Životní cyklus technologií v tunelech pozemních komunikací

Metodický pokyn představuje holistický přístup zavádění kontrolovaných procesů do systému údržby tunelů pozemních komunikací vedoucí k její optimalizaci, ve smyslu doporučení mezinárodní silniční asociace PIARC.

Eltodo a.s.

Obsah

URČENÍ METODIKY

Metodický pokyn pro sledování životnosti zařízení a systémů technologií tunelu nemá předchůdce v jiném národním dokumentu. To je také důvodem, proč obsahuje poměrně rozsáhlou teoretickou část.

Metodický pokyn poskytuje provozovatelům, správcům, pověřeným osobám, silničním správním orgánům a subjektům zodpovědným za provozování a bezpečnost tunelů pozemních komunikací základní ideu, jak systémově kontrolovat životnost technologických systémů. Na základě této metodiky, a s přihlédnutím k možnostem organizace, je možné postupně připravovat příslušnou dokumentaci pro takto organizovanou údržbu ve stávajících tunelech, resp. definovat požadavky pro zhotovitele připravovaných tunelů. Základem je nezbytný sběr událostních a poruchových dat, jejich zpracování a výsledná interpretace vedoucí k řízeným zásahům údržby

Dokument poskytuje metodologický přístup, jak by měla být údržba organizována a to i ve smyslu doporučení mezinárodní silniční organizace PIARC, která se touto problematikou intenzivně zabývá. Základní myšlenkou je, že bezchybná činnost technologií a tím i provozní bezpečnost pro uživatele tunelu souvisí s životním cyklem použitých technologií a to, že bezchybná činnost zařízení se dá prodloužit kontrolovanou a systematickou údržbou.

Vzhledem k tomu, že každý tunel je svým způsobem unikátní dílo a každý správce či provozovatel může mít specifické požadavky z hlediska provozu, není cílem tohoto dokumentu poskytnout detailní návod, ale pouze poskytnout rámcové informace a příklad, na základě kterých je možné zpracovat detailní provozní předpisy, řešící problematiku představenou v této metodice.

VŠEOBECNĚ

V posledních letech hrají aspekty životního cyklu (LC – Life Cycle) technologických systémů a zařízení stále významnější roli, protože jejich znalost umožní optimalizovat investiční náklady již ve stádiu návrhu tunelu a s tím svázané i náklady provozní. Požadavky na tuto optimalizaci souvisí úzce i se stále se zvyšujícími investicemi do bezpečnostních a dalších technologií. Podrobná znalost stavu zařízení umožní lépe organizovat preventivní i pravidelnou údržbu tunelů a tím minimalizovat škody vznikající údržbou nesystémovou. Cíle mapování životního cyklu zařízení lze shrnout do následujících bodů:

- rozhodování o investicích je často orientováno jen technicky a neberou se v úvahu provozní náklady související s životním cyklem zařízení;
- cena a složitost technologii v posledních létech roste a je nutné znát omezení takto komplexních systémů z hlediska životního cyklu;
- znalost životního cyklu pomáhá zaměřit údržbu na bezpečnostně kritická zařízení a tím zvyšovat bezpečnost pro účastníky tunelu;
- znalost procesu stárnutí systémů umožní predikovat náklady na budoucí údržbu.

Metodický pokyn „Životní cyklus technologií v tunelech pozemních komunikací“ (dále MP ZCT) dává do souvislosti stárnutí technologických systémů doprovázené zvyšujícím se počtem poruch a nutnou údržbou se zaměřením na zařízení a systémy ovlivňující bezpečnost v tunelech. Požadavky na zachování plánované bezpečnosti po celou dobu provozování tunelu jsou zakotveny v evropské direktivě 54/2004/ES, lit. [1] a v nařízení vlády NV č. 264/2009 Sb. o bezpečnostních požadavcích na tunely pozemních komunikací, lit. [2].

Tento metodický pokyn předpokládá, že čtenář je seznámen s TP98 „Technologické vybavení tunelů pozemních komunikací“, lit. [3], které stanovují zásady pro technologické vybavení tunelu pozemní komunikace a které jsou základem pro systémově sjednocenou technologii tunelů v České republice.

Dále se technologickým vybavením tunelů stručně zabývá ČSN 73 7507 „Projektování tunelů pozemních komunikací“, přičemž se v kap. 11 „Vybavení tunelu“ na TP98 odvolává s tím, že technické podmínky řeší technologické vybavení tunelu více v detailu a jsou tedy nutným doplňkem této normy.

Předkládaný MP ZCT vychází z TP154 „Provoz, správa a údržba tunelů pozemních komunikací“ (2. vydání z roku 2009), lit. [4]. V těchto TP je kapitola „Provoz, prohlídky, revize a kontroly provozuschopnosti,

údržba a oprava tunelů“, která popisuje základní principy údržby zařízení. Na rozdíl od TP154, kde jsou popsány obecné požadavky na údržbu, je zde pozornost soustředěna na získávání provozních informací o poruchách zařízení z řídicího systému jako základu pro plánování údržby zařízení a sledování životního cyklu.

POUŽITÉ ZKRATKY

CT1/2	Lokální redundantní řídicí stanice tunelu
ČSN	Česká technická norma
ISO	Mezinárodní standardizační komise
IZS	Integrovaný záchranný systém
j.p.; JP	Jízdní pruh
PDZ	Proměnné dopravní značky
PIARC	Mezinárodní silniční organizace
SCADA	Dispečerské řízení a sběr dat (Supervisory Control and Data Acqusition)
TP	Technické podmínky
ZPI	Zařízení pro provozní informace

TERMINOLOGIE Z OBLASTI TECHNOLOGIE A BEZPEČNOSTI

Vzhledem k novosti problematiky je v této kapitole vytvořen základ pro terminologii vzniklou rozšířením a úpravou terminologie z TP229 „Bezpečnost v tunelech pozemních komunikací“ (2010).

Vybrané pojmy z oblasti bezpečnosti

Analýza rizik (*Risk Analysis***):** Použití dostupných informací ke stanovení společenských, ekonomických a dalších rizik pro jednotlivce, společnost, majetek nebo životní prostředí, s ohledem na daná nebezpečí.

Poznámka: Obecně zahrnuje definici rozsahu rozboru, identifikaci nebezpečí a odhad rizik.

Bezpečnost (*Safety***):** Stav, kdy je riziko možného poškození omezeno na přijatelnou úroveň.

Bezpečnost tunelu (*Tunnel Safety***):** Bezpečnost a ochrana osob, majetku a okolí stavby; je výsledkem hodnocení rizik, zdůvodněním řešení z hlediska rizik, požárně bezpečnostního řešení stavby, řešení vlivu stavby na životní prostředí, ochranu památek, přírody a krajiny. Hodnocení bezpečnosti podléhá trvalé aktualizaci i po uvedení stavby do provozu – je podkladem pro bezpečnostní dokumentaci tunelu.

Bezpečnostní dokumentace tunelu (*Tunnel Safety Documentation***):** Jednotná a přehledná forma části projektové dokumentace řešící otázky bezpečnosti a ochrany osob, majetku a okolí stavby; Bezpečnostní dokumentace se zpracovává pro jednotlivé fáze výstavby a provozu tunelu v odpovídajícím rozsahu (viz TKP-D kapitola 7, příloha č. 5, NV 264/2009 Sb.). Bezpečnostní dokumentace má textovou i grafickou podobu a podléhá trvalé aktualizaci i po uvedení stavby do provozu.

Bezpečnostně kritický proces: je to proces, jehož dysfunkce znamená přímé ohrožení životů nebo materiální škody (nemožnost uzavření tunelu příslušnou technologií v případě požáru ohrožuje životy lidí vjíždějících do tunelu).

Bezporuchovost (*Reliability***):** Schopnost systému nebo jeho části plnit stanovené požadavky v průběhu daného časového intervalu a za stanovených podmínek.

Četnost (*Frequency***):** Počet výskytů daného jevu za časovou jednotku.

Hodnocení rizik (*Risk Evaluation***):** Postup použitý k ověřování rizik a k analýze alternativ.

Identifikace nebezpečí (*Hazard Identification***):** Postup rozpoznání nebezpečí a stanovení jeho charakteristik.

Kritický proces: je to proces, jehož dysfunkce neznamená přímé ohrožení životů nebo materiální škody, ale zvýší riziko pro účastníky provozu. Například při náhradním osvětlení a při zachování přiměřeného chování a respektování pravidel mohou řidiči tunelem bezpečně projet.

Kritická cesta: selhání či disfunkce zařízení v procesu vykonávání nějaké funkce, které může ohrozit účastníky provozu či způsobit materiální škody

Událost (*Event*): Výskyt určitého souboru okolností.

Událost nepříznivá (*Undesired Event*): Jev, který může způsobit smrtelný úraz, zranění, poškození životního prostředí nebo ekonomické ztráty.

Management bezpečnosti (*Safety Management*): Systematický postup přijatý organizacemi k dosažení a udržení stupně bezpečnosti, který plní stanovený účel.

Management rizik (*Risk Management*): Kompletní postup posouzení a řízení rizik.

Následek (*Consequence*) Možný výsledek očekávaných nebo neočekávaných jevů.

Nebezpečí (*Hazard*): Řada okolností, které mohou způsobit jevy s možnými nežádoucími následky.

Poznámka: v odborné literatuře zatím existují dva odlišné přístupy, podle kterých může nebezpečí představovat nepříznivé podmínky pro vznik nežádoucího jevu nebo přímo samotný nežádoucí jev, který však nemusí nezbytně nastat.

Obnova: je jev, spočívající v obnovení schopnosti objektu plnit po poruchovém stavu požadované funkce

Pravděpodobnost (*Probability*): Věrohodnost nebo stupeň výskytu jednotlivých jevů v daném časovém období.

- **objektivní pravděpodobnost (*Objective Probability*):** Pravděpodobnost stanovená na základě statistických dat nebo s použitím teoretických argumentů.
- **subjektivní pravděpodobnost (*Subjective Probability*):** Pravděpodobnost stanovená na základě intuice nebo zkušenosti.

Porucha: je jev spočívající v ukončení schopnosti objektu plnit požadovanou funkci. Objekt po poruše je v poruchovém stavu

Redukce rizik (*Risk Reduction*): Opatření zaměřená na snížení pravděpodobností, záporných následků spojených s uvažovaným rizikem nebo obojí.

Riziko (*Risk*): Očekávaný rozsah následků nepříznivých jevů. Zpravidla se vyjadřuje jako součin pravděpodobnosti výskytu určitého jevu a jeho nežádoucích následků.

- **individuální riziko (*Individual Risk*):** Pravděpodobnost úmrtí jedince při dané aktivitě;

  Poznámka: Hodnota individuálního rizika se zpravidla vyjadřuje za časovou jednotku (např. za 1 rok), za počet pracovních úkonů, počet ujetých kilometrů, apod.
- **přijatelné riziko (*Acceptable Risk*):** Stupeň rizika, které ještě není jednotlivcem nebo společností vnímáno jako vážné, a které tím může být považováno za referenční bod v kritériu rizik;
- **reziduální riziko (*Residual Risk*):** Riziko, které zbývá po úpravě rizika;
- **společenské riziko (*Societal Risk*):** Pravděpodobnost nebo četnost jevu *F* (zpravidla za 1 rok), při kterém počet úmrtí překročí stanovený limit *N*;
- **tolerovatelné riziko (*Tolerable Risk*):** Stupeň rizika, který jsou jedinec nebo společnosti ochotni podstoupit k zajištění určitých výhod za předpokladu, že riziko bude odpovídajícím způsobem řízeno.

  Poznámka: Tolerovatelné riziko nemusí být zanedbatelné, musí však být pod stálou kontrolou.

Řízení rizik (*Risk Control*): Aktivity zahrnující rozhodování a sledování rizik v rámci managementu rizik.

Poznámka: Může zahrnovat trvalé monitorování, opakované vyhodnocování a ověřování kritérií.

