem výrobci. Překážkou je mj. i to, že data by uživatel poskytoval pravděpodobně jen za úplatu, což by při kalkulacích mělo dopad do výnosu výrobce. Určité zlepšení může přinést přechod k tzv. full-servisu, kdy výrobce zajišťuje dodavateli servisní služby po celou dobu provozu (technického života) výrobku.

- V databázi chybí zatím data o preventivní údržbě, která společně s daty o údržbě po poruše lze využívat pro optimalizaci udržovatelnost výrobku a optimalizaci zajištěnosti údržby výrobku.
- Nízká úroveň zpětné vazby z provozu pro modifikaci a regeneraci výrobku a zavádění opatření ke zlepšení ´“slabých míst“ výrobku z hlediska spolehlivosti, bezpečnosti nebo nákladů životního cyklu.
- Zatím nedostatečná spolupráce s významnými dodavateli. Setkáváme se s tím, že nám dodavatel poskytne požadované hodnoty bezporuchovosti (predikované), ale žádá od nás pravidelné vyhodnocování skutečně dosahovaných hodnot v provozu, aby je mohli porovnávat s predikcemi. To jsme momentálně připraveni provádět u komponentů nebo subsystémů trolejbusů, podstatně horší máme pozici u výrobků dodávaných jiným výrobcům vozidel.
- Není definována povinnost a odpovědnost za správu datové základny a za její průběžnou kontrolu, aktualizaci dat a ukončování HSZ.
- Funkčně orientované rozpady výrobků neobsahují údaje o počtu identických komponentů ve výrobku, což je údaj nezbytný pro hodnocení bezporuchovosti komponentů.
- Zatím nedokážeme dostatečně sledovat skutečné náklady životního cyklu, resp. té části LCC, která souvisí s RAM.
- V databázi zatím chybí data z diagnostických zařízení výrobků, která by mohla významně přispět k odhalování skutečných příčin (Root Cases) provozních poruch a k přijímání cílenějších opatření.

# 6. Závěr

V příspěvku jsem se pokusil poskytnout aktuální informace o stavu datové základny RAMS ve ŠKODA ELECTRIC a.s., hlavně o jejím vývoji od posledních prezentací v odborné skupině pro spolehlivost České společnosti pro jakost, ale také upozornit na úskalí a problémy při její tvorbě a správě. Mimo jiné také s vírou, že v odborné diskusi můžeme najít náměty na odstranění našich problémů a získat zkušenosti z jiných společností nebo institucí, které se oblastí RAMS/LCC také zabývají.

ŠKODA ELECTRIC a.s.

# Management spolehlivosti ve výrobě pohonů trakčních vozidel

Ing. Jan Kraus, ŠKODA ELECTRIC a.s.
tel. +420 378 181 229, e-mail: jan.kraus@skoda.cz

## 1. Úvod

Spolehlivost výrobků určených pro drážní aplikace představuje aspekt kvality, jehož význam neustále roste. Pro úspěšné splnění požadavků na spolehlivost výrobků je nutné zavést a důsledně uplatňovat management spolehlivosti. To platí pro dodavatele všech částí drážních zařízení a také pro dodavatele subsystémů finálních výrobků. Cílem tohoto příspěvku je nástin realizace managementu spolehlivosti ve společnosti ŠKODA ELECTRIC, a.s. doplněný o příklady problémů procesu řízení spolehlivosti pohonů trakčních vozidel.

## 2. Management spolehlivosti drážních zařízení

Základní normou pro management spolehlivosti drážních zařízení je ČSN EN 50126-1. Tuto normu lze použít v průběhu celého životního cyklu drážního zařízení[8] pro vytvoření požadavků na bezporuchovost (R), pohotovost (A), udržovatelnost (M) a bezpečnost (S) a pro dosažení shody s těmito požadavky. Skutečnost, že norma ČSN EN 50126-1 pokrývá všechna zařízení drážního systému, usnadňuje hodnocení vzájemného působení mezi jednotlivými prvky drážního systému z hlediska požadavků RAMS. Zároveň však široký záběr normy ztěžuje její aplikaci na subsystémy drážních zařízení.

Návod na použití normy EN 50126-1 pro oblast kolejových vozidel poskytuje technická zpráva CLC/TR 50126-3. Zpráva rozděluje 14 etap životního cyklu kolejového vozidla do tří fází a pro jednotlivé fáze popisuje hlavní aktivity a také dokumenty, jež mají být vypracovány. Rozdělení etap životního cyklu do fází je patrné z tabulky 1. Je zřejmé, že s řízením spolehlivosti výrobku je nezbytné začít již ve fázi probíhajícího výběrového řízení. Pro výrobce jednotlivých subsystémů kolejových vozidel tato skutečnost přináší některé komplikace, které budou zmíněny v další části příspěvku.

Dalším důležitým faktorem managementu spolehlivosti kolejových vozidel je rozdělení (sdílení) odpovědností. V průběhu životního cyklu kolejového vozidla zasahuje do procesu řízení spolehlivosti více účastníků a proto je třeba jednoznačně vymezit odpovědnost jednotlivých subjektů. Kromě výrobce (dodavatele) kolejového vozidla a výrobce příslušného subsystému kolejového vozidla vystupují ve smluvních vztazích také provozovatel vozidla, vlastník vozidla a subjekt zajišťující údržbu vozidla. V některých případech vykonává jeden subjekt více rolí (např. dodavatel vozidla zároveň zajišťuje údržbu, provozovatel vozidla je současně jeho vlastníkem apod.). Ve smluvních vztazích vystupují jednotlivé subjekty buď v pozici dodavatele nebo v pozici zákazníka, přičemž jeden subjekt může být zároveň dodavatelem i zákazníkem (výrobce

[8] ČSN EN 50126-1 definuje životní cyklus systému jako „činnosti probíhající v časovém intervalu od vymyšlení systému do okamžiku, kdy už systém není použitelný, je vyřazen z provozu a zlikvidován“.
Norma ČSN EN 60300-3-3 používá poněkud odlišnou definici, podle níž je životní cyklu „časový interval od stanovení koncepce produktu po jeho vypořádání (likvidaci)“.

vozidla je vůči dodavateli subsystému zákazníkem a zároveň je ve vztahu s provozovatelem vozidla v pozici dodavatele).

Tabulka 1: Fáze životního cyklu dle CLC/TR 50126-3

| Fáze | Číslo a označení etapy |
|---|---|
| Tendr | 1 Koncepce<br>2 Definice systému a podmínky použití<br>3 Analýza rizika<br>4 Požadavky na systém<br>5 Rozdělení požadavků na systém |
| Návrh | 6 Návrh a zavedení<br>7 Výroba<br>8 Instalace<br>9 Validace systému<br>10 Přejímka systému |
| Provoz | 11 Provoz a údržba<br>12 Sledování výkonnosti<br>13 Modifikace a regenerace<br>14 Vyřazení z provozu a likvidace |

# 3. Řízení spolehlivosti ve ŠKODA ELECTRIC, a.s.

Ve společnosti ŠKODA ELECTRIC, a.s. (Š-ELC) jsou požadavky na stanovení a prokázání RAMS dle normy ČSN EN 50126-1 implementovány do integrovaného systému managementu. Základními řídicími dokumenty pro oblast RAMS v Š-ELC jsou *Směrnice SM-ŘJ-17 Management RAMS* a *Směrnice SM-ŘJ-19 Standardní program RAMS*. První z uvedených směrnic popisuje požadavky na systém managementu RAMS a jeho uplatňování v Š-ELC, druhá směrnice poskytuje návod na vypracování Programu RAMS pro konkrétní projekt nebo produkt. Management RAMS úzce souvisí s celou řadou zavedených procesů systému kvality. Souvislost mezi etapami životního cyklu, procesy systému kvality a příslušnými procesními dokumenty je zachycena v tabulce 2.

Podle *Směrnice SM-ŘJ-19 Standardní program RAMS* je v Š-ELC program RAMS vytvářen vždy, když je to vyžadováno zákazníkem, a také u všech projektů spadajících pod normu IRIS[9]. U ostatních projektů rozhoduje o vytvoření programu RAMS vedení příslušné divize Š-ELC. Program RAMS konkrétního projektu vzniká přizpůsobením Standardního programu RAMS, který je navržen pro typické projekty realizované ve společnosti Š-ELC a představuje univerzální a široce pojatý program pro stanovení a prokázání požadavků na RAMS. Pro každou etapu životního cyklu jsou stanoveny cíle, z nichž vyplývají příslušné požadavky na činnosti. Jednotlivé činnosti jsou realizovány formou úkolů. Kromě úkolů spojených s každou etapou jsou

[9] Norma IRIS (International Railway Industry Standard) vytvořená Evropskou asociací železničního průmyslu (UNIFE) vychází z ustanovení normy ISO 9001 a specifikuje požadavky na systém managementu kvality pro oblast železničního průmyslu.

v programu RAMS stanoveny odpovědnosti za realizaci úkolů a termíny realizace. Nedílnou součástí každé etapy je též proces ověřování (verifikace), při němž je potvrzováno, že byly splněny specifikované požadavky. Výsledky každé etapy jsou dokumentovány a v průběhu všech fází životního cyklu tak vzniká celá řada dokumentů. Jejich přehled je v tabulce 3.