Scénář nebezpečí (*Hazard Scenario*): Pořadí možných jevů s nežádoucími následky, které mohou nastat při daném nebezpečí.

Systém (*System*): Soustava souvisejících, vzájemně závislých nebo vzájemně působících prvků s vymezenými vazbami na okolí.

Údržba (Maintenance)**:** souhrn všech technických a administrativních činností, včetně činností dozoru, zaměřených na udržení ve stavu nebo navrácení objektu do stavu, v němž bude plnit požadovanou funkci

Vnímání rizika (*Risk Perception***):** Způsob, jakým jedinec, skupina jedinců nebo organizace vnímají riziko na základě hodnot nebo obav.

Zachování rizika (*Risk Retention***):** Přijetí zátěže ztráty nebo výhody zisku z určitého rizika.

Poznámka: Zachování rizika zahrnuje přijetí rizik, která ještě nebyla identifikována a nezahrnuje úpravy související s pojištěním nebo přenesením jinými způsoby. Uplatňují se různé stupně přijetí nebo závislosti na kritériích rizik.

Zmírnění (*Mitigation***):** Omezení záporných následků určitého jevu

Životnost: je to schopnost objektu plnit požadované funkce v daných podmínkách používání a údržby do dosažení ukončení užitečného života.

Vybrané pojmy z oblasti technologického vybavení tunelů

Kabiny SOS (*Emergency Stations***):** Technické zařízení sloužící především k verbálnímu spojení s operátorem řídicího systému tunelu, mohou být v provedení kabin SOS a hlásek SOS**.**

Náhradní napájení elektrickou energií (*Emergency Power Supply***):** V případě výpadku zdroje normálního napájení elektrickou energií je tento způsob napájení zajištěn přepnutím na náhradní zdroj napájení elektrickou energií nebo zdroj (zdroje) nepřerušované dodávky elektrické energie**.**

Náhradní osvětlení tunelu (*Substitute Tunnel Lighting***):** Je zpravidla zajišťováno funkcí vybraných svítidel normálního osvětlení tunelové trouby a je součástí náhradního osvětlení tunelu.

Normální napájení elektrickou energií (*Power Supply***):** Hlavní způsob napájení komplexu silničního tunelu, zpravidla z elektroinstalační sítě ze dvou na sobě nezávislých distribučních zdrojů, z nichž každý musí mít takový výkon, aby při přerušení dodávky z jednoho zdroje byla dodávka plně zajištěna ze zdroje druhého**.**

Normální osvětlení tunelu (*Tunnel Lighting***):** Zpravidla regulované osvětlení pozemní komunikace v tunelové troubě ve standardním stavu tunelu, zajišťující osvětlení ve dne i v noci**.**

Nouzové únikové osvětlení tunelu (*Emergency Evacuation Tunnel Lighting***):** Je zajišťováno samostatnou soustavou svítidel, jejichž funkce je určena pro základní orientaci a optické vedení unikajících osob na nechráněné únikové cestě**.**

Provozní větrání tunelu (*Tunnel Ventilation***):** Větrání tunelu zajišťuje koncentraci škodlivin v ovzduší tunelu v mezích nejvyšších přípustných škodlivin, dobrou viditelnost pro průjezd vozidel odstraněním kouře a prachu, řízení rozptylu škodlivin do okolí tunelu s cílem snížení imisního zatížení okolí a snížení účinků kouře a tepla při požáru vozidel v tunelu.

Spojovací a dorozumívací vybavení (*Communication System***):** Zahrnuje prostředky pro bezdrátové spojení složek integrovaného záchranného systému a složek provozovatele, servisní (provozní) telefonické spojení, přenos rozhlasového vysílání umožňují dispečerovi provozovatele vstup do tohoto vysílání, služby operátora (operátorů) mobilních telefonů a zařízení pro provozní ozvučení v komplexu silničního tunelu.

Systém videodohledu (*Video System***):** Zabezpečuje vizuální informace především o dopravních situacích v tunelové troubě a před portály; v případě mimořádných událostí poskytuje automaticky (prostřednictvím funkcí řídicího systému) vizuální informace o lokalitách, kde jsou mimořádné situace lokalizovány.

Technologické vybavení tunelu (*Tunnel Equipment***):** Technické vybavení komplexu tunelu pozemní komunikace slouží k zvýšení bezpečnosti a ochrany zdraví účastníků provozu i pracovníků provozovatele, bezpečnosti a plynulosti provozu na pozemních komunikacích a k zabezpečení odpovídajících podmínek pro výkon obsluhy a údržby pracovníky provozovatele.

Větrání pomocných prostor tunelu (*Ventilation Area***):** Jedná se o větrání technologických a služebních prostor tunelu.

Vodní hospodářství (*Water Supply***):** Zahrnuje požární vodovod, požární nádrže, čerpací stanice, standardní zásobování pitnou vodou technologických prostor s trvalou obsluhou a systémy odpadních vod.

Zařízení bezpečnostního systému (*Safety Equipment***):** Část vybavení tunelu určená zvláště pro případy zvláštního a mimořádného stavu tunelu; je představováno prostředky pro primární zásah, prostředky pro přenos poplachových signálů a verbální (akustické) komunikace s dispečerem provozovatele, evakuační označení tunelových prostor, výstražné, informativní a bezpečnostní značení, dopravní zařízení a prostředky pro eliminaci vlivu nepříznivých klimatických podmínek.

Zařízení pro odvod kouře a tepla (*Fire Ventilation Equipment***):** Systém pro řízení odvodu kouře a tepla, který odvádí kouř a teplo, vzniklé při požáru, z objektu nebo z části objektu.

Zdroj nepřerušené dodávky elektrické energie (*Uninterrupted Source of Power Supply***):** Elektrotechnické zařízení pro nepřetržitou dodávku elektrické energie daného el. výkonu po určenou dobu.

Vybrané pojmy z oblasti provozu tunelů

Dispečer (*Operator***):** Pracovník ovládající řízení procesů automobilové dopravy nebo technologické vybavenosti tunelů.

Dopravní řád (*Traffic Instruction***):** Základní dokument o provozování dopravy v tunelu a ve vymezené části komunikačního systému, který souvisí s provozem tunelu. Stanovuje všechny varianty provozování dopravy, různé druhy jejího omezení, včetně její úplné výluky pro všechny předpokládané dopravní situace.

Havarijní plán/Krizový plán (*Emergency Plan***):** Soubor opatření pro zajištěni bezpečné a rychlé záchranné akce v tunelu, je zpracován pro všechny předpokládané typy mimořádných událostí a havárií.

Manuál pro ovládání (*Operation Instruction***):** Tato část provozní dokumentace poskytuje úplný a podrobný návod pro ovládání a řízení tunelu.

Mimořádný stav tunelu (*Emergency Operation Mode)*: Důsledek mimořádné události, která svým rozsahem resp. dopady má vliv nejen na život, zdraví a majetek účastníků silničního provozu nebo obslužného personálu, ale má také vliv na vlastní tunel a jeho širší okolí.

Pověřená osoba (*Safety Inspector***):** zajišťuje koordinaci opatření k zajištění bezpečného provozu tunelu se složkami integrovaného záchranného systému a podílí se na přípravě provozních plánů. Vykonává povinnosti specifikované v NV č. 264/2009 o bezpečnostních požadavcích na tunely pozemních komunikací delší než 500 metrů.

Provozní dokumentace (*Operation Documentation***):** Soubor všeobecně platných základních dokumentů, které upravují organizaci, vztahy a činnosti v rámci provozování tunelu, viz TP154.

Řád prohlídek, údržby, oprav, revizí a kontrol provozuschopnosti (*Inspection, Control and Maintenance Instruction***):** Stanovuje úkoly a plány kontroly, prohlídek, revizí a údržby.

Standardní stav tunelu (*Standard Operation Mode***):** Základní stav provozování tunelu, který je charakterizován bezpečným a plynulým dopravním provozem, bezproblémovou činností technologie, v tunelu nebo ve služebních prostorách se neprovádí opravy, doprava i technologie jsou v řádném stavu.

Tunelová kniha (*Tunnel Book***):** podává ucelený přehled o tunelu, jeho stavební i technologické části, rozmístění zařízení, vedení kabelů, způsobu ovládání a řízení tunelu, řády pro provádění oprav nebo údržby a také poskytuje návod, jak neustále zdokonalovat obsluhující personál.

Zvláštní stav tunelu (*Special Operation Mode*) vyskytuje se zejména při provádění údržby (plánovaného uzavření tunelu) a také pokud např. systém pracuje v mimo tolerančním pásmu, není však ohrožena bezpečnost účastníků provozu ani personálu. Jedná se typicky o případ, kdy není technologie řízena automaticky a obsluha řídí manuálně, například proměnné dopravní značky. Dále zde patří dopravní problémy, které způsobí tvorbu kongescí, popřípadě dopravní nehoda, odstavení vozidla, ztráta nákladu, apod., kdy není nutné tunel ihned uzavřít

CITOVANÉ A SOUVISEJÍCÍ PRÁVNÍ PŘEDPISY A NORMATIVNÍ DOKUMENTY

- ČSN 36 5601 „Světelná signalizační zařízení - technické a funkční požadavky. SSZ pro řízení silničního provozu. SSZ pro zvýraznění nebezpečných míst“
- ČSN 73 0875 „ Požární bezpečnost staveb. Navrhování elektrické požární signalizace“
- ČSN 73 6021 „SSZ - umístění a použití návěstidel“
- ČSN 73 6100 „Názvosloví silničních komunikací“
- ČSN 73 6101 „Projektování silnic a dálnic“
- ČSN 73 6110 „Projektování místních komunikací“.
- ČSN 73 7507 „Projektování tunelů pozemních komunikací“
- ČSN EN 12 899-1 „Stálé svislé dopravní značení – Část 1: Stálé dopravní značky“
- prEN 12 899-2 „Silniční zařízení – Pevné svislé dopravní značky – Prosvětlované dopravní majáčky“
- prEN 12 966-1 „Svislé dopravní značky – Proměnné dopravní značky“
- Nařízení vlády č. 11/2002 Sb. Ze dne 14. listopadu 2001, kterým se stanoví vzhled a umístění bezpečnostních značek a zavedení signálů.
- TP100 „Zásady pro orientační dopravní značení na pozemních komunikacích“, CDV, Brno, 1999
- TP141 „Zásady pro systémy proměnného dopravního značení a zařízení pro proměnné provozní informace na pozemních komunikacích“, City-Plan, Praha, 2000
- TP154 „Provoz, správa a údržba tunelů pozemních komunikací“, Eltodo EG, a.s., Praha, 2002
- TP65 „Zásady pro dopravní značení na pozemních komunikacích“, CDV, Brno, 2002
- Zákon č. 361/2000 Sb., o provozu na pozemních komunikacích
- Vyhláška 30/2001 Sb., kterou se provádějí pravidla provozu na pozemních komunikacích a úprava a řízení provozu na pozemních komunikacích
- Zákon č. 12/1997 Sb., o bezpečnosti a plynulosti provozu na pozemních komunikacích
- Zákon č. 133/1985 Sb., o požární ochraně, ve znění pozdějších předpisů
- Vyhláška 246/2001 Sb., kterou se provádějí některá ustanovení zákona o požární ochraně /vyhláška o požární prevenci/ - zpracování požárně bezpečnostního řešení stavy tunelu
- ČSN 730875 Požární bezpečnost staveb-Navrhování elektrické požární signalizace
- ČSN 342710 Předpisy pro zařízení elektrické požární signalizace
- Metodický pokyn „Technicko-ekonomické hodnocení výstavby tunelů pozemních komunikací“, MDS, 2001, zpracovatel ILF Praha
- TKP 7 „Technické kvalitativní podmínky pro dokumentaci staveb pozemních komunikací“, Pragoprojekt 1998
- NV č. 264/2009 Sb. o bezpečnostních požadavcích na tunely pozemních komunikací
- TP98 „Technologické vybavení tunelů pozemních komunikací“, Eltodo EG, Praha, 2004, ISBN 80-239-0110-9, str. 106
- TP154 „Provoz, správa a údržba tunelů pozemních komunikací“, Eltodo EG, Praha, 2009, ISBN 978-80-254-4193-0

1 ÚVOD

Životní cyklus zařízení je důležitý pojem, který nejenom souvisí s údržbou tunelů, ale velmi ovlivňuje i bezpečnostně kritické procesy v tunelu. Bezpečnostně kritickými[1] procesy rozumíme procesy, jejichž disfunkce může mít přímý vliv na zranění či životy lidí nebo na materiální škody většího rozsahu. Proto je v úvodních této metodiky diskutován pojem bezpečnostně kritických zařízení a jsou vyjmenovány

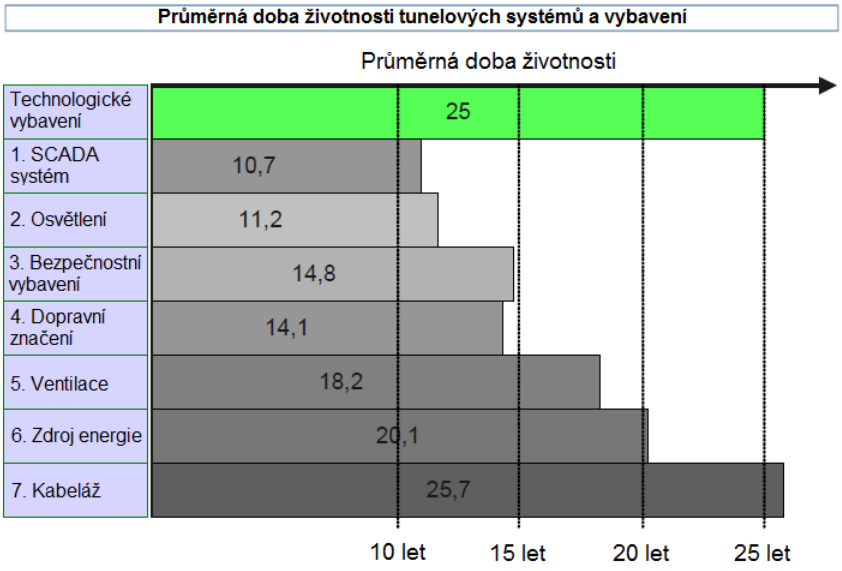
[1] tento pojem, používaný v zabezpečovací technice, je nově zaveden i do oblasti tunelových technologií

technologické systémy či zařízení, o které je nutno speciálně dbát, neboť ovlivňují bezpečnost uživatelů a leží na kritické cestě požadovaného chování zařízení tunelu.

Požadavky na údržbu souvisí s životním cyklem zařízení. Je prokázáno, že s rostoucím časem se začíná zvyšovat počet poruch daných například opotřebováním, které nakonec vedou k nutnosti dané zařízení vyměnit. V řadě případů je možné prodloužit životnost zařízení správnou údržbou a preventivními dílčími zásahy.

Současné SCADA (Supervisory Control and Data Acquisition) řídicí systémy zaznamenávají velké množství nejrůznějších dat. Metodický pokyn předkládá vzor systému pro správu údržby zařízení vycházející ze zpracovávání dat o poruchách. Ve výsledku by z těchto hodnot měly být odhadovány doby života jednotlivých zařízení. Na tomto základě by se měla plánovat nejenom údržba, ale lze i predikovat finanční nároky na obnovu zařízení.

Na ukázku lze uvést průměrné životnosti technologických tunelových systémů řady zemí zpracovaný na základě dotazníkového průzkumu organizací PIARC, lit. [5]. Ten ukázal několik zajímavých výstupů, které je vhodné dát do vztahu s našimi zkušenostmi z provozování tunelů. Problematika stárnutí a obnovy zařízení je již zcela aktuální, protože od otevření prvního, moderně vybaveného tunelu již uplynulo 15 let (Strahovský tunel, 1997), krátce poté následoval Husovický tunel v Brně a v dalších létech byly uváděny do života další tunely v intravilánu i extravilánu.



Obr. 1: Ilustrace průměrných dob života technologického vybavení tunelu, lit. [5]

Z výše uvedeného ilustrativního obrázku je patrné, že nejnižší dobu života vykazuje řídicí SCADA systém (TP98, kap. 10) a hned po něm osvětlení. Ze zkušeností je zřejmé, že potřebu výměny řídicího systému po cca 11 letech si u nás uvědomuje málokdo. Pro dopravní značení a tedy i proměnné dopravní značky vychází doba života 14 let, ventilátory ještě o čtyři roky více a samozřejmě nejvíce by měla vydržet kabeláž. Ovšem jen v případě, že se jedná o kabely nevystavené vodě, vlhku, tepelnému nebo mechanickému namáhání. Pokud nejsou dodrženy tyto podmínky je doba života násobně kratší.

2 FAKTORY OVLIVŇUJÍCÍ BEZPEČNOST PROCESŮ

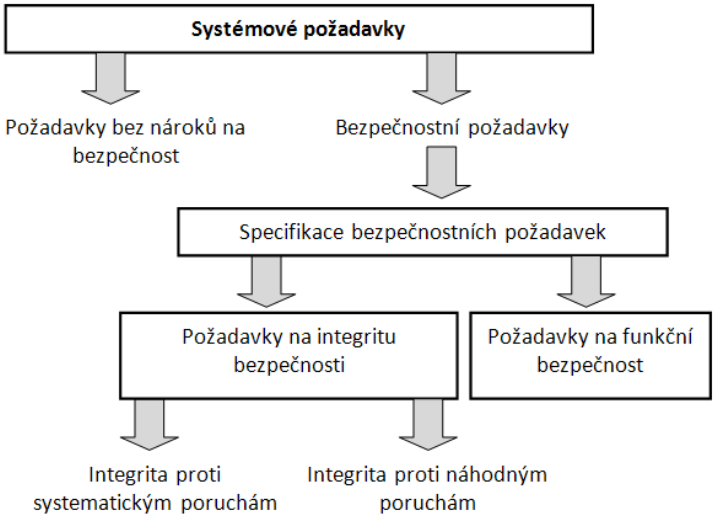
Bezpečnost (*Safety*) je v praxi hodnocení technických systémů chápaná jako jeden z atributů komplexního ukazatele dostupnosti (*Dependability*), který vyjadřuje míru, do jaké míry se uživatel může spolehnout, že systém funguje v daných podmínkách a v daném čase tak, jak bylo požadováno. Podrobnější teoretický výklad ke kap. 2 a kap. 4 „sledování životnosti zařízení“ lze nalézt v lit. [7] a [8].

Bezpečnostně kritický proces: pro tunely je nově definováno, co znamená bezpečnostně kritický proces. Je to proces, jehož dysfunkce znamená přímé ohrožení životů nebo materiální škody. Typickým příkladem je nemožnost zastavit dopravu v tunelu, resp. před portály v případě požáru v tunelu. Od bezpečně kritických systémů se očekává realizace specifické funkce zajišťující omezení rizik na předem danou minimální úroveň. V daném případě jsou na kritické cestě senzory identifikující požár, řídicí systém vykonávající předem dané funkce, ventilační systém a proměnné dopravní značky a světelné signály zamezující vjezdu dalších vozidel do prostoru požáru.

Kritický proces: dále lze definovat kategorii kritických procesů, která je specifická pro tunely pozemních komunikací. Jedná se o procesy, jejichž disfunkce může znamenat ohrožení životů nebo materiální škody, přičemž výsledek ale ovlivňuje přímo uživatel tunelu. Typickým příkladem je výpadek osvětlení v tunelu, kdy lze bez problémů z tunelu vyjet, protože vozidla mají rozsvícené reflektory a situace se podobá jízdě po neosvětlené komunikaci.

Od bezpečnostně kritických systémů se předpokládá, že splňují následující požadavky:

- požadavky na funkční bezpečnost: co má systém dělat, aby fungoval bezpečným způsobem. Tyto požadavky jsou výsledkem analýzy hrozeb (*Hazard Analysis*);
- požadavky na integritu bezpečnosti: s jakou mírou jistoty se daná bezpečnostní funkce vykoná. Ta vyplývá z procesu hodnocení rizik (*Risk Assessment*).



Obr. 2: Bezpečnostné požiadavky a integrita bezpečnosti, lit. [8]

Řízení bezpečnostně kritických procesů se od řízení standardních (bezpečnostně nekritických) procesů odlišuje výběrem prostředků, které umožní dopředu určit, jak systém zareaguje při výskytu určité kategorie poruch.

Systém je bezpečnostně kritický, pokud jeho nesprávnou činností může vzniknout některý z následujících důsledků: úmrtí, fyzické zranění, významné škody na životním prostředí, velké škody na majetku nebo nesplnění důležitého poslání. Bezpečnostně kritický systém plní funkci s předem definovanou úrovní bezpečnosti.

2.1 Poruchy systémů a zařízení

Poruchy vznikají působením různých vnitřních a vnějších vlivů, které jsou často špatně odhadnutelné a dopředu se obtížně stanovují. Proto mají poruchy vybraných zařízení a systémů v souvislosti se specifickými procesy v tunelu velký význam.

Z hlediska důsledků je možné poruchy rozdělit na:

- kritické (nebezpečné): vyvolávající poruchový stav, o kterém lze usuzovat, že může způsobit ohrožení osob, značné materiální ztráty nebo může mít jiné nepřijatelné důsledky. V řadě případů nemusí nastat nebezpečný důsledek hned při výskytu poruchy, ale nastane v souvislosti s dalšími provozními okolnostmi (porucha zákazové značky B1 „Zákaz vjezdu všech vozidel“ na vjezdu tunelu se v důsledcích projeví až při požáru nebo jiné nebezpečné situaci v tunelu);
- nekritické: vyvolávající poruchový stav, o kterém lze usuzovat, že nemůže způsobit ohrožení osob, značné materiální ztráty a nemá jiné nepřijatelné důsledky. Dále lze rozlišit:
  - závažné poruchové stavy, které ovlivňují důležité funkce zařízení;
  - nezávažné poruchové stavy, které neovlivňují žádnou zásadní funkci.

Z hlediska toho, zda lze předpokládat, že porucha vznikne, se dělí poruchy na:

- odhadnutelné: jde o poruchy, u kterých se pravděpodobnost výskytu pohybuje nad předem definovanou hodnotou;
- neodhadnutelné: jde o poruchy, u kterých se pravděpodobnost výskytu pohybuje pod předem definovanou hodnotou.

Z hlediska příčin, které poruchy vyvolaly lze mluvit o poruchách:

- konstrukčních: – způsobených nesprávným návrhem, projektem nebo konstrukcí objektu;
- výrobních: způsobené neshodou výroby od stanovených výrobních postupů
- poruchách z poddimenzování: způsobených poddimenzováním prvků, když je vystavený námaze;
- poruchy z nesprávného používání: způsobené vyšším zatěžováním, než které je přípustné;
- poruchy vyvolané nesprávným zacházením: způsobené nerespektováním předepsaných postupů při provozování, obsluze a údržbě;
- poruchy vyvolané stárnutím nebo opotřebením: způsobené v důsledku vnitřních procesů u zařízení;
- poruchy vlivem okolí: způsobené nepředpokládanými změnami klimatických, mechanických, elektrických podmínek, ale i vlivem působení jiných systémů; tyto poruchy mohou mít i dočasný účinek (rušení).

Z hlediska výše uvedeného výčtu jsou v průběhu životnosti tunelu důležité poruchy kategorie f), tedy stárnutí související s životním cyklem zařízení a nelze ani vyloučit poruchy způsobené změnou vnějších, například klimatických, podmínek – kategorie g). Poruchy, které byly do systému zaneseny při jeho návrhu, jsou obvykle odstraněny během komplexních zkoušek či v rámci zkušebního provozu.