Tabulka 2: Souvislost etap životního cyklu a procesů systému kvality

| **Etapa životního cyklu** | **Procesy systému kvality** | **Procesní dokumenty** |
|---|---|---|
| Etapa 1: Koncepce | P 702.1 Řízení tendru<br>P 702 Přezkoumání smlouvy | SM-OÚ-01 Přezkoumání smlouvy<br>PP-ŘJ-04 RAMS etapa 1 - Koncepce |
| Etapa 2: Definice systému a podmínky použití | P 702 Přezkoumání smlouvy<br>P 704 Řízení návrhu | SM-OÚ-01 Přezkoumání smlouvy<br>SM-TÚ-01 Řízení návrhu<br>PP-ŘJ-05 RAMS etapa 2 - Definice produktu/systému a podmínky použití |
| Etapa 3: Analýza rizika | P 702 Přezkoumání smlouvy<br>P 704 Řízení návrhu | SM-OÚ-01 Přezkoumání smlouvy<br>SM-TÚ-01 Řízení návrhu<br>PP-ŘJ-06 RAMS etapa 3 - Analýza rizika |
| Etapa 4: Požadavky na systém | P 702 Přezkoumání smlouvy<br>P 704 Řízení návrhu | SM-OÚ-01 Přezkoumání smlouvy<br>SM-TÚ-01 Řízení návrhu<br>PP-ŘJ-07 RAMS etapa 4 - Požadavky na systém |
| Etapa 5: Rozdělení požadavků na systém | P 704 Řízení návrhu | SM-TÚ-01 Řízení návrhu<br>PP-ŘJ-08 RAMS etapa 5 - Rozdělení požadavků na systém |
| Etapa 6: Návrh a zavedení | P 704 Řízení návrhu<br>P 706 Nakupování a skladování | SM-TÚ-01 Řízení návrhu<br>SM-N-01 Nákup a sklady<br>SM-ŘJ-09 Změnové řízení<br>PP-ŘJ-09 RAMS etapa 6 - Návrh a zavedení |
| Etapa 7: Výroba<br>Etapa 8: Instalace | P 709 Výroba<br>P 801 - 804 Kontroly a zkoušky<br>P 703 Řízení projektu | SM-VÚ-01 Plánování a řízení výroby<br>SM-TK-01 Kontrola a zkoušení<br>SM-ŘP-01 Řízení projektů<br>SM-ŘJ-09 Změnové řízení<br>PP-ŘJ-10 RAMS etapa 7 a 8 - Výroba a instalace |
| Etapa 9: Validace systému<br>Etapa 10: Přejímka systému | P 704 Řízení návrhu<br>P 801 - 804 Kontroly a zkoušky<br>P 712 Uvedení do provozu | SM-TÚ-01 Řízení návrhu<br>SM-TK-01 Kontrola a zkoušení<br>SM-PS-01 Poprodejní služby<br>SM-ŘJ-09 Změnové řízení<br>PP-ŘJ-11 RAMS etapa 9 a 10 - Validace a přejímka systému |
| Etapa 11: Provoz a údržba<br>Etapa 12: Sledování výkonnosti | P 712.1 Poprodejní služby | SM-PS-01 Poprodejní služby<br>SM-ŘJ-09 Změnové řízení<br>PP-ŘJ-12 RAMS etapa 11 a 12 - Provoz, údržba a sledování výkonnosti |
| Etapa 13: Modifikace a regenerace | P 715 Řízení změn | SM-ŘJ-09 Změnové řízení |

| | | |
|---|---|---|
| Etapa 14: Vyřazení z provozu a likvidace | P 717 Management konfigurace<br>P 718 Managament zastaralých položek<br>P 704 Řízení návrhu | SM-TÚ- Identifikace a sledovatelnost<br>SM-TÚ-01 Řízení návrhu<br>PP-ŘJ-12 RAMS etapa 11 a 12 - Provoz, údržba a sledování výkonnosti<br>Managament zastaralých položek |

Tabulka 3: Výstupy realizace úkolů RAMS

| **Etapa životního cyklu** | **Výstupy etapy** |
|---|---|
| Etapa 1: Koncepce | Studie proveditelnosti projektu z hlediska RAMS,<br>Rámcový program RAMS projektu. |
| Etapa 2: Definice systému a podmínky použití | Technická zpráva shrnující výsledky předběžné analýzy nebezpečí a definující kritéria přípustnosti rizika,<br>Rámcový plán RAMS projektu doplněný o úkoly plánu bezpečnosti,<br>Koncepce RAMS,<br>Specifikace podmínek dlouhodobého provozu a údržby. |
| Etapa 3: Analýza rizika | Analýza rizika. |
| Etapa 4: Požadavky na systém | Stanovení funkčních požadavků na bezpečnost a na integritu bezpečnosti (SIL),<br>Souhrnná specifikace RAMS,<br>Souhrnná specifikace kritérií RAMS pro přejímku,<br>Plán validace / přejímky RAMS,<br>Management validace RAMS,<br>Podrobný program RAMS s aktualizovanými úkoly bezpečnosti. |
| Etapa 5: Rozdělení požadavků na systém | Specifikace RAMS pro subsystémy,<br>Specifikace kritérií RAMS pro přejímku subsystémů,<br>Revidovaný program RAMS s aktualizovanými úkoly bezpečnosti. |
| Etapa 6: Návrh a zavedení | Technická zpráva o výsledcích analýzy bezporuchovosti,<br>Technická zpráva o výsledcích analýzy pohotovosti,<br>Technická zpráva o výsledcích analýzy udržovatelnosti,<br>Technická zpráva o výsledcích analýzy bezpečnosti,<br>Model nákladů životního cyklu systému,<br>Návrh koncepce údržby systému,<br>Soupis požadavků na logistickou podporu vyplývající z RAMS,<br>Aktualizovaný program RAMS projektu. |
| Etapa 7: Výroba | Technická zpráva o výsledcích zkoušek pro ověření namáhání vlivy okolního prostředí,<br>Technická zpráva o výsledcích zkoušek růstu bezporuchovosti,<br>Záznamy o výsledcích třídění namáháním pro zlepšení bezporuchovosti,<br>Aktualizované analýzy bezpečnosti a záznamy o nebezpečí,<br>Funkční systém hlášení poruch a opatření k nápravě (FRACAS). |
| Etapa 8: Instalace | Program instalace systému (případně manuál pro instalaci),<br>Výcvik pracovníků pro kvalifikovanou údržbu systému (případně manuál pro údržbu systému),<br>Přehled doporučených náhradních dílů s postupem jejich obstarávání. |

| | |
|---|---|
| Etapa 9: Validace systému | Záznam o provedené validaci systému ověřený zákazníkem,<br>Program uvedení systému do provozu (případně manuál pro obsluhu a uvádění do provozu). |
| Etapa 10: Přejímka systému | Záznamy o výsledcích provedených zkoušek (pokud jsou realizovány),<br>Záznam o provedení přejímky systému v oblasti RAMS odsouhlasený zákazníkem. |

Tabulka 3: Výstupy realizace úkolů RAMS - pokračování

| | |
|---|---|
| Etapa 11: Provoz a údržba | Aktualizovaná koncepce údržby a provozní postupy,<br>Aktualizované záznamy o nebezpečí,<br>Údaje ze systému FRACAS,<br>Záznamy o realizovaných úkolech RAMS a zavedených opatřeních v rámci FRACAS. |
| Etapa 12: Sledování výkonnosti | Funkční systém sběru dat o RAMS v provozu,<br>Výsledky průběžného vyhodnocování statistických dat týkajících se RAMS,<br>Záznamy o provozu a údržbě výrobku,<br>Aktualizovaná dokumentace postupů pro provoz, údržbu a výcvik,<br>Výsledky vyhodnocování záznamů o provozu, poruchách a údržbě výrobku. |
| Etapa 13: Modifikace a regenerace | Příprava procesu modifikace výrobku,<br>Technická zpráva shrnující důsledky modifikace nebo regenerace na RAMS systému. |
| Etapa 14: Vyřazení z provozu a likvidace | Příprava procesu pro vyřazení a likvidaci výrobku,<br>Plán bezpečnosti pro vyřazení a likvidaci systému,<br>Soupis informací o stupni opotřebení, stárnutí a poškození jednotlivých subsystémů (prvků),<br>Analýza výkonnosti životního cyklu výrobku. |

# 4. Specifické problémy managementu spolehlivosti trakčních pohonů

V oblasti řízení spolehlivosti se výrobce trakčních pohonů kolejových vozidel setkává s řadou specifických problémů, které se opakovaně vyskytují v různých projektech. Následující přehled shrnuje typické problémy v jednotlivých fázích životního cyklu, resp. projektu.

### *Fáze tendru*

**Nedůslednost a „lidová tvořivost“ v terminologii použité v tendrové dokumentaci**

Tendrová dokumentace je většinou tvořena celou řadou dokumentů a ne vždy je použitá terminologie důsledně dodržována ve všech dokumentech. Stává se, že některé pojmy nejsou definovány vůbec nebo jsou definice nesrozumitelné. Situaci ještě zhoršuje nízká jazyková úroveň tendrové dokumentace nebo jejích překladů.

Lidová tvořivost se projevuje v používání vlastních výrazů a zkratek pro veličiny, které jsou včetně doporučených zkratek definovány v normách. I zde platí, že některé použité výrazy postrádají definici. Fantazii autorů je možné ilustrovat na pojmu *střední ujetá vzdálenost mezi poruchami (MDBF)*. V dokumentech výběrových řízení se lze bez bližšího vysvětlení setkat například s následujícími variantami:

MKTF – Mean Kilometer to Failures[10],

AKBD – Average Kilometer Between Defects.