Podle změny parametrů systému v závislosti na čase lze rozdělit poruchy na:

- náhlé: což jsou poruchy vznikající zpravidla bez předem zjištěné příčiny a způsobují skokovou změnu některého/některých parametrů systému;
- postupné: které se projevují postupnou změnou některého/některých parametrů systému.

Podle stupňů narušení funkčností systému rozeznáváme poruchy:

- úplné: porucha způsobuje neschopnost systému plnit projektované funkčnosti a trvá až do odstranění vnějším zásahem;

- občasné: pokud porucha vznikne, trvá po omezenou dobu a zaniká bez vnějšího zásahu; způsobuje krátkodobou ztrátu provozuschopnosti;
- částečné: hodnota jednoho nebo více parametrů je mimo toleranční pole, ale jejich výskyt neznemožňuje používání systému; porucha zabraňuje plnit jen některé funkce;
- přerušované: opakovaně vznikající občasná porucha jednoho a stále stejného charakteru.

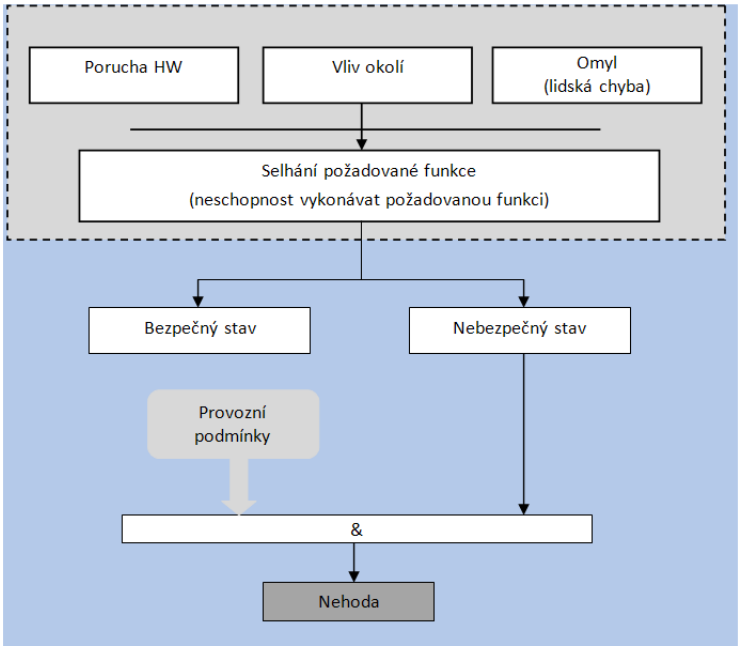
Podle vztahu k jiným poruchám rozlišujeme poruchy:

- závislé: jejich vznik souvisí s poruchami jiných částí systému a vznikají v důsledku jiné poruchy systému;
- nezávislé: jejich vznik nesouvisí s poruchami jiných částí systému a nevznikají v důsledku jiné poruchy systému

Návrh tunelových systémů je vyznačen významnou snahou o předcházení poruchám a snahou o omezení jejich významu, pokud se vyskytnou. Z toho důvodu je trojnásobně zálohováno napájení tunelu, všechny počítačové okruhy jsou zdvojovány apod. Slabšími místy jsou jednotlivá koncová zařízení vykonávající zásadní funkce z hlediska koncových uživatelů.

Aby se dalo účinně předcházet poruchám, nebo negovat jejich důsledky je třeba odhalit, kde a jaké poruchy se mohou vyskytovat a jaké jsou příčiny a důsledky jejich vzniku

Na Obr. 3 je sestavený logický model, ve kterém je naznačen proces přechodu od příčin vzniku poruchového stavu až k nehodě.



Obr. 3: Model přechodu od příčin vzniku poruchového stavu k nehodě, lit. [8]

2.2 Předcházení poruchám

Předcházet poruchám znamená včas odhalit poruchy, které se dají odhalit a vhodnými organizačními nebo funkčními prostředky je možné tyto poruchy odstranit. Předcházet poruchám je možné ve všech fázích životního cyklu systému:

- ve fázi konceptu systému;
- ve fázi návrhu a vývoje systému;
- ve fázi přípravy výroby a výroby systému;
- ve fázi instalace a uvádění systému do provozu (zkušební provoz);
- provozování a údržba;
- změny v systému.

Pro všechny fáze životního cyklu systému existuje soubor opatření a doporučení, která v konečném důsledku snižují pravděpodobnost vzniku poruchy v cílovém systému.

2.2.1 Zvládání poruch

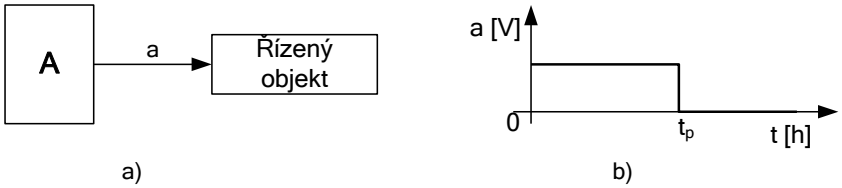
Opatření na předcházení poruch nedokážou úplně vyloučit možnost vzniku poruchy v systému či zařízení, na který byly aplikovány. Z tohoto důvodu musí systém obsahovat mechanizmus (příp. mechanizmy), pomocí kterého bude možné včas odhalit vzniklou poruchu a uvést systém či zařízení do předem definovaného bezpečného stavu. Tento stav systému je možné dosáhnout různými způsoby:

- odpojení systému od řízeného procesu;
- odpojení pouze té části od řízeného procesu, ve které se vyskytla porucha;
- zastavení vykonávání všech funkcí systému;
- zastavení vykonávání těch funkcí, které mohou být vzniknutou poruchou ovlivněny;
- omezení rozsahu zpracovaných informací pouze na informace, které mohou být zpracovány bezpečně.

Po přechodu systému do bezpečného stavu je nutné odstranit poruchu, která tento stav vyvolala, až potom je možné uvést systém do stavu, ve kterém bude vykonávat specifikované funkce. Systém nesmí tento stav opustit samovolně, ale proces musí být řízený.

Existují tři hlavní techniky zvládání poruch. Na dosažení vlastností fail-safe je možné je použít samostatně nebo je vhodně kombinovat. Z hlediska rozsahu této problematiky je uveden pouze princip jejich činnosti.

2.2.1.1 Technika vlastní bezpečnosti systému



Obr. 4 a) Struktura systému s vlastní bezpečností. b) Reakce systému na poruchu, lit. [8]

Technika vlastní bezpečnosti systému se realizuje jen s pomocí jedné funkční jednotky (Obr. 4). V takovémto systému je možné použít pouze takové stavební prvky, jejichž každá uvažovaná porucha se projeví přechodem systému do bezpečného stavu (obvykle elektricky pasivního, tj. s nulovým výstupním napětím jednotky *A*). Prvky s popsanou vlastností se nazývají prvky s asymetrickým projevem poruch. Reakce systému na poruchu se projeví zánikem povolujícího signálu řídicí jednotky *A* v okamžiku vzniku poruchy t_p.

2.2.1.2 Redundance a metody zálohování systémů

V tunelových systémech se používají metody redundance a zálohování v převážné míře. Formy realizace zálohy lze třídit několika různými způsoby. Každý z nich zdůrazňuje jinou vlastnost, takže i získané rozdělení je vhodné pro jiný účel. Použitá kritéria jsou do značné míry nezávislá, takže se jich může uplatnit několik současně. Popisovaná kritéria třídění typů zálohy budou postupně: použité prostředky, stupeň využití zálohy v čase, úroveň využití zálohy, vztah záložního a zálohovaného prvku a funkce zálohy.

Prostředky používané při realizaci zálohy zahrnují tyto systémové zdroje:

- technické vybavení (hardware);
- programové vybavení (software);
- informace;
- čas.

Tyto prostředky nikdy nelze beze zbytku oddělit, protože použití jednoho obvykle implikuje též použití některých dalších. Při malém zjednodušení lze tvrdit, že technické a programové vybavení představují základní formy zálohy, zatímco nadbytečné informace a nadbytečný čas spotřebovaný během výpočtu jsou v podstatě důsledky jejich použití.

Nadbytečné technické vybavení, označované též jako obvodová nebo prostorová záloha, představuje bezesporu nejznámější a nejpoužívanější formu zálohování. Do této kategorie patří např. záložní součástky, spoje, obvody a celé funkční bloky. Pro nadbytečné technické vybavení je charakteristický růst nákladů, rozměrů systému, váhy a často i spotřeby energie.

2.2.1.3 Stupeň využití zálohy v čase

Podle toho, do jaké míry jsou záložní prostředky využívány v čase, rozlišujeme obvykle dva typy zálohy, a to statickou a dynamickou. Statická záloha pracuje nepřetržitě po celou dobu funkce systému a je trvale připojena na vstupy a výstupy systému. Proto se tento typ zálohy označuje též jako záloha bez přepínání. Její hlavní výhodou je schopnost maskovat poruchu a nepřipustit šíření chyby na výstup systému. Navíc je způsob připojení záložního prvku do systému velmi jednoduchý, takže odpadá přepínač, který je potenciálním zdrojem nespolehlivosti a vyžaduje složité řízení. Proto lze statickou zálohu využít na libovolné úrovni počínaje jednotlivými součástkami a konče komplexními systémy. V tunelových systémech se takto zálohují řídicí počítače.

Hlavní nevýhodou statické zálohy je dodatečná spotřeba energie (všechny prvky musí být trvale připojeny na napájení) a malá hodnota střední doby bezporuchového provozu, protože všechny prvky jsou trvale zatíženy a opotřebovávají se stejně rychle.

Dynamická záloha se naproti tomu začíná využívat teprve tehdy, když je to nutné, tedy po poruše některé jiné části systému. Připojuje se prostřednictvím přepínače, a proto se označuje též jako záloha s přepínáním. Její hlavní výhodou je možnost dosáhnout vyšší hodnoty střední doby bezporuchového provozu a nižší spotřeby energie než u statické zálohy, protože dynamickou zálohu lze částečně nebo zcela odpojit od napájení. Typickým příkladem aplikace v tunelu je přechod z napájení sítě na napájení z agregátů.

Hlavní nevýhodou dynamické zálohy je nebezpečí, že během přepínání ze základního prvku na záložní dojde k dočasnému výpadku signálu na výstupu systému, nebo dokonce, že se po nějakou dobu bude na výstupu objevovat chybný signál. Vzhledem k tomu, že přepínač bývá poměrně složitý a navíc vyžaduje složité řízení, používá se dynamická záloha pouze na vyšších systémových úrovních, protože teprve tam lze zaručit, že přepínač bude podstatně jednodušší, než přepínaný prvek.

2.2.1.4 Úroveň využití zálohy

Úroveň, na níž je záloha využita, má vliv na cenu a složitost výsledného systému (čím větší celky zálohujeme, tím menší je objem pomocných obvodů a tím jednodušší je také struktura řídicího podsystému) a v neposlední řadě i na účinnost zálohy, tedy na počet a typ poruch, ze kterých se systém dokáže zotavit. Tuto úroveň lze popsat např. pomocí velikosti bloku, který je jako celek zálohován, tedy názvy zálohovaných konstrukčních jednotek, jako jsou součástky, montážní uzly, funkční bloky, systémy,

apod. Takovéto označení úrovní však není vždy zcela jednoznačné. Proto je někdy účelnější charakterizovat úroveň zálohy relativně, tedy na základě vztahu velikosti zálohovaného a záložního prvku.

Tento vztah může být v podstatě dvojí: buď se k existující (zálohované) jednotce přidá jedna nebo několik záložních jednotek, schopných převzít její funkci v případě potřeby, nebo se provedou konstrukční změny v jednotce, kterou je třeba zálohovat. Popsaný rozdíl je ovšem ve skutečnosti jen výsledkem odlišného pohledu na tentýž jev, protože konstrukční změna na určité úrovni (např. vybavení paměti samo-opravným kódem) může být chápána jako přidání shodných jednotek (paměťových jednotek) na nižší úrovni.