**Nekonzistentní údaje v zadávací dokumentaci**

V některých případech je tentýž údaj uváděn ve více dokumentech, ale hodnoty v jednotlivých dokumentech se navzájem liší. Další variantou nekonzistence vstupních údajů je situace, kdy se v různých dokumentech tendrové dokumentace objevují údaje, které lze vzájemně přepočítávat, ovšem výsledkem přepočtu není v souladu s údaji uvedenými v ostatních dokumentech. Příkladem mohou být data pro analýzu nákladů životního cyklu, kdy nesouhlasí údaje o ročním projezdu s údaji o projezdu za kratší časový úsek. (V dokumentaci byl stanoven roční projezd 120 000 km a zároveň denní projezd 300 km. Jednoduchým výpočtem z uvedených údajů plyne, že by kolejové vozidlo muselo být v provozu 400 dnů v roce, což je zjevný nesmysl.) V jiném tendru se objevil údaj o tom, že kolejové vozidlo bude provozováno každý měsíc v průměru 30,4 dne a zároveň bude vozidlo odstaveno na 2 dny v měsíci za účelem preventivní údržby. Opět lze jednoduše vypočítat, že by v takovém případě musel mít kalendářní rok cca 389 dnů. Naštěstí jsou i projekty, v jejichž zadávací dokumentaci jsou údaje kompletní a konzistentní. Ukázka takové dokumentace je v příloze 1.

**Nespecifikovaný či nejasný způsob vyhodnocování parametrů spolehlivosti**

Požadavky na spolehlivost a bezpečnost kolejového vozidla a jeho subsystémů se objevují v každém tendru, ale velmi často není stanoveno, jakým způsobem budou vybrané parametry spolehlivosti[11] sledovány a vyhodnocovány. V tendrové dokumentaci chybí ustanovení o sběru, předávání a zpracování dat o provozu a poruchách zařízení. Tyto nedostatky se plně projevují až ve fázi provozu a mohou vést až k vážným sporům mezi provozovatelem, výrobcem kolejového vozidla a výrobcem příslušného subsystému vozidla, zejména v případech, kdy je neplnění spolehlivostních parametrů sankcionováno. Častým problémem je nepochopení základních pojmů z teorie spolehlivosti a používaných matematických nástrojů a jejich chybná aplikace při vyhodnocování parametrů spolehlivosti subsystémů kolejových vozidel.

**Nesmyslná alokace požadavků na dodavatele subsystémů kolejového vozidla**

Důležitým krokem při zajišťování spolehlivosti kolejového vozidla je rozdělení požadavků na RAMS mezi jednotlivé subsystémy vozidla. Rozdělení provádí výrobce kolejového vozidla tak,

[10] Pojmy jsou ponechány v původním tvaru použitém v tendrové dokumentaci, včetně gramatických chyb.

[11] Nejčastěji sledovanými a vyhodnocovanými parametry spolehlivosti subsystémů kolejových vozidel jsou *střední doba provozu mezi poruchami (MTBF)*, případně *střední ujetá vzdálenost mezi poruchami (MDBF)*, *střední doba do obnovy (MTTR)*, *pohotovost (A)*. Dále jsou sledovány náklady na preventivní údržbu a náklady na údržbu po poruše.

aby splnil požadavky kladné na celé vozidlo. Opakovaně jsme se setkali se situací, kdy výrobce kolejového vozidla použije požadavky na vozidlo a mechanicky je přenese na subsystém, například na trakční pohon. Po výrobci subsystému tak výrobce kolejového vozidla vyžaduje to samé, co je požadováno pro celé vozidlo. Pro výrobce konkrétního subsystému je v takovém případě část přenesených požadavků irelevantní, protože se daného systému netýkají, a část požadavků výrobce subsystému nemůže splnit už jen proto, že nemá všechny nezbytné informace o kolejovém vozidle, jeho částech a jejich vzájemných interakcích.

V jiných případech rozdělil výrobce kolejového vozidla požadavky na bezporuchovost a pohotovost subsystémů mezi jednotlivé subsystémy způsobem, který nerespektuje specifické vlastnosti a složitost subsystémů vozidla. Výsledek byly nesmyslně vysoké požadavky na bezporuchovost trakčního pohonu a dalších elektrických a elektronických zařízení a zároveň relativně nízké požadavky na mechanické části kolejového vozidla. Objevil se i nápad rozdělit požadovanou úroveň bezporuchovosti a pohotovosti vozidla rovným dílem mezi všechny subsystémy, opět bez ohledu na charakter a složitost subsystémů kolejového vozidla.

**Nedostatek času na splnění úkolů příslušných etap životního cyklu**

Krátké termíny pro podání nabídek ve výběrových řízeních komplikují řádné plnění úkolů spojených s tendrovou fází životního cyklu. Dodavatel subsystému kolejového vozidla má na zpracování nabídky ještě méně času než dodavatel kolejového vozidla a jeho situace je z pohledu managementu RAMS o to složitější. Většina času, jež je k dispozici pro zpracování nabídky, je spotřebována na návrh řešení splňujícího technické požadavky na dodávané zařízení a na posouzení požadavků na RAMS, provedení předběžných RAMS analýz a porovnání jejich výsledků s požadavky zbývá velmi málo času. Přitom je vyžadováno, aby se údaje a hodnoty uvedené v nabídce v případě vítězství ve výběrovém řízení přenesly do příslušných smluv.

***Fáze návrhu (a výroby)***

**Nedostupnost a nedůvěryhodnost RAM údajů od subdodavatelů**

Typickým problémem ve fázi návrhu pohonu trakčního vozidla je špatná dostupnost a malá důvěryhodnost údajů o spolehlivosti jednotlivých dílů. Od řady subdodavatelů je složité získat příslušné údaje a podaří-li se je získat, lze často pochybovat o jejich kvalitě. Zčásti je tato situace způsobená neochotou výrobců poskytovat údaje o spolehlivosti a zčásti skutečností, že výrobci nemají věrohodné údaje o spolehlivosti svých výrobků. U některých výrobců stále přetrvává nízké povědomí o problematice spolehlivosti. Na obrázku 1 je ukázka výpočtu MTBF provedená známým výrobcem prvků pro jištění elektrických obvodů. Úryvek dokumentu je ponechán v autentickém znění s výjimkou označení dílu, jež bylo odstraněno.

**Analýza poruch:**
Analýza poruch se vztahuje k dolnímu držáku pro návěstní zařízení. Tato analýza vychází z množství reklamací vztahující se na celkový počet hodin provozu a prodaných dolních držáků pro návěstní zařízení.

Analýza poruch je provedena v souladu s MILITARY HANDBOOK, Reliability Prediction of Electronic Equipment, MIL-HDBK-217F, Department of Defense, Washington D.C., 1991.

**Výpočet:**
Výpočet je založen na pojmu intenzity poruch λ. Intenzita byla stanovena jako poměr počtu poruch a sledovaného období.

P – počet poruch
T – celkový počet hodin provozu použitých dolních držáků
Λ – intenzita poruch
MTBF – střední doba poruchy

$\Lambda = P/T = 0/ 5{,}35 \cdot 10^{11} = 0\ h^{-1}$

MTBF = 1/ Λ = 1/ 0 = +∞ roků

Výsledná střední doba poruchy MTBF u dolního držáku je +∞ roků.

Obrázek 1: Ukázka nekorektního výpočtu MTBF provedeného výrobcem dílu

**Neefektivní spolupráce a tok informací mezi odděleními uvnitř firmy**

Nutno (i když nikoliv postačující) podmínkou úspěšného managementu spolehlivosti ve výrobě pohonů trakčních vozidel je úzká, trvalá a efektivní spolupráce jednotlivých oddělení výrobního závodu. To je ideální stav, ke kterému bohužel stále máme velmi daleko. Mezery existují jak ve vnitrofiremním toku informací týkajících se RAMS, tak ve spolupráci při plnění konkrétních úkolů definovaných v Programu RAMS. Management spolehlivosti je uvnitř firmy často chápán jen jako další papírování, pracovníkům není zřejmý smysl a cíl řízení spolehlivosti.

### *Fáze provozu*

**Nefunkční sběr a předávání dat o provozu a poruchách subsystémů kolejového vozidla**

Data o provozu a poruchách kolejového vozidla a jeho subsystémů mají zásadní význam pro výrobce kolejového vozidla i pro subdodavatele. Po dobu trvání garance, kdy je údržba zajišťována dodavatelem vozidla, je sběr provozních a poruchových dat relativně snadný. To ovšem platí pro výrobce celého vozidla. Dodavatel subsystému často nedostává od výrobce vozidla dostatečné informace o poruchách svých zařízení, u dat o provozu je dostupnost ještě horší. S koncem garance většinou končí i systematický sběr dat o provozu a poruchách, případně se data stávají nedostupnými pro výrobce vozidla a tudíž i pro výrobce subsystémů. Při porovnání s požadovanou životností kolejového vozidla, jež běžně bývá 30 let, je zřejmé, že z většiny doby životnosti vozidla nemá jeho výrobce k dispozici data o provozu a poruchách.

**Nevěrohodnost a nekompletnost dat o provozu a poruchách**

Kromě zajištění sběru a předávání dat o provozu a poruchách kolejového vozidla má klíčovou roli také kvalita dat, tj. jejich kompletnost a věrohodnost. Na kvalitě dat závisí korektní vyhodnocení plnění smluvně dohodnutých parametrů spolehlivosti a kvalitní data jsou pro výrobce kolejového vozidla a výrobce subsystémů nenahraditelným zdrojem informací o skutečně dosahované úrovni spolehlivosti jejich výrobků. V praxi bohužel často není kvalita dat dostačující. Data nebývají kompletní, tj. nejsou zaznamenány všechny poruchy, které v daném časovém období nastaly, a chybí informace o subsystémech a jejich částech v provozu, na nichž se závada nevyskytla. U zaznamenaných poruch je problémem nízká věrohodnost některých údajů (např. projezd kolejového vozidla, správná identifikace příčiny poruchy apod.).

# 5. Závěr

Management spolehlivosti trakčních pohonů a dalších subsystémů kolejových vozidel je komplexním procesem zasahujícím do všech fází životního cyklu. Efektivní řízení spolehlivosti představuje pro výrobce subsystému kolejového vozidla náročný a dlouhodobý úkol, při jehož plnění se třeba řešit řadu dílčích leč zásadních problémů. V příspěvku bylo nastíněno, jakým způsobem je management spolehlivosti implementován ve ŠKODA ELECTRIC, a.s. a jaké překážky při řízení spolehlivosti překonáváme. Lze konstatovat, že po cestě řízení spolehlivosti jsme již kus ušli, ale pořádnou část cesty k efektivnímu managementu spolehlivosti máme stále ještě před sebou.

Příloha 1: Ukázka specifikace požadavků v zadávací dokumentaci

## 22.3 RELIABILITY PROGRAM

22.3.1 **General**

22.3.1.1 The Commission requires the Contractor to design and deliver a vehicle with a high level of reliability. The reliability levels specified in this Section are the minimum levels that shall be considered acceptable. Equipment selection shall be based on providing equipment proven in a transit environment with the highest degree of reliability. The Contractor shall develop and implement a program to ensure that the vehicle and its major systems meet or exceed the reliability requirements specified in this section. The Contractor shall be responsible for providing all measures required to meet the specified reliability requirements. Where the vehicle does not meet the specified requirements the Contractor shall be responsible for the actions necessary to improve the reliability to achieve the requirements including design, manufacture, software update, installation, retrofit of the entire fleet, and all changes.

22.3.1.2 The Contractor shall develop a reliability model based on established reliability prediction techniques. The technique used shall be subject to the approval of the Engineer. The Contractor shall revise the model on a regular basis to reflect current designs.

22.3.1.3 Vehicle system reliability calculations shall be based on single vehicle operation with an average speed of 17 km/h and an average of 50 000 km per vehicle year.

22.3.2 **Reliability Estimate**

22.3.2.1 The Contractor shall submit for approval a reliability estimate demonstrating how the vehicle shall achieve compliance with the reliability requirements specified. The Contractor shall provide a reliability estimate for the entire vehicle and for each major system (excluding TTC furnished equipment) down to at least the LRU level. Estimates shall be expressed in terms of Mean Distance Between Relevant Failures (MDBRF) for each of the Failure Mode Categories defined in TS 22.3.3.4.

22.3.2.2 The Reliability Estimate shall be supported by an allocation of the reliability requirements to each system, subsystem, and major component identified in TS 22.3.3.7. Once reviewed by the Engineer, the reliability allocation will be used to monitor the compliance of the vehicle and systems with the reliability requirements. Adjustments to the reliability allocation shall be submitted to the Engineer for review and comment.

22.3.2.3 Estimates shall, where possible, be based on actual revenue service results for identical equipment operating under service conditions and duty cycles equivalent to, or more severe than those specified. Reasonable extrapolations may be made for non-identical but similar equipment. Supporting documentation for the extrapolations shall be submitted to the Engineer for approval.

22.3.2.4 For equipment that is a new design or a significant evolution or upgrade of existing equipment, the prediction shall be developed based upon the methodology of MIL-HDBK-217 or historical reliability data, including Reliability Analysis Center (RAC) Non-electronic Parts Reliability Data (NPRD). The Contractor shall submit details of the methodology to be used for the reliability estimate prior to submission of the estimate. This shall be subject to approval by the Engineer.

22.3.3 **Reliability Criteria**

22.3.3.1 All equipment failures during the warranty period will be reviewed by the Contractor and the Commission and classified as either relevant or non-relevant. The Contractor shall prepare, maintain, and submit a report recording the performance of the reliability fleet, including trends in reliability, availability and maintainability; this shall be reported within the System Assurance Progress Reports.

22.3.3.2 The report will contain all the information required to calculate MDBRF as specified in TS.

22.3.3.4. The Contractor shall supply within the System Assurance Progress Report a monthly report based on the FRACA information listing the results for MDBRF A, B, C, D and the overall vehicle and system/component level MDBRFs. This report will cover the most recent 12-month period. After twelve months, the report will be a rolling twelve-month report with the oldest month being dropped and the new month added. This report will be used for the reliability, availability and maintainability assessment.

22.3.3.3 Light Rail Vehicle kilometres are defined as the total fleet mileage of all the Light Rail Vehicles. The measurements shall be performed weekly. The results shall be reported using a 12 month moving interval.

22.3.3.4 The minimum Fleet MDBRF for each mutually exclusive Failure Mode Category shall be at least:

| Category | Definition | Failure Effects | Requirement |
|---|---|---|---|
| A | Severe Vehicle Impairment | Rescue towing/pushing is required | 800,000 km |
| B | Vehicle Impairment | Five minute delay in service, or removal from service after all passengers have disembarked at the nearest stop | 35,000 km |
| C | Minor Vehicle Impairment | In service until next terminus is reached with or without minor operational restrictions | 15,000 km |
| D | No Vehicle Impairment | In service until end of day according to scheduled service | 10,000 km |

Where:

(a) Category A relevant failure is a failure that requires the Light Rail Vehicle to be rescued, such as complete propulsion failure or primary current collection failure.

(b) Category B relevant failure is a failure that:
i. results in a delay to service of 5 minutes or greater; or
ii. results in unscheduled removal from revenue service or prevention of scheduled entry into service.

(c) Category C relevant failure is a failure that results in reduced vehicle performance such as single door cut-out (excluding the accessibility ramp equipped door), loss of propulsion on one bogie, loss of braking on one bogie, loss of one saloon HVAC unit. The required function is partially fulfilled due to the redundant design of the components.

(d) Category D relevant failure include all failures that are not Category A, B or C, including resets. The operational ability of the vehicle is not restricted.

22.3.3.5 For the purposes of this calculation, the fleet, includes all vehicles which have received Final Acceptance. This measure is established to ensure that life-cycle costs of the vehicle are minimized.

$$MDBRF = \frac{\text{Total travelled Light Rail Vehicle kilometres}}{\text{Total number of relevant failures}}$$

22.3.3.6 A relevant failure is defined as any failure that requires a non-scheduled maintenance action resulting in repair or replacement of any vehicle subsystem or component which is not an approved consumable but has not achieved its design life. Relevant failures shall include failures requiring the

operator to reset or bypass systems, regardless of whether the event leads to a delay to service or loss of performance or other penalty. Exclusions to this definition are failures caused by:

(a) A dependent failure in another system or subsystem
(b) A planned preventative maintenance action
(c) Incorrect or abusive operating use by operating or maintenance personnel
(d) Implementation of maintenance procedures, practices or materials inconsistent with those prescribed by the Contractor
(e) External influences including force majeure or exceptional climatic conditions
(f) Actions occurring as part of regularly scheduled maintenance
(g) Replacement of consumable items such as light bulbs and filters
(h) Retrofit/modification activities
(i) Traffic accident not associated with the normal operation of items
(j) Vandalism
(k) Parts supplied as free issue by TTC

22.3.3.7 The Contractor's Reliability Estimate shall identify the anticipated reliability levels for the following systems and components of the vehicle (assuming routine maintenance is performed as recommended by the Contractor):

(a) Auxiliary Electrical System
(b) Bogies & Suspension
(c) Carbody (Non-structural)
(d) Destination Signs
(e) Disc Brakes
(f) Doors & Door Controls
(g) High Voltage Power System
(h) HVAC
(i) Hydraulics
(j) Lighting (except light bulbs)
(k) MDS
(l) Onboard Communications
(m) Pneumatics
(n) Track Brakes
(o) Traction Equipment & Controls

Note: Any components within a system listed shall not contribute more than 20% to the overall vehicle MDBRF. The assignment of components shared by two or more systems will be determined by the Engineer. For vehicle components and systems not listed, the cumulative fleet defect rate in any 12 consecutive month period shall not exceed 10% of the overall failure rate.

22.3.4 **Reliability, Maintainability and Availability Verification Programs**

22.3.4.1 The Reliability Verification Program shall commence when the first production vehicle Light Rail Vehicles enters revenue service and continue to the end of the warranty period of the final accepted vehicle, or until the entire fleet achieves the reliability levels specified, whichever is later.

22.3.4.2 The procedures which will be used to track and monitor the reliability performance of the Light Rail Vehicles and major subsystems shall be mutually agreed to by the Contractor and the Commission 120 calendar days prior to the delivery of the first Light Rail vehicle.