2.2.1.5 Vztah záložního a zálohovaného prvku

Podle vzájemného vztahu záložního a zálohovaného prvku můžeme zálohu dále třídit na konfigurační a funkční. Jako konfigurační (též masivní) záloha se označuje případ, kdy zálohovaný prvek i všechny záložní prvky jsou přesně stejného typu. Výhodou takového řešení je koncepční jednoduchost, protože určitý prvek stačí vyrobit nebo nakoupit v několika exemplářích a ty pak začlenit do systému namísto jednoho. Proto se s tímto druhem zálohy setkáváme v praxi velmi často, např. při zdvojování procesorů, funkčních bloků, přídavných zařízení, nebo celých počítačů.

Funkční záloha vznikne tak, že k zálohovanému prvku určitého typu přidáme záložní prvek nebo prvky jiného typu. Podmínkou použitelnosti takového typu zálohy je to, že všechny použité prvky musejí být schopny vykonávat stejnou, nebo alespoň podobnou funkci. Konstrukčně odlišné jednotky mají také různé technické parametry, takže při přepnutí na zálohu často dochází k degradaci výkonnosti systému.

2.2.2 Funkce zálohy

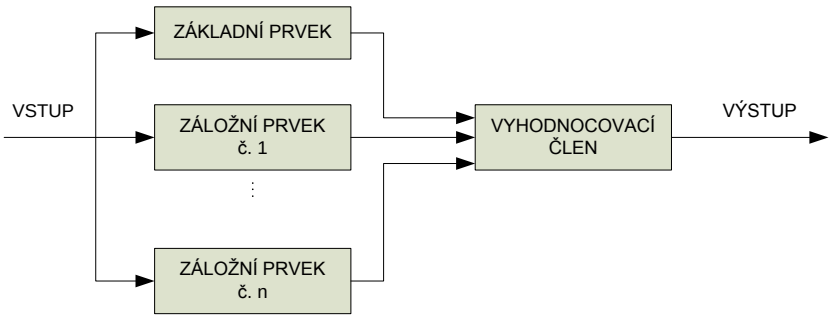
Podle toho, jak složitě má záloha reagovat na poruchu, lze specifikovat tyto tři funkce zálohy:

- detekce poruchy;
- maskování poruchy;
- zotavení po poruše.

Základním předpokladem správné reakce systému na poruchu je její detekce. Maskování poruchy je velmi dokonalý způsob využití zálohy pro zlepšení spolehlivosti systému, protože při něm se porucha vůbec nemůže projevit navenek. V obecném případě lze pro tento účel použít kterýkoli samo opravný kód, nejčastěji se maskování provádí majoritní funkcí. Zotavení po poruše je poměrně složitý sled úkonů, jehož úkolem je návrat systému do provozuschopného stavu.

2.2.2.1 Statická záloha

Z hlediska vztahu mezi zálohovaným a záložním prvkem převládají při aplikaci statické zálohy dvě varianty: konfigurační záloha (přidání stejného prvku) a konstrukční změny uvnitř prvku. Typická struktura systému s konfigurační statickou zálohou je na Obr. 5. Pro tento způsob spojení základního prvku se záložním je charakteristické, že vyhodnocovací člen je velmi jednoduchý, takže prakticky nevnáší do systému žádnou další nespolehlivost. Prvky použité jako záložní jsou stejného typu jako zálohovaný takže často vzniká symetrické zapojení, v němž nelze jednoznačně rozhodnout, který prvek je zálohovaný a který záložní. V případě napájení v tunelu se používá dvou přívodů z nezávislých rozvoden (stejný typ zálohy) a dále zálohování agregátem a UPS.

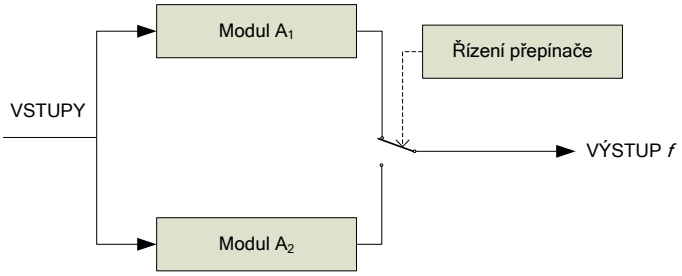


Obr. 5: Princip konfigurační statické zálohy: takto je zálohováno napájení v tunelu, lit. [8]

2.2.2.2 Dynamická záloha - Duplexní systém

Zdvojení důležitých prvků systému je metoda zálohování, která je pro svou jednoduchost velmi oblíbená. Z její jednoduchosti však vyplývají též některé nedostatky, které vymezují oblast její použitelnosti. Duplexní systém totiž nemůže současně využít výstupů obou prvků. Nelze tedy dosáhnout maskování chyby a řízená soustava je ohrožena chybou nebo výpadkem řídicího signálu během přepínání na záložní prvek.

Pro detekci chyb v základním prvku se používají dvě hlavní metody: pravidelné srovnávání výsledků se záložním prvkem nebo průběžná kontrola zabezpečeným kódem. Je-li záložní prvek odlehčený nebo nezatížený, lze samozřejmě použít pouze kontrolu zabezpečeným kódem, protože žádné kontrolní výsledky nejsou k dispozici. Pokud naopak v duplexním systému používáme zatíženou zálohu (což je nejčastější případ), můžeme volit mezi oběma variantami detekce chyb, případně je kombinovat.



Obr. 6: Blokové schéma duplexního systému, lit. [8]

2.3 Bezporuchovost tunelových systémů

Pokud se hovoří, že systém je bezpečný, neznamená to absolutní bezpečnost, ale úroveň bezpečnosti, která byla předem pro systém stanovena. Hlavním cílem řízení bezpečnostně kritického procesu je udržení bezpečného stavu po celou dobu jeho života.

V případě řídicích procesů realizovaných v tunelu to znamená například to, že se musí zajistit zabránění vjezdu vozidel do tunelu v případě požáru. Vzhledem k mechanickým komponentám proměnných dopravních značek nelze zajistit absolutní bezpečnost, tu ale nelze zajistit prakticky u žádného zařízení. Proto musí existovat i jiná možnost, která zabrání vjezdu do tunelu. Mohou to být například dvojbarevné světelné signály umisťované na portálu a v pravidelných vzdálenostech v tunelu. V tomto případě je zálohování prováděno dvěma či více odlišnými prvky, z nichž každý má svou vlastní spolehlivost provozu, viz kap. 2.2.2.1 „Statická záloha“.

Snahou však musí být, aby zařízení ovlivňující poškození zdraví či vyvolávající materiální škody byla co nejkvalitnější a spolehlivá. Proto je nutné se zabývat fakty, které mají vliv na bezpečnost. Hlavní faktory ovlivňující bezpečnost jsou: poruchy systému, technická diagnostika systému, proces obnovy systému, míra nadbytečnosti a lidský faktor.

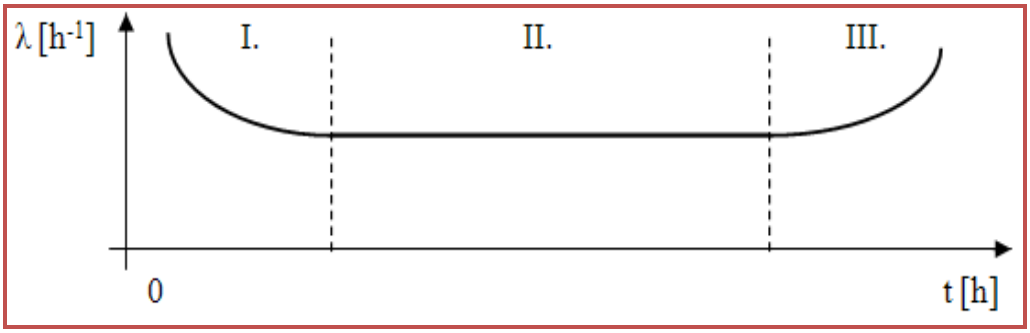
2.3.1 Bezporuchovost

Bezporuchovost (*reliability*): je chápána jako schopnost systému plnit požadovanou funkci v daných podmínkách a v daném časovém intervalu. Ukazateli bezporuchovosti jsou:

- Pravděpodobnost bezporuchového provozu $R(t1,t2)$: pravděpodobnost, že systém může plnit požadovanou funkci v daných podmínkách a v daném časovém intervalu.
- Střední čas do poruchy MTTF (*Mean time to failure*): očekávaný čas výskytu poruchy systému.
- Střední doba provozu mezi poruchami MTBF: očekávané doba provozu mezi poruchami
- Intenzita poruch $\lambda(t)$: limita poměru podmíněné pravděpodobnosti, že časový okamžik vzniku poruchy objektu T padne do časové podmínky intervalu $(t,\ t + \Delta t)$ v délce časového intervalu, kde $\Delta t \rightarrow 0$.

Intenzita poruch je časově závislá a má tvar vanové křivky, Obr. 7. Pro tuto křivku jsou charakteristické tři části:

- První část (I) se označuje jako údobí prvních poruch. Je to typické pro počáteční období fungování systému, kdy dochází k výskytu poruch daných například nekvalitní výrobou či montáží. Jejich intenzita s časem výrazně klesá. Toto období se v případě tunelů překonává zkušebním provozem, kdy mají být tyto chyby vychytány.
- Druhá část (II) se označuje jako období konstantní intenzity poruch systému a vyskytují se v něm hlavně náhodné poruchy systému. Intenzita poruch je přibližně konstantní.
- Třetí část (*III*) se označuje jako údobí poruch způsobených stárnutím anebo opotřebováním. V tomto údobí dochází k nárůstu intenzity poruch systému v důsledku přirozeného procesu stárnutí a opotřebování.



Obr. 7: Časová závislost intenzity poruch (vanová krivka)

Právě sledování intenzity poruch λ v závislosti na čase dokáže odhalit přibližování se konci životnosti nebo poskytne informace pro preventivní údržbu či obnovu dílčích částí zařízení či systémů. V následující kapitole jsou popsány technologie diagnostiky systémů.

2.3.2 Technická diagnostika systému

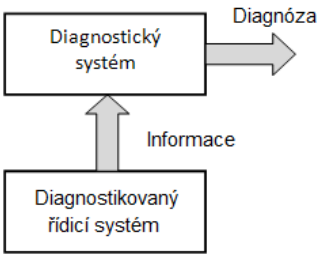
Hlavní úlohou diagnostiky je zkoumání technického stavu systému, zda vykonává předepsané funkce, a zda je vykonává korektně. V případě tunových technologií zajišťuje převážně funkční diagnostiku SCADA systém. V souvislosti s diagnostikou se:

- zkoumá technický stav systému v minulosti (technická genetika) a vyhodnocuji se historické informace o činnosti systému nebo informace vedoucí k nežádoucímu stavu systému kvůli předcházení obdobným situacím v budoucnosti (například identifikaci systematických chyb software);
- zjišťuje technický stavu systému v přítomnosti (technická diagnostika); čas detekce poruchy má vliv na pravděpodobnost výskytu nebezpečného stavu systému, rychlá a přesná lokalizace poruchy má vliv na zkrácení času opravy a zvýšení pohotovosti systému;
- předvídá technický stav systému v určitém časovém intervale v budoucnosti (technická prognostika); na základě historických a aktuálních informaci o systém je možno efektivněji organizovat proces údržby systému, což má pozitivní vliv na efektivnost provozu systému a jeho pohotovost.

Technická diagnostika může nabývat různé formy: funkční diagnostika, testovací diagnostika, periodická diagnostika, průběžná diagnostika.

2.3.2.1 Funkční diagnostika

Při tomto typu diagnostiky diagnostický systém jen analyzuje signály vytvářené činností diagnostikovaného systému (Obr. 8).