22.3.4.3 The Light Rail Vehicle Fleet shall be considered as having successfully passed the Reliability Verification Program when the individual 12 month moving average for each MDBRF Failure Mode Category has met its specified level in TS 22.3.3.4. Where the demonstration shows compliance with the reliability requirements prior to the end of the warranty period of the final accepted vehicle, the Contractor shall continue to monitor reliability throughout the demonstration program. Where reductions below 85%

of the reliability performance requirement for any MDBRF Failure Mode Categories occurs, the Contractor shall address the reliability performance as per TS 22.3.4.9.

22.3.4.4 The Reliability Verification Program shall demonstrate that the Light Rail Vehicle achieves the specified reliability, maintainability and availability requirements detailed in the SAPP as approved by the Engineer.
22.3.4.5 All subsystems shall be included in the reliability verification program. The Contractor shall perform failure/incident data analyses, component analyses and provide corrective action. The Contractor shall submit monthly status reports shall include as a minimum a statement of failures, identified causes, and achieved MDBRF for each subsystem.

22.3.4.6 The maintainability verification program shall be conducted on assemblies, components, and subsystems selected by the Engineer. The Contractor shall submit a list of LRUs together with the MTTR for each item. The Engineer shall select items to be demonstrated from this list. The Contractor shall assume that a minimum of 30% of all LRUs shall be subjected to Maintainability Demonstration.

22.3.4.7 Each Light Rail Vehicle shall enter the verification program upon entry into revenue service.

22.3.4.8 During the period of the Reliability Verification Program, the Contractor shall compute and report the MDBRF of each subsystem and the complete Light Rail Vehicle on a monthly basis.

22.3.4.9 If the Fleet MDBRF reliability requirements for any Failure Mode Category set out in this Section, once achieved, is not maintained to the level specified in TS 22.3.4.3, the Contractor shall prepare and submit within 30 calendar days to the Engineer an analysis of the causes of the unreliability for acceptance. The analysis shall include the steps necessary to achieve the minimum specified reliability including, if necessary a retrofit plan to upgrade, at the Contractor’s expense, deficient components or systems. The plan shall include detailed timelines for achievement of the reliability requirements.

# Funkční bezpečnost systémově

Ing. Pavel Fuchs, CSc., Technická univerzita v Liberci
tel. +420 485 353 287, e-mail: pavel.fuchs@tul.cz

## 1. Úvod

Pro efektivní řízení rizika je třeba umět riziko správně posuzovat. V technické praxi se posuzování rizika stává jedním ze základních prostředků k prokázání, že zařízení je dostatečně bezpečné. To se promítá i do norem v různých průmyslových odvětvích. Tyto normy vyžadují provést posouzení rizika zařízení a prokázat, že riziko je přijatelné. Pro posuzování rizika pak nabízejí různé přístupy k hodnocení rizika – kvalitativní, semikvantitativní a kvantitativní. Tyto normy zpravidla nedávají konkrétní návod, jak postupovat při hodnocení rizika v jednotlivých případech. S ohledem na různorodost nebezpečných jevů a jejich následků jsou koncipovány jako obecná doporučení. Pokud normy tato obecná doporučení konkretizují formou příkladů, jsou tyto příklady řazeny do příloh, které jsou označovány jako informativní. Nejsou tedy závazné.

Za základní normy funkční bezpečnosti jsou považovány IEC 61508-5 [1] a IEC 61511-x [2]. Jejich principy pak přejímají další normy z různých průmyslových odvětvích se vztahem k funkční bezpečnosti, např. IEC 62061 [3], ISO 13849 [4], IEC 61513 [5], EN 50129 [6] a další. Uvedené základní normy jsou výsledkem historického vývoje chápání úlohy bezpečnostních systémů při redukci rizika plynoucího z provozu technických zařízení. Jsou zaměřeny na to, aby návrh, výroba a provozování těchto bezpečnostních systémů zajistily jejich dostatečnou odolnost proti náhodným a systematickým poruchám. Jinými slovy řečeno, aby zajistily vysokou funkceschopnost bezpečnostních systémů. Za tím účelem předepisují postupy a techniky, které je třeba aplikovat. Čím více je třeba snížit riziko, tím sofistikovanější a nákladnější jsou bezpečnostní systémy k tomu určené.

Při aplikaci požadavků norem pro konkrétní technické řešení je tedy třeba správně chápat podstatu rizika a způsobů jeho hodnocení. Nelze tedy neuváženě aplikovat příklady hodnocení rizika, které jsou uváděné v normách. To by mohlo vést k podhodnocení nebo nadhodnocení rizika. A ve svých důsledcích k neefektivnímu řízení rizika.

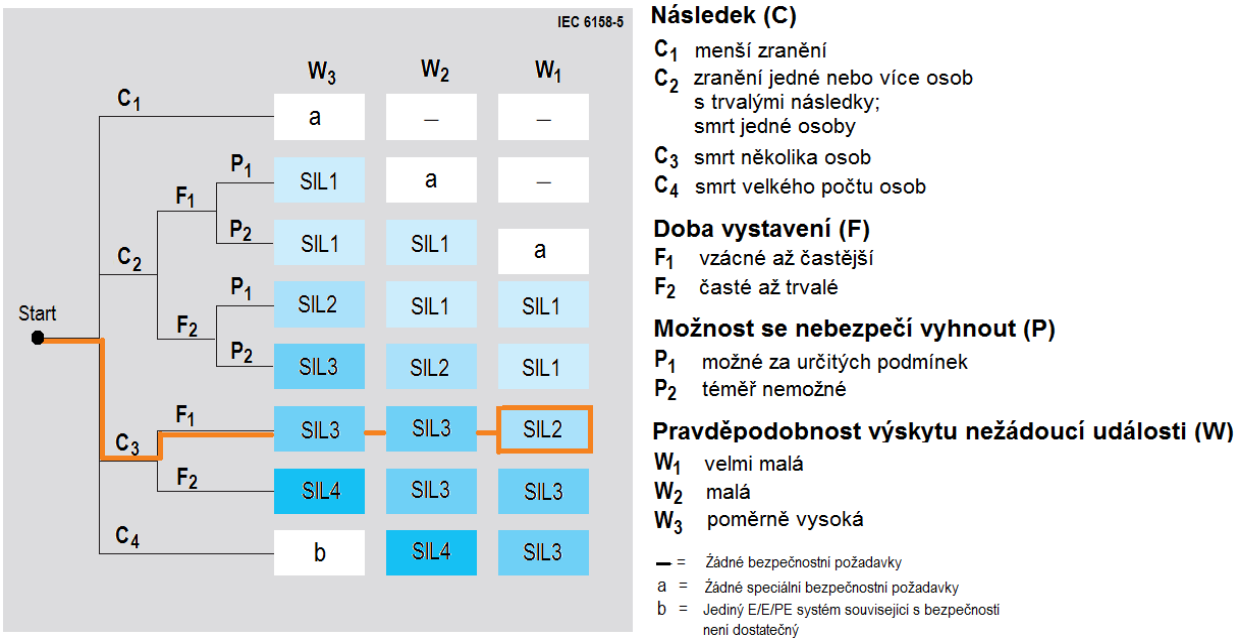
Je tedy zřejmé, že prvním krokem při snižování rizika pomocí bezpečnostních systémů je stanovení hodnoty rizika z provozovaného zařízení, označovaného jako EUC (Equipment Under Control). Pokud není riziko v tomto kroku stanoveno korektně, není dosaženo optimálního řešení. Bezpečnostní systémy jsou pak navrhovány buď s nadměrnou, nebo nedostatečnou odolností proti systematickým a náhodným poruchám. Z toho pak vyplývají příslušné ekonomickými a bezpečnostními důsledky.

Při nepochopení toho, že systémový přístup k návrhu bezpečnostních systémů znamená především systémové poznání rizika, může být aplikace zjednodušených postupů uvedených v informativních přílohách příslušných norem zavádějící.

V tomto příspěvku je nejprve prezentována analýza zjednodušených přístupů k určování integrity bezpečnosti podle IEC 61508-5. Následně je stručně zmíněna praxe při návrhu bezpečnostních systémů podle IEC 61508-5 v energetice ČR. Účelem příspěvku je poukázat na východiska a slabiny v hodnocení rizika a posuzování jeho přijatelnosti při použití této normy.

## 2. Riziko a SIL podle IEC 61508-5

Norma IEC 61508-5 prezentuje v Příloze E (informativní) kvalitativní metodu pro určení SIL, označovanou jako diagram rizika. Princip této metody je zřejmý z obr. 1.




Obr. 1: Prvky hodnocení rizika a určování SIL podle IEC 61508-5

Tento zjednodušený postup je založen na vztahu

$$R = (f)\ specifikovaného\ (C) \tag{1}$$

a předpokladech, že $C_1 < C_2 < C_3 < C_4$; $F_1 < F_2$; $P_1 < P_2$; $W_1 < W_2 < W_3$.

Kde

*R* je riziko bez použití systémů souvisejících s bezpečností;

*f* je četnost (frekvence) nebezpečné události bez použití systémů souvisejících s bezpečností;

*C* je následek nebezpečné události (tyto následky se mohou týkat škod souvisejících se zdravím a bezpečnosti nebo škod z poškození environmentu).