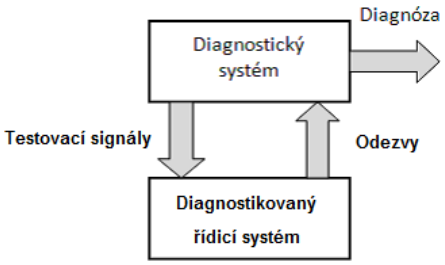
Obr. 8: Funkční diagnostika, lit. [8]

Takto jednoduchý diagnostický systém používaný v tunelech se zatím nepodrobuje analýze bezpečnosti. V případě tunelů se diagnostikuje činnost zařízení, například signálem pomocného kontaktu při výpadku napájení, ale také se diagnostikují mimotoleranční hodnoty proměnných či tzv. zabloudění programu.

2.3.2.2 Testovací diagnostika

Při testovací diagnostice diagnostický systém zavádí testovací vstupní signály do diagnostikovaného systému a analyzuje výstupní signály (Obr. 9).

Pokud je testovací diagnostika vykonávána v čase, kdy je diagnostikovaný systém mimo provoz, potom lze hovořit o servisní diagnostice. Pokud se tento diagnostický systém používá i během provozování objektu, tak jde o provozní diagnostiku a testovací signály nesmí v žádném případě ovlivnit normální činnost diagnostikovaného systému.



Obr. 9: *Testovací diagnostika, lit. [8]*

Testovací diagnostika se využívá na odhalení poruch, které se neprojeví okamžitě v činnosti diagnostikovaného systému (maskované poruchy), ale časem mohou vést k nebezpečnému stavu. V případě testovací diagnostiky musí být analýze bezpečnosti podrobeny i testovací postupy.

2.3.2.3 Periodická diagnostika

Periodická diagnostika se vykonává pravidelně v daných časových intervalech, přičemž se přeruší vykonávaní funkce diagnostikovaného systému. Pokud funkci diagnostikovaného systému není možné pravidelně přerušovat, potom se diagnostický test vykoná (celý nebo po částech), pokud vzniká časový prostor na diagnostický test nebo aspoň na jeho část. Maximální časový interval diagnostického cyklu musí být stanovený dle požadované SIL (viz dále) diagnostikovaného systému a intenzity poruch diagnostikovaného systému tak, aby pravděpodobnost poruchy mezi testy byla pod požadovanou úrovní.

2.3.2.4 Průběžná diagnostika

Průběžná diagnostika se vykonává nepřetržité sledováním a vyhodnocováním signálů, bez přerušení funkce diagnostikovaného systému. Předpokladem průběžné diagnostiky je, že zpracovávané informace obsahují určitou formu nadbytečnosti, nebo zpracování informaci probíhá s určitou formou nadbytečnosti.

Průběžná diagnostika se může realizovat jako vnější (např. komparátor při vícekanálových systémech), nebo jako vnitřní, jak hardwarová nebo softwarová kontrola signálů je součástí systému.

2.3.2.5 Diagnostické pokryti

Diagnostické pokryti vyjadřuje kvalitu testovaní systému a nejčastěji se udává jako procentuální poměr poruch, které jsou testem detekovatelné k celkovému počtu poruch.

2.4 Obnova systému

Vliv údržby zařízení je zcela zásadní, jak dokládá i výzkum v rámci PIARC („Recommendations on Management of Maintenance and Technical inspection of Road Tunnels", 2011; "Life Cycle Aspects of Tunnel Equipment", 2011). Na Obr. 10 je ukázána typická vanová křivka i s parametry charakterizujícími tři stádia doby života, viz Obr. 10:

I. Počáteční zvětšený výskyt poruch
   částečné eliminace lze docílit:

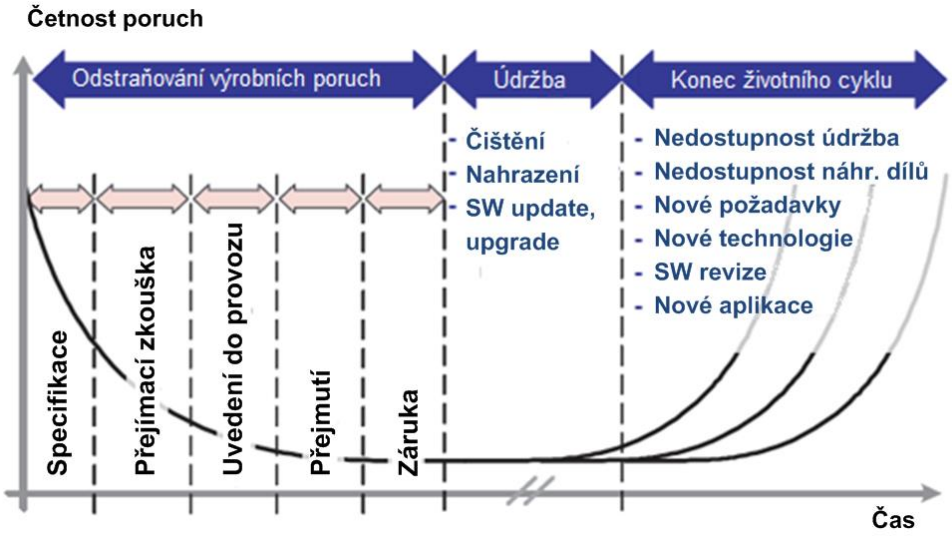
- precizní specifikací systému a zařízení
- přejímacími zkouškami, testy ve výrobních zařízeních
- komplexními zkouškami a detailním převzetím systému systémem záruk.

II. Následuje střední část, na jejíž maximální rozšíření má vliv údržba, náhrady dílčích částí, SW aktualizace a úpravy, modernizace, čištění zařízení apod.

III. Konec životnosti je charakterizován vysokým poměrem výskytu poruch, kdy už nepomáhá běžná údržba a zařízení je nutné vyměnit, či zásadně repasovat. Důvodem je ale také:

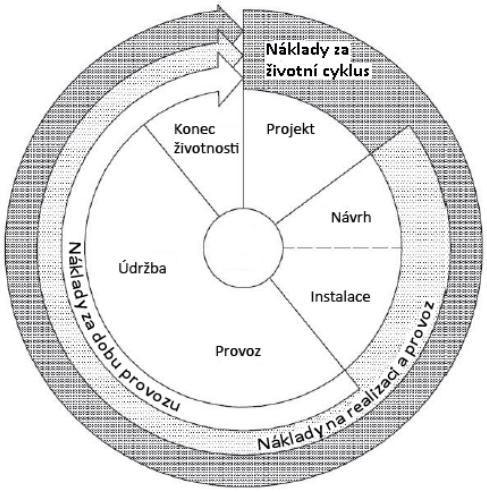
- projevuje se nedostatek náhradních dílů
- vznikají nové požadavky a předpisy
- objevují se moderní technologie
- vznikají nové SW produkty apod.

Zde platí zásada, že „zakonzervovaný" systém by neměl bránit nástupu moderních technologií.



Obr. 10: Počet poruch v závislosti na délce provozování zařízení, lit. [5];

Také další graf z dílny PIARC je velmi důležitý, protože uvádí, jak se jednotlivé složky mohou podílet na rozumné době života zařízení. V počátečním stádiu je to projekt a vlastní dodávka a dále údržba, které mají vliv a mohou ovlivnit dobu životnosti. Pokud je již zařízení instalováno, má mimořádný význam způsob jeho provozování a údržby (levá polorovina grafu – více než 50%).

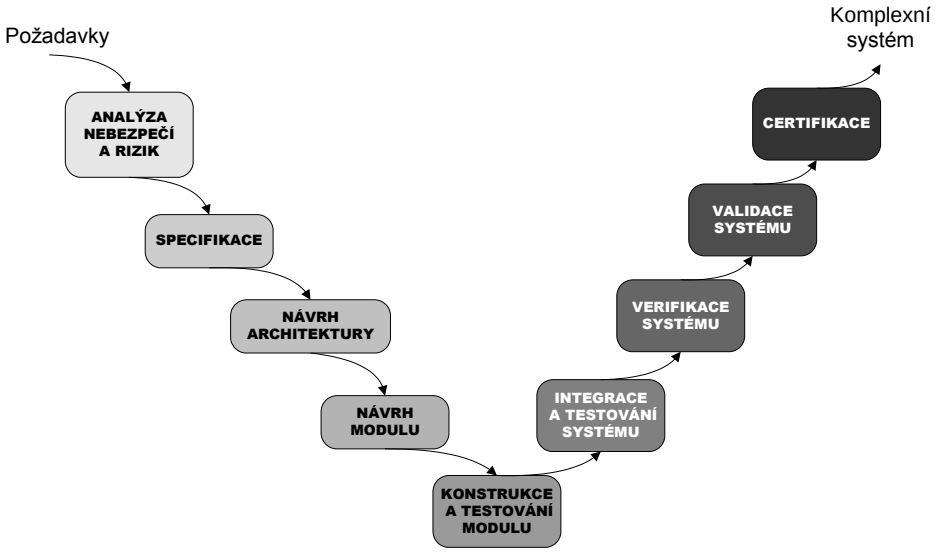


2.4.1 Technický život bezpečnostně relevantních systémů

Proces vytváření bezpečnostně relevantních systémů je obvykle dosti komplikovaný a vyžaduje i jistý čas. Tak jako všechny vyvíjené projekty i on má různé fáze, a opět jako u všech projektů, může být reprezentován schématem modelu životního cyklu, Obr. 11.

Zajímavostí tohoto modelu je jeho forma „shora-dolů“ zvýrazňující cestu návrhu (z levé strany diagramu) a „zdola-nahoru“ zvýrazňuje testování. Takovéto modely jsou pouze určitým přiblížením k vývoji systému: v praxi nejsou často v různých stupních realizovány takovým přísně sekvenčním (postupným) způsobem. Návrh často zahrnuje velké množství opakování, řada operací je vykonávána opakovaně až dokud nedostaneme uspokojivý výsledek.

Model životního cyklu na obrázku může byť aplikovaný na vývoj jakéhokoliv systému. Pro některé bezpečnostní systémy je požadovaná detailnější fáze analýzy nebezpečí a rizik za účelem určit vhodnou úroveň integrity pro systém. To potom pomůže určit návrh systému a vývojové metody pro zbytek projektu. Pro systémy s několika nebo se žádnými bezpečnostními funkcemi, formální certifikace není požadována a projekt se obvykle ukončí testem akceptace zákazníka. Velmi kritické systémy projdou procesem formální certifikace, určeným normami v daném průmyslovém odvětví.

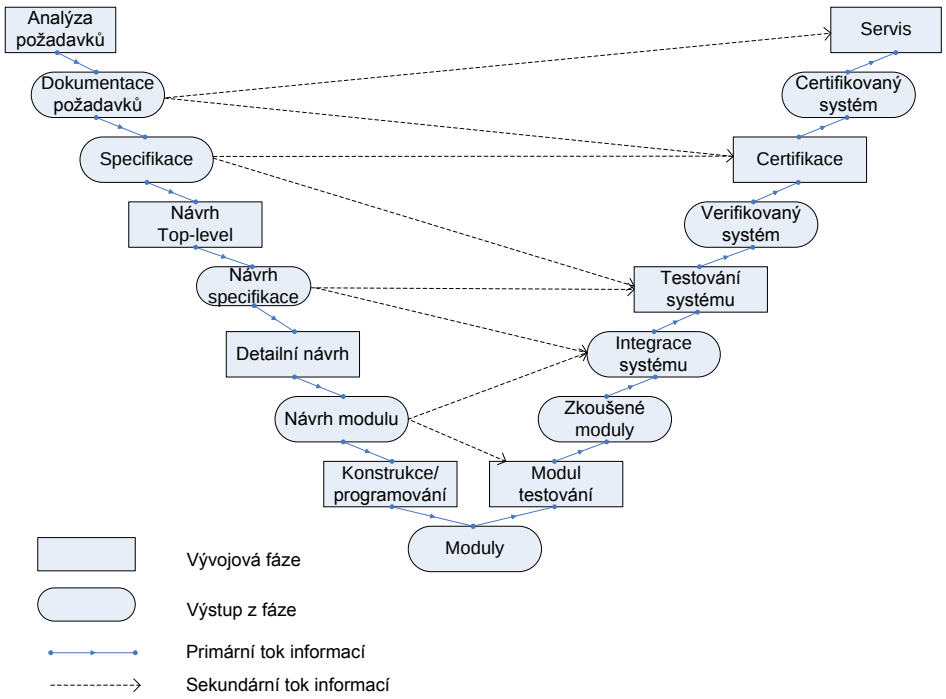


Obr. 11: Typické etapy technického života BKS, , lit. [8]

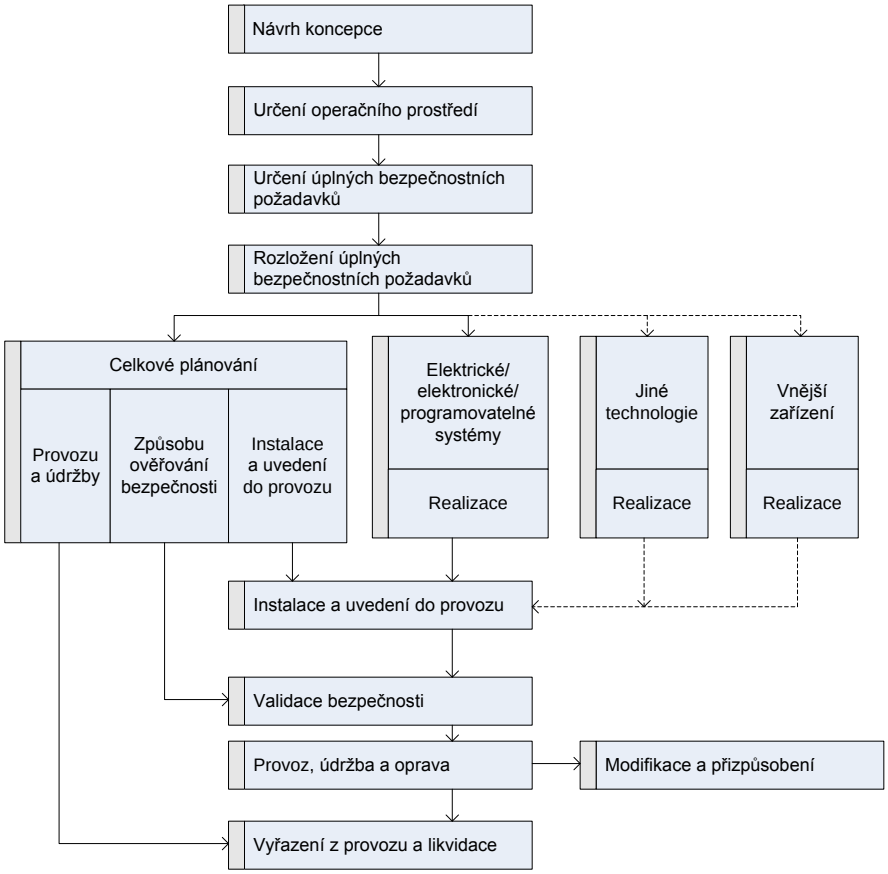
2.4.1.1 Modely životního cyklu

Široké možnosti pro reprezentaci životního cyklu vyvíjeného systému nabízí „V“ diagram. Tento model může být rozšířen k indikaci důsledků v každé fázi a též ukazuje tok informací mezi fázemi. Příklad relativně jednoduchého diagramu je zobrazen na Obr. 12. Ukazuje, že i když primární tok informací sleduje jednoduchý postup z jedné fáze do druhé, údaje z dřívějších fází jsou použity v pozdějších stupních. Například informace z fáze specifikace představují důležitou část analýzy a certifikace činnosti. Podobně, modul návrhu specifikace je testován v modulu testování a ve fázi systémové integrace.

Jiné široké použití modelu životního cyklu je dané v návrhu IEC 61 508 a znázorněné na Obr. 12. Tato norma se dotýká především těch aspektů systému, které se opírají o elektronické systémy. IEC model obsahuje všechny aspekty projektu, od představy o systému až po jeho vyřazení z provozu a likvidaci. Též zvažuje dopad modifikace v průběhu života systému. Norma popisuje podrobnou činnost v průběhu každé fáze životního cyklu a ukazuje vstupy a výstupy každé fáze.



Obr. 12: V-model technického života systémů, lit. [7]



Obr. 13: Celkový vývoj modelu životního cyklu podle IEC 61 508, lit. [7]

2.4.1.2 Bezpečnostní životní cyklus

Kromě celkového modelu životního cyklu popsaného v předcházející části, návrh IEC 61 508 též popisuje bezpečnost životního cyklu, jak je vidět na Obr. 13. Ten obsahuje všechny aspekty systémového života, od představy o systému, až po jeho vyřazení z provozu a likvidaci, též zvažuje všechny aspekty jeho realizace. Tvar životního cyklu bezpečnosti je velmi podobný celkovému životnímu cyklu systému, včetně fází týkajících se analýzy nebezpečí a rizik. Různé fáze bezpečnostního životního cyklu mohou být zmapovány v příslušných fázích životního cyklu systému, s dalšími fázemi analýzy nebezpečí a rizik, vytvářejících část celkové fáze systémových požadavků. Důležitost bezpečnosti životního cyklu je v tom, že se soustředí na ošetření bezpečnostních aspektů každé fáze vývoje procesu.

Různé fáze životného cyklu bezpečnosti jsou reprezentovány číselnými hodnotami uvnitř diagramu. Každá fáze má vstup, definovanou funkci a sdružený výstup. Výstup z jedné fáze reprezentuje vstup do další fáze. Každá fáze má přidružený soubor bezpečnostních činností. Verifikace a odhad se konají uvnitř každé fáze na zabezpečení toho, že tyto činnosti jsou vykonávány správně. Pojmově, analýza nebezpečí (hazardů) a rizik je spojená s fází 3 modelu použitého uvnitř fáze 4 na zjištění vhodné úrovně integrity pro systém. Uvnitř fáze 5 různé bezpečnostní požadavky identifikované ve fáze 4 jsou přiděleny vhodným bezpečnostně relevantním systémům. Tedy, fáze 5 zahrnuje úlohu přidělování bezpečnostních funkcí k nejvíce vhodným subsystémům, které obecně zahrnují kombinaci elektrických a neelektrických technologií. V této fáze je též úloha identifikace jiných technik, které mohou být použity na redukci rizik spojených s aplikací. Bezpečnost systému je zjišťována nejen při jeho návrhu a vývoji, ale i podle toho jak je nainstalován, používán a udržován. Z tohoto důvodu celková strategie pro uvedení do provozu, manipulaci a údržbu je zavedena do dřívějších stupňů v procesu vývoje, v čase kdy můžeme ovlivnit detailní návrh systému. Tyto činnosti zodpovídají fázi 6 a 8 v modelu. Fáze 9, 10 a 11 bezpečného životního cyklu se vztahují k návrhu a realizaci různých bezpečnostně relevantních systémů a funkcí. Diagram na Obr. 13 dělí tuto fázi do tří složek, a to fázi 9, která se zabývá bezpečnostně relevantními systémy opírajícími se o technologie elektronických systémů; 10 se zabývá bezpečnostně relevantními systémy založenými na jiných technologiích; a 11 technikami redukce externích rizik.

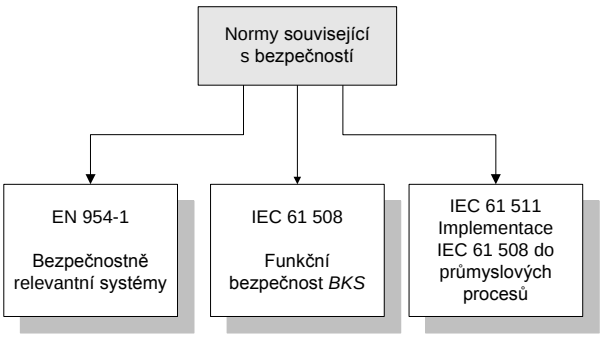
Potom nastává pro různé bezpečnostně relevantní systémy průběh instalace ve fáze 12 a kompletní systém podléhá celkové validaci ve fázi 13. Stupeň provozu a údržby života systému se skrývá ve fáze 14 a nějaká modifikace, nebo dodatečná montáž ve fáze 15. Nakonec fáze 16 se zabývá vyřazením systému z provozu a jeho likvidací. Podrobný popis jednotlivých fází bezpečnostního životního cyklu je uveden v normě IEC 61508: „*Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems (E/E/PES)*“.

2.5 Bezpečnostně kritické systémy v normách IEC a EN

V této kapitole je proveden pouze základní informace o normách, které by se potenciálně měly brát v úvahu při navrhování a provozování technologií v tunelech pozemních komunikací.

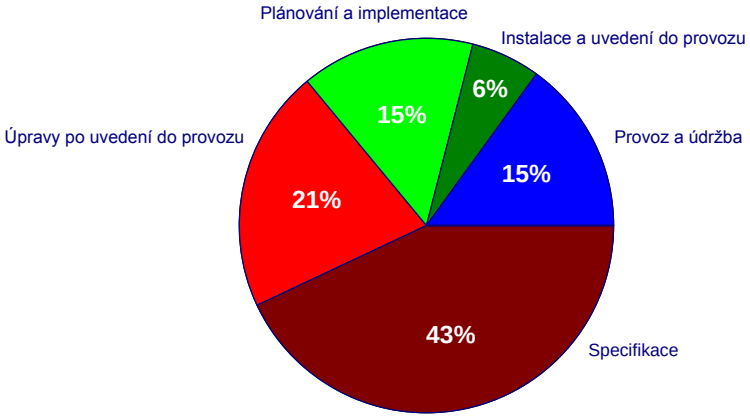
Funkce vykonávané BKS se dále nazývají „bezpečnostní funkce“. *BKS* by měl být navržen a konfigurován tak, aby byl dostatečně spolehlivý (při pohledu na chyby a důsledky) a současně vykonával funkce nezbytné k dosažení nebo udržení bezpečného stavu nebo alespoň redukci důsledků nebezpečí. Rozlišujeme dvě skupiny BKS a to ty, které používají programovatelné technologie, a ty, které nepoužívají programovatelné elektronické zařízení (používají např. elektromechanické součástky).

Hlavním důvodem tohoto rozdělení je pomoci konstruktérovi rozhodnout se, která ze dvou hlavních norem je aplikovatelná pro návrh *BKS*: IEC 61508 nebo EN 954-1. Bez ohledu na to, která norma se použije, návrh musí plně brát do úvahy úroveň redukce rizika, která se požaduje pro daný systém.



Obr. 14: Normy vztahující se na BKS, lit. [7]

Graf na Obr. 15 ilustruje příčiny 34 případů havárií technických systémů vyhodnocených nezávislou technickou komisí. Graf naznačuje, že příčiny havárií se vyskytují během celé doby života, počínaje návrhem, přes jeho realizaci, použití a modifikaci v průběhu používání. Alarmující je zjištění, že více než 44 % chyb způsobili ti, kteří měli specifikovat systém řízení nebo bezpečnostní systém, případně se měli podílet na specifikaci nebezpečných míst v technologii. Provozování, údržba a dodatečné úpravy systému tvoří více než 35 %. Je úplně běžné, že se mnohokrát pracuje s neúplnou dokumentací, k zařízení jsou někdy postavení lidé, kterým provozovatel neumožnil školení u výrobce, nebo úpravy existujícího systému byly svěřeny nekompetentní servisní společnosti.