Četnost (frekvence) nebezpečné události *f* je v tomto případě tvořena třemi ovlivňujícími činiteli:

- četností výskytu a dobou vystavení v nebezpečné oblasti;
- možností se nebezpečné události vyhnout;
- pravděpodobností výskytu nebezpečné události bez přidání jakýchkoli systémů souvisejících s bezpečností, tj. pravděpodobnost nežádoucího výskytu.

To vede k těmto čtyřem parametrům rizika:

- následku nebezpečné události (*C*);
- četnosti (frekvenci) výskytu a době vystavení v nebezpečné oblasti (*F*);
- možnosti se nebezpečné události vyhnout (*P*);
- pravděpodobnosti nežádoucího výskytu (*W*).

Úroveň integrity bezpečnosti (SIL) systému souvisejícího s bezpečností je proti netolerovatelnému riziku specifikována prostřednictvím cílových hodnot míry poruch uvedených v tab. 1.

Tab. 1: Úroveň integrity bezpečnosti podle IEC 61508-5 – cílové hodnoty míry poruch bezpečnostní funkce

| **Úroveň integrity bezpečnosti (SIL)** | **Průměrná pravděpodobnost nebezpečné poruchy na vyžádání bezpečnostní funkce [1] (PFDavg)** | **Průměrná frekvence nebezpečné poruchy bezpečnostní funkce [$h^{-1}$] (PFH)** |
|---|---|---|
| 4 | ≥1E-5 to <1E-4 | ≥1E-9 to <1E-8 |
| 3 | ≥1E-4 to <1E-3 | ≥1E-8 to <1E-7 |
| 2 | ≥1E-3 to <1E-2 | ≥1E-7 to <1E-6 |
| 1 | ≥1E-2 to <1E-1 | ≥1E-6 to <1E-5 |

Podle terminologie používané ve spolehlivosti je pravděpodobnost nebezpečné poruchy na vyžádání totožná s nepohotovostí a frekvence nebezpečné poruchy je totožná s intenzitou (nebezpečných) poruch, resp. parametrem (nebezpečných) poruch.

# 3. Korektnost hodnocení rizika a úrovně integrity bezpečnosti

## 3.1 Základní úvahy k řešenému problému

Hodnocení rizika je spojeno s aleatorní nejistotou a epistemickou nejistotou. Aleatorní nejistoty jsou dány přirozenými náhodnostmi v chování zkoumaného objektu. Epistemické nejistoty jsou způsobeny nedostatky v našich znalostech o zkoumaném objektu. Použití zjednodušených metod pro posuzování rizika má smysl tehdy, pokud zjednodušením nedojde k významnému zvýšení epistemické nejistoty. Tedy, pokud se k epistemické nejistotě znalostí o riziku objektu nepřipojí epistemická nejistota hodnocení rizika zjednodušeným přístupem.

Účelem zkoumání je zjistit, jak korektní je hodnocení rizika při použití zjednodušených přístupů. Výsledkem zkoumání je pak lepší poznání zákonitostí platných pro použití zjednodušených přístupů k hodnocení rizika a tedy snížení epistemické nejistoty při jejich použití.

Je evidentní, že při kvantitativním hodnocení rizika je pravděpodobnost realizace následku nežádoucí události dána součinem pravděpodobnostních parametrů a následku. Tedy násobením hodnot všech parametrů. Pokud bychom znali hodnoty těchto parametrů, jsme schopni exaktně riziko hodnotit.

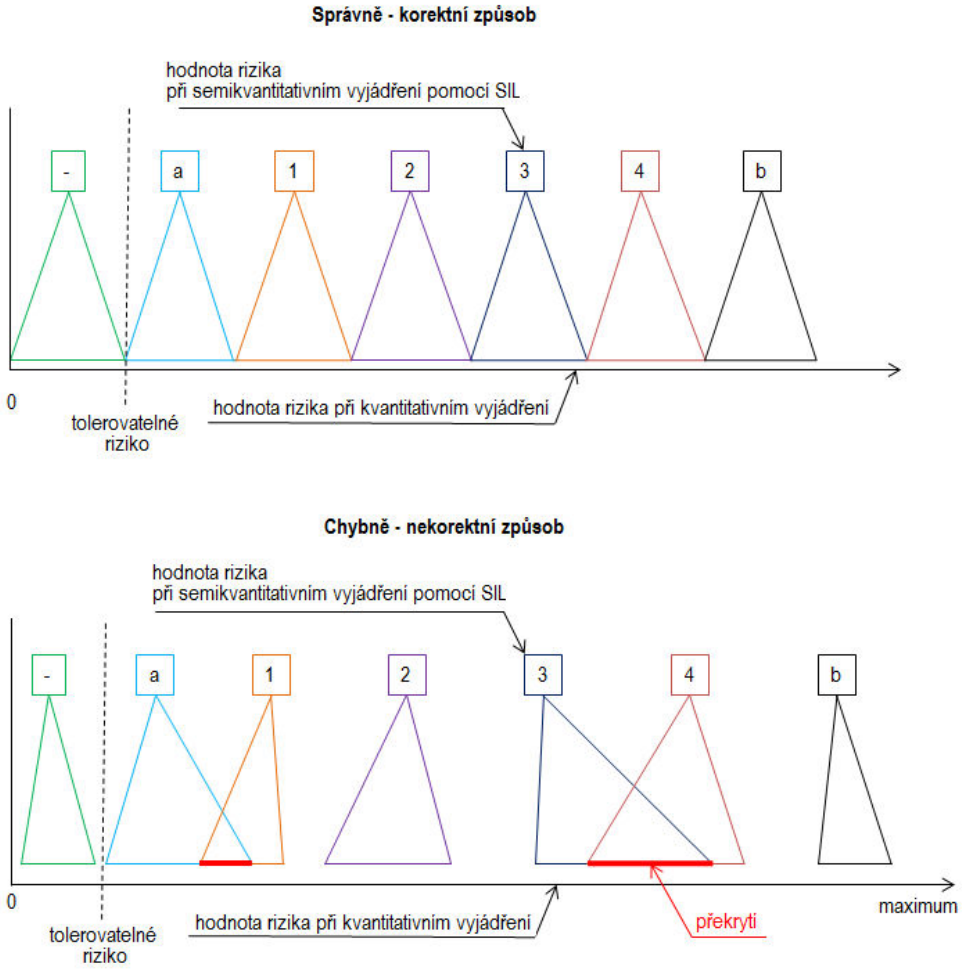
Při použití zjednodušených přístupů se však nepoužívají skutečné hodnoty parametrů. Parametry jsou rozděleny do pásem. V pásmech se pak místo skutečných hodnot používají slovní (kvalitativní) hodnocení nebo poměrné (semikvantitativní) hodnocení vyjádřené např. v bodech. Na základě stanovených pravidel, viz kap. 2, se pak riziko hodnotí a přiřazuje se úroveň integrity bezpečnosti. To platí nejen pro IEC 61508-5, ale i pro IEC 62061, ISO 13849-1 a další normy, které prezentují zjednodušené přístupy pro hodnocení rizika. Proto je nezbytné mít představu o

tom, jaký vliv má volba způsobu ocenění parametrů a použitých pravidel na korektnost hodnocení rizika.

### 3.2 Posouzení korektnosti zjednodušeného přístupu podle IEC 61508-5

Metoda stanovení úrovně integrity bezpečnosti (SIL) je založena na kvalitativním hodnocení rizika. Pásma parametrů *C*, *F*, *P* a *W* a jejich rozsah jsou oceněna slovním popisem. Podle popisu pásem lze u parametrů *C*, *F* a *P* usoudit, že pásma jsou uspořádána do stupnice sestavené podle geometrické posloupnosti bez specifikovaného kvocientu. Pro parametr *W* lze usuzovat, že i jeho stupnice je sestavena podle geometrické posloupnosti s neznámým kvocientem.

Pokud je zjednodušený přístup korektní, musí jeho výsledky odpovídat výsledkům získaným při použití plně kvantitativního hodnocení rizika. Jednotlivé úrovně funkční bezpečnosti (-, a, 1, 2, 3, 4, b) pokrývají po sobě jdoucí intervaly rizika. Při správném nastavení pásem parametrů *C*, *F*, *P* a *W* by nemělo dojít k jejich překrývání, viz obr. 2.




Obr. 2: Pokrytí rizika prostřednictvím SIL

Posouzení korektnosti zjednodušeného přístupu bylo založeno na zkoumání, zda lze pásma parametrů *C*, *F*, *P* a *W* nastavit tak, aby došlo k jednoznačnému pokrytí rizika prostřednictvím SIL. Musí tedy platit nerovnost

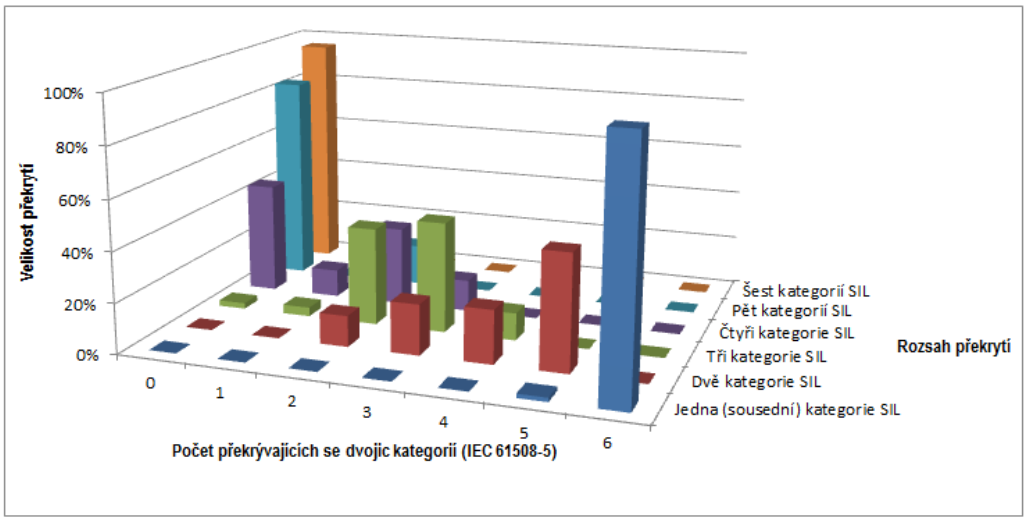
$$R_{\_} < R_a < R_1 < R_2 < R_3 < R_4 < R_b \qquad (4)$$

Není-li nerovnost splněna, dochází k překrytí rizika dvěma či více SIL a zjednodušený přístup nelze považovat za korektní.

Pomocí simulací v Matlabu byly zjištěny výsledky pro všechny celočíselné kombinace v intervalu <2; 20> kvocientů stupnic s geometrickou posloupností parametrů *C*, *F*, *P* a *W*. Bylo tedy prověřeno celkem $19^4 = 130\,321$ možností hodnocení rizika podle zjednodušeného přístupu. Zjištěný počet překrytí dvěma či více SIL je uveden v tab. 2 a obr. 3.

Tab. 2: Počet překrytí (IEC 61508-5)

| **Rozsah překrytí** | **Počet překrývajících se dvojic kategorií SIL** | | | | | | |
|---|---|---|---|---|---|---|---|
| | **0** | **1** | **2** | **3** | **4** | **5** | **6** |
| Jedna (sousední) kategorie SIL | 0 | 0 | 0 | 14 | 82 | 2 114 | 128 111 |
| Dvě kategorie SIL | 2 | 169 | 16 107 | 26 263 | 27 773 | 6 007 | 0 |
| Tři kategorie SIL | 2 995 | 4 695 | 50 819 | 57 508 | 14 304 | 0 | 0 |
| Čtyři kategorie SIL | 58 236 | 14 490 | 41 143 | 16 452 | 0 | 0 | 0 |
| Pět kategorií SIL | 108 870 | 0 | 21 451 | 0 | 0 | 0 | 0 |
| Šest kategorií SIL | 124 922 | 5 399 | 0 | 0 | 0 | 0 | 0 |



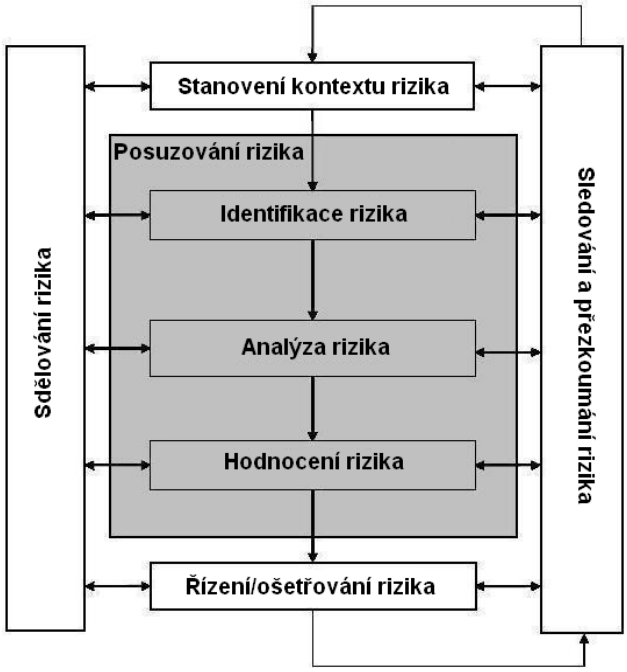

Obr.3: Rozsah a velikost překrytí (IEC 61508-5)

Pokud by zjednodušený přístup hodnocení rizika byl stejně dobrý jako exaktní kvantitativní způsob hodnocení rizika, obsahovala by tab. 5 ve sloupci "0" v každém řádku hodnotu 130 321. Z rozložení nenulových hodnot a jejich velikosti lze usuzovat na to, jak je zjednodušená metoda citlivá na přesnost odhadu parametrů *C*, *F*, *P* a *W*. Při generování možných odhadů rizika byly samozřejmě vygenerovány i "brutální" kombinace, které by při aplikaci zjednodušeného přístupu v praxi nebyly použity. Ty jsou reprezentovány např. hodnotou 5 297 kombinací kvocientů, kdy překrytí jde přes šest kategorií SIL. Přesto je z prezentovaných výsledků zřejmé, že zjednodušený přístup vede ke značným nepřesnostem při hodnocení rizika a určování SIL. Zjednodušený přístup se ani v jediném případě nevedl ke korektnímu určení SIL, viz hodnota 0 ve sloupci "0". Nelze jej tedy považovat za korektní.

# 4. Funkční bezpečnost v energetice

## 4.1 Základní přístup

Při výstavbě nových klasických elektráren zadal ČEZ, a.s., požadavek, aby jejich projektant a dodavatel ŠKODA Praha Invest s.r.o. přistupoval k funkční bezpečnosti podle normy IEC 61508-1. K tomu je nezbytné provést posouzení rizika a při návrhu a výrobě bezpečnostních systémů postupovat v souladu s požadavky na zmírnění rizika, které vyplývají z posouzení rizika. Vlastní proces managementu rizika [7], jehož jádrem je posuzování rizika je zachycen na obr. 4.




Obr.4: Proces managementu rizika

Posuzování rizika je složeno z identifikace, analýzy a hodnocení rizika, viz obr. 1. K tomu účelu byly použity dvě metody. Pro identifikaci a analýzu rizika byla použita metoda HAZOP [8]. Hodnocení rizika bylo provedeno podle IEC 61508-5 metodou kvalitativního odhadu rizika pro stanovení úrovně funkční bezpečnosti SIL.

Metoda HAZOP byla vyvinuta pro potřeby identifikace a analýzy rizik chemického průmyslu. Rozšířila se i do dalších odvětví. ČEZ ji uplatňuje v ČR při výstavbě nových klasických elektráren na základě požadavků příslušných orgánů udělujících povolení k výstavbě.

Metoda HAZOP využívá systému návodných slov (např. „více“, „méně“, „jiný než“ atd.), která jsou aplikována na parametry zařízení (např. teplota, tlak, hladina, složení atd.) za účelem nalezení možných odchylek a navržení vhodných doporučení k vyřešení problémů, vyplývajících z uvedených odchylek. HAZOP tedy identifikuje příčiny a analyzuje následky nežádoucích událostí. Stručný příklad záznamu HAZOP s identifikovanou a analyzovanou bezpečnostně významnou situací je uveden v tab. 3.

Tab. 3: Příklad záznamu HAZOP kotle

| E2-NO4: Určení za normálního provozu: Dodávat natlakovanou VT páru z VT bubnu přes parní potrubí do komory syté páry, dále potrubím do VT přehříváku1, do VT přehříváku 2, pak do VT přehříváku 3, dále přes potrubí LBA30 a hlavní parní šoupě LBA30AA001E spotřebiči. | | | | |
|---|---|---|---|---|
| **Návodné slovo** | **Odchylka** | **Příčina** | **Následek** | **Zabezpečení** |
| NE, NENÍ | Žádný průtok | Uzavřené hlavní parní šoupě LBA30AA001E | Nárůst tlaku páry – možné poškození všech výhřevných ploch uvnitř kotle a/nebo potrubí voda/pára mimo kotel – **nebezpečné pro osoby v okolí kotle**. | Tlakový monitorovací systém LBF31GH001E VT by-passu LBF31AA101C s bezpečnostní funkcí - otevření VT by-passu LBF31AA101C s bezpečnostní funkcí. Měření průtoku LBA30CF001 – signalizace na velín. |

Takových situací na kotli elektrárny je samozřejmě analyzováno mnohem více. Všechna identifikovaná a analyzovaná rizika je třeba individuálně vyhodnotit. Hodnotí se z hlediska jeho přijatelnosti či nepřijatelnosti. V případě nepřijatelného rizika je pak třeba implementovat bezpečnostní funkci, která zaručí snížení rizika na přijatelnou hodnotu.

Pro všechna analyzovaná rizika se rizika bylo hodnocení rizika provedeno metodou kvalitativního odhadu rizika podle IEC 61508-5 to prostřednictvím stanovení úrovně funkční bezpečnosti SIL. Na základě této kvalitativní metody byla ohodnocena všechna rizika kotle a k nim přiřazena požadovaná úroveň funkční bezpečnosti SIL požadovaná pro funkce bezpečnostních systémů kotle. Záznam hodnocení rizika a přiřazení SIL je uveden v tab. 4.

Tab. 4: Příklad záznamu hodnocení rizika a přiřazení SIL

| **E2: Systém VT vody / páry** | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **č.** | **Zdroj ohrožení** | **Příčina ohrožení** | **Následky** | **E/E/EP + JTP** | **Hodnocení rizika** | | | | |
| | | | | | **C** | **F** | **P** | **W** | **SIL** |
| 1 | Vysoká teplota vody / páry | Uzavřené hlavní parní šoupě LBA30AA001E | Nárůst tlaku páry – možné poškození všech výhřevných ploch uvnitř kotle a/nebo potrubí voda/pára mimo kotel – **nebezpečné pro osoby v okolí kotle**. | Tlakový monitorovací systém LBF31GH001E VT by-passu LBF31AA101C s bezpečnostní funkcí (BF). | C3 | F1 | P2 | W2 | 2 |

## 4.2 Úskalí při uplatňování

Velké elektrárenské bloky představují komplexní technický systém. Na jeho projektování, výrobě, výstavbě a dalších činnostech se podílí řada dodavatelů. Dodávky ucelených funkčních celků elektrárny jsou předmětem výběrových řízení v tzv. obchodních balíčcích (OB). Funkční bezpečnost se uvažuje ve všech dodávkách. To znamená, že pro jednotlivé OB jsou zpracovány studie s posouzením rizika a stanovením požadavků na SIL. Avšak při aplikaci IEC 61508-5 jsou i renomovanými dodavateli používány zjednodušené metody kvalitativního odhadu diagramem rizika podle informativní přílohy. Problémem je, že tito dodavatelé si neuvědomují úskalí zjednodušené metody a jejich volba stupnic a parametrů rizika není zcela korektní.

K tomu ještě přistupuje skutečnost, že i tuto zjednodušenou metodu používají v různých modifikacích. To dokumentuje tab. 5. Z pochopitelných důvodů jsou dodavatelé anonymizováni.

Tab. 5: Specifikování rizikových parametrů

| OB | SIL zpracoval | Parametr | | | |
|---|---|---|---|---|---|
| | | C | F | P | W |
| 01 | Dodavatel 1 | C = 4 – 14 podle kombinace počtu postižených osob a následků pro nejpostiženější osobu | F = 2 – 10 podle kombinace doby expozice nebezpečím a možnosti, že dojde k zasažení osoby | P = 2 – 10 podle kombinace doby od detekce nebezpečí k vzniku újmy a možnosti se nebezpečí vyhnout | W = 1 – 9 podle roční četnosti (frekvence) výskytu nežádoucí události |
| 03 | Dodavatel 2 | C1 = žádné zranění nebo malé provozní ztráty<br>C2 = lehké zranění nebo velké provozní ztráty<br>C3 = těžké zranění nebo střední náklady na opravy<br>C4 = smrt nebo velké náklady na opravu | F1 = vzácné až častější,<br>F2 = časté až trvalé | P1 = možné za určitých podmínek - dbalá obsluha a dobrý systém kontroly může odhalit a předejít události (> 80%)<br>P2 = téměř nemožné - šance na předejití události menší než 80 % | W1 = méně než jednou za 10 let<br>W2 = jednou za 10 let<br>W3 = jednou za rok<br>W4 = více než 10 výskytů za rok |
| 08 | Dodavatel 3 | C1 = menší zranění<br>C2 = zranění jedné nebo více osob a trvalými následky; smrt jedné osoby<br>C3 = smrt několika osob<br>C4 = smrt velkého počtu osob | F1 = vzácné až častější,<br>F2 = časté až trvalé | P1 = možné za určitých podmínek<br>P2 = téměř nemožné | W1 = velmi malá pravděpodobnost, že dojde k nežádoucím výskytům a je pravděpodobných pouze několik nežádoucích výskytů<br>W2 = malá pravděpodobnost že dojde k nežádoucím výskytům a pravděpodobných je málo nežádoucích výskytu<br>W3 = poměrně vysoká pravděpodobnost, že dojde k nežádoucím výskytům a časté nežádoucí výskyty jsou pravděpodobné |
| 02<br>04<br>05<br>06<br>07<br>12 | Dodavatel 3 | C1 = žádné nebo menší zranění<br>C2 = zranění jedné nebo více osob a trvalými následky; smrt jedné osoby<br>C3 = smrt několika osob<br>C4 = smrt velkého počtu osob | F1 = vzácné až častější<br>F2 = časté až trvalé. | P1 = možné za určitých podmínek - dbalá obsluha a dobrý systém kontroly může odhalit a předejít události (> 80%)<br>P2 = téměř nemožné - šance na předejití události menší než 80 % | W1 = méně než jednou za 10 let<br>W2 = jednou za 10 let<br>W3 = jednou za rok |

Jen u parametru *C* si lze ve všech případech učinit představu o jeho hodnotě na základě ohodnocení následků na zdraví a životy osob. Vyjma OB01 chybí uvedení rozsahu pro parametry F a P. Rozsah parametru W není uveden pro OB08. Je zřejmé, že vágní stanovení rozsahu parametrů ve většině případů vede k zavádějícímu hodnocení rizika. Navíc není zdůvodněna volba hodnot (pásma) parametru. **Z uvedených důvodů nelze klasifikaci SIL považovat za korektní**.

Uvedený případ má za následek, že v jednotlivých OB mohou být proti stejně velkému riziku navrhovány odlišné SIL. Proto po zjištění této situace bylo přistoupeno ke sjednocení těchto analýz.

# 5. Závěr

Norma IEC 61508-5 a další normy řešící problematiku funkční bezpečnosti, jako je IEC 62061, ISO 13849-1 a další, neuvádějí žádné primární zdroje s odkazy na fundamentální práce s oboru rizika. Normyy sice v obecné rovině doporučují aplikovat kvantitativní hodnocení rizika, ale pro praktické použití nabízejí informativní návody na kvalitativní a semikvantitativní hodnocení rizika formou grafů či matic rizika a z nich pak vyplývajících požadavků na SIL. Aplikace těchto standardů bez přihlédnutí k charakteru objektů, které jsou zdrojem rizika, může být zdrojem závažných chyb.

Zejména zjednodušené přístupy hodnocení rizika prezentované v informativní příloze normy IEC 61508-5 jsou velmi závislé na správném chápání rizika. Jsou značně citlivé na způsob sestavení stupnic parametrů rizika. Proto při hodnocení rizika komplexních systémů (elektrárny, chemické provozy, kolejová vozidla a další) je třeba zjednodušený přístup aplikovat jednotně pro všechna zařízení, která tvoří systém. Při kvalitativním či semikvantitativním hodnocení rizika komplexních systémů nelze zaručit korektní stanovení SIL, pokud nejsou korektně sestaveny stupnice parametrů rizika. Může dojít k fatálním omylům, které lze částečně eliminovat jednotným způsobem nastavení parametrů rizika (pravděpodobnosti a následku) pro všechny dodavatele zařízení, která tvoří komplexní systém. To znamená, že je třeba používat ve všech případech stejné rozpětí stupnic pro hodnocení pravděpodobnosti a pro hodnocení následků. Riziko zařízení je v tomto případě vyjádřeno implicitně. Tolerovatelnost rizika není jednoznačně stanovena. Je skryta. Odvozuje se od stupnic pravděpodobnosti a následků a rozhodnutí od jaké kombinace pravděpodobnosti a následků se začíná uplatňovat nejnižší SIL.

Při plně kvantitativním hodnocení rizika se tento problém nevyskytuje. Je zaručena jednotnost způsobu hodnocení. Pokud je úroveň tolerovatelnosti rizika stanovena shodná pro všechna zařízení komplexního systému, nedochází k rozporům při určování potřebné SIL. Riziko je při kvantitativním přístupu vyjádřeno explicitně. Jednoznačně je stanoveno, zda riziko zařízení je či není tolerovatelné. To je dáno rozhodnutím o mezní hodnotě tolerovatelnosti individuálního a společenského rizika, případně ekonomického či environmentálního rizika. Jednoznačně jsou specifikovány požadavky na SIL pro dosažení tolerovatelné úrovně rizika.

# Literatura

[1] ČSN EN 61508-5:2002, *Funkční bezpečnost elektrických/elektronických/programovatelných elektronických systémů souvisejících s bezpečností – Část 5: Příklady metod určování úrovní integrity bezpečnosti.*

[2] ČSN EN 61511-x:2005, *Funkční bezpečnost. Bezpečnostní přístrojové systémy pro sektor průmyslových procesů.*

[3] ČSN EN 62061:2005, *Bezpečnost strojních zařízení – Funkční bezpečnost elektrických, elektronických a programovatelných elektronických řídicích systémů souvisejících s bezpečností.*

[4] ČSN EN ISO 13849-1:2006, *Bezpečnost strojních zařízení – Bezpečnostní části ovládacích systémů – Část 1: Všeobecné zásady pro konstrukci*.

[5] ČSN IEC 61513:2003, *Jaderné elektrárny – Systémy kontroly a řízení důležité pro bezpečnost – Všeobecné požadavky na systémy*.

[6] ČSN EN 50129:2003, *Drážní zařízení - Sdělovací a zabezpečovací systémy a systémy zpracování dat - Elektronické zabezpečovací systémy*.

[7] ČSN ISO 31000:2010, *Management rizik – Principy a směrnice*.

[8] ČSN IEC 61882:2002, *Studie nebezpečí a provozuschopnosti (studie HAZOP) – Pokyn k použití*.

**Případové studie realizace projektů spolehlivosti**
Sborník přednášek, vydán Českou společností pro jakost
Kolektiv autorů
Rok vydání 2012
1. vydání
42 stran
Vazba brožovaná

**ISBN 978-80-02-02363-0**