Obr. 15: Příčiny havárií technických zařízení během doby života, lit. [7]

2.5.1 Norma IEC 61 508

Začátkem devadesátých let minulého století byla vydána norma DIN V 19 250 s návrhem analyzovat všechna rizika ve vlastním procesu i v korelaci s řídicím systémem, lit. [9]. Tuto koncepci si osvojili i tvůrci mezinárodní normy IEC 61 508, lit. [10]. Navíc vyslovili potřebu zabývat se bezpečností procesu od analýzy rizik již při návrhu bezpečného systému, péčí o systém během celé doby životnosti, až do ukončení činnosti systému, či jeho demontáž. Do nejvyšší dokonalosti, pokud lze toto slovní spojení použít, dovedli tento přístup normotvůrci z organizace IEC (*International Electrotechnical Commission*), i když ochránci životního prostředí nejsou celkem spokojeni s mírou akcentování vlivu havárií na životní prostředí. Je to především norma IEC 61 508 „*Functional Safety of Electrical/Electronic/Programmable Electronic Safety Related Systems*“. Norma má následující části:

Část 1: Obecné požadavky.

Část 2: Hardwarové požadavky.

Část 3: Softwarové požadavky.

Část 4: Definice a zkratky.

Část 5: Příklady.

Část 6: Průvodce po částech 2 a 3.

Část 7: Přehledy techniky a forem tvorby software.

Z hlediska bezpečnosti systémů lze považovat za základní části 1, 2, 3 a 4. Je však třeba poznamenat, že tyto části nejsou použitelné pro ty systémy, jejichž úroveň integrity bezpečnosti (*angl. safety integrity level* - SIL) je nižší, než nejnižší předpokládaná v normě IEC 61 508.

Je zřejmé, že výskyt poruch může mít významné negativní ekonomické důsledky. Norma je určená na specifikaci každého elektronického zařízení určeného na ochranu technologie a výrobků. Mezi typické aplikační oblasti normy IEC 61508 patří:

- systémy havarijního a nouzového vypnutí strojů a zařízení;
- požární a plynové systémy;
- řídicí systémy turbín;
- řízení plynových hořáků;
- dopravní systémy včetně železniční zabezpečovací techniky;
- automatická indikace nebezpečného nákladu jeřábů;
- ochranné systémy strojních zařízení.

Norma uvádí čtyři třídy bezpečnostních systémů SIL 1 až 4, přičemž SIL 1 reprezentuje nejnižší požadavky, SIL 4 nejvyšší. Jak jsou definovány limity pro jednotlivé SIL, ukazuje Tab. 1.

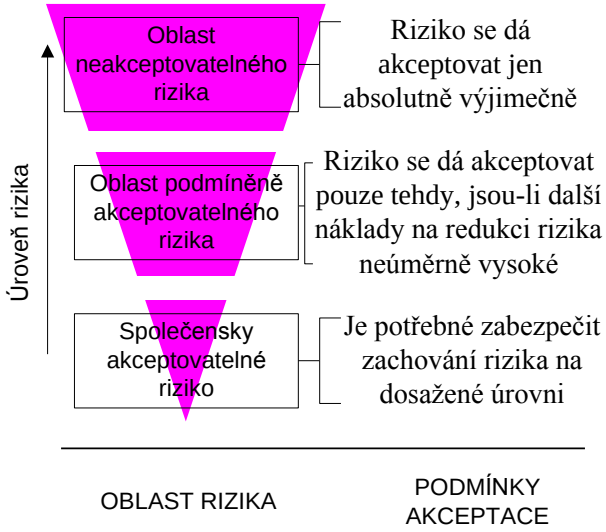
SIL	Pravděpodobnost výskytu chyb navrženého systému (nízké požadavky na způsob provozu)	Pravděpodobnost jedné nebezpečné chyby za hodinu, kontinuální provoz (vysoké požadavky na způsob provozu)
4	$[10^{-5}; 10^{-4})$	$[10^{-9}; 10^{-8})$
3	$[10^{-4}; 10^{-3})$	$[10^{-8}; 10^{-7})$
2	$[10^{-3}; 10^{-2})$	$[10^{-7}; 10^{-6})$
1	$[10^{-2}; 10^{-1})$	$[10^{-6}; 10^{-5})$

Tab. 1: Doporučené pravděpodobnosti podle IEC 61 508

Norma IEC 61 508 hovoří i o vlivu lidského činitele na výskyt nebezpečí a nebezpečných událostí už v průběhu návrhu BKS.

Ještě před vydáním IEC 61 508 se rozlišovaly tři aspekty systému bezpečnosti. První se týkal **primární bezpečnosti**, která byla zaměřena na rizika při styku se zařízením, jako je např. riziko úrazu elektrickým proudem, riziko popálení atd. Druhým je **funkční bezpečnost** a třetím je **nepřímá bezpečnost**, vyplývající z generování takových výsledků procesu, které nezpůsobí přímé následky v čase generování, ale mají dopad na další rozhodování (např. nesprávné analýzy v medicínské praxi). Již vzpomínané normy se zabývají druhým aspektem, který je vázán na bezpečnou funkci řízeného zařízení (*angl. Equipment Under Control,* EUC), což zahrnuje zařízení, stroje a aparáty na produkci, zpracování, transport, skladování atd. Už z definice je patrné, že se jedná o komplex prostředků, jejichž činnost je řízená tak, že na základě vstupních signálů se generují výstupní signály takového charakteru, aby proces probíhal požadovaným směrem. Normy uvádějí riziko EUC, které vzniká v zařízení v interakci s řídicím systémem. Toto riziko je referenční hodnotou (dá se vyjádřit číselně), která je základem pro návrh bezpečnostního systému Obr. 16.

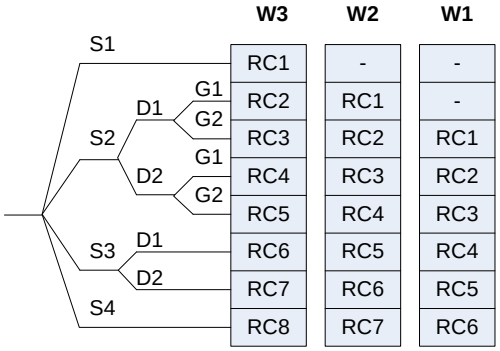
Bezpečnostní systém je určen na dosažení integrity bezpečnosti a zvýšení pravděpodobnosti, že systém ve vlastním *EUC* bude plnit bezpečnostní funkce. Kromě toho implementuje požadované bezpečnostní funkce na udržení *EUC* v bezpečném stavu.



Obr. 16: Interpretace oblastí akceptovatelnosti rizika, lit. [7]

Potlačení rizika se může odehrát na úrovni řídicího systému, jakož i pomocí jiných opatření nebo externích systémů nezávislých od EUC. Pokud se vyčerpala všechna dostupná a ekonomicky zvládnutelná opatření (což se obvykle v praxi nedosahuje až po akceptovatelnou míru rizika), zbytek musí saturovat bezpečnostní systém konstruovaný a certifikovaný podle požadavků mezinárodních norem.

Norma IEC 61 508 byla implementována do soustavy evropských norem, a následně v rámci harmonizace s evropskými normami se v roku 2002 dostala i do soustavy slovenských technických norem. Podobný proces proběhl i v České republice. Platnost všech norem, které jsou v určitém smyslu v rozporu s kmenovou normou IEC/EN 61508, jako je DIN V 19 250, DIN V 19 251, DIN VDE 0801, DIN VDE 0801/A1 se skončila k datu 1.8.2004.



Min. nutná redukce rizika	SIL
-	Bez bezpečnostních požadavků
RC1	Bez specifických bezpečnostních požadavků
RC2, RC3	1
RC4	2
RC5, RC6	3
RC7	4
RC8	E/E/PES není postačující

Důsledek, rizikový parameter
S1 drobná poranění
S2 vážná trvalá poranění 1 nebo více osob, nebo smrt jedné osoby
S3 smrt více osob
S4 smrt většího množství osob

Opakovatelnost, čas působení
D1 drobná poranění
D2 velmi často až permanentně

Možnost vyvarovat se nebezpečných událostí
G1 Je možné za určitých podmínek
G2 Téměř nemožné

Pravděpodobnost výskytu nežádoucí události
W1 velmi malá pravděpodobnost
W2 malá pravděpodobnost
W3 relativně velká pravděpodobnost

Obr. 17: Graf rizik podle DIN V 19250

2.5.2 Norma IEC 61 511

Paralelně s revizí normy IEC/EN 61 508 se dotvářela poslední ze tří částí normy IEC 61 511 „*Functional Safety; Safety Instrumented Systems for the Process Industry Sector*"[2], lit. [11] Ta je určena výhradně pro spojité výrobní procesy a na rozdíl od IEC/EN 61 508 není určena výrobcům zařízení. Nová norma přinesla mnohá objasnění a podle všeho uživatel (ať již systémový integrátor nebo koncový uživatel) dostane do ruky kvalitní materiál, který výrazně posouvá problematiku zavádění bezpečnostních systémů do praxe. Je třeba poznamenat, že ke znalosti problematiky je nevyhnutné poznat obě normy. Též je potřebné vzpomenout, že IEC 61 511 nenahrazuje normu IEC/EN 61 508. Ta je kmenovou normou platnou pro jakékoliv procesy a tvoří základ pro národní, oborové nebo specializované normy, které si mohou vytvářet různá sdružení nebo odvětví průmyslu. Kmenovou normu lze použít všude tam, kde neexistuje speciální norma pro ten který sektor. Je však potřebné připustit, že je terminologicky a konstrukcí poněkud těžkopádná. Norma IEC 61 511 používá přijatelnější terminologii. Zavádí i jiné označení pro bezpečnostní systém, tzv. *Safety Instrumented System* (SIS).

Norma se skládá ze tří částí, které se obsahově kryjí s jednotlivými částmi IEC 61508 podle následujícího uspořádání:

1.část (koresponduje s částmi 1, 2, 3, 4 a částečně i částí 7 normy IEC 61 508):

- specifikuje požadavky na architekturu systému, konfiguraci bezpečnostních funkcí, aplikační software a celkovou systémovou konfiguraci;
- popisuje funkce bezpečnostního managementu, analýzu rizika v procese a přiřazení bezpečnostních funkcí ke stanovenému SIL;
- v závěru pojednává o testech navrhnutých bezpečnostních systémů u výrobce, instalaci a uvedení do chodu.

2. část (koresponduje s částí 6 a částečně i 7):

- uvádí obecné informace o IEC 61 511, definice a zkratky;
- dává návod k aplikaci části 1 normy v šesti informativních přílohách, kterými jsou:
  - příloha A: management bezpečnostní funkce, požadavky na software, bezpečný životní cyklus;
  - příloha B: kalkulace pravděpodobnosti funkční způsobilosti bezpečnostního systému;
  - příloha C: příklad aplikace v chemickém průmyslu a typická architektura bezpečnostního systému;
  - příloha D: programovací jazyky pro bezpečnostní systém a příklady vývoje uživatelského software;
  - příloha E: příklad přístupu výrobce k vývoji bezpečnostního PLC v souladu s IEC 61 508,
  - příloha F: přehled bezpečnostních technik a prostředků ve vztahu k částem 1, 2 a 3 normy IEC 61 511.

3. část (koresponduje s částí 5 a částečně i 7): pojednává ilustračně o kvalitativních a kvantitativních metodách stanovení SIL.

Kmenová norma IEC/EN 61 508, i norma IEC 61 511 se zabývají celým životním cyklem prvků a zařízení.

2.5.3 Norma EN 954-1

Norma je zaměřená výhradně na bezpečnostně relevantní části řídicích systémů strojů a zařízení. Uvádí bezpečnostní požadavky a zásady pro návrh bezpečnostně relevantních částí řídicích systémů. Pro tyto části jsou v normě určeny kategorie a požadované bezpečnostní funkce. Uvedená doporučení se vztahují na všechny bezpečnostně relevantní části řídicích systémů bez ohledu na druh použité energie. Kategorie

[2] zmíněné normy lze najít a zakoupit na http://webstore.iec.ch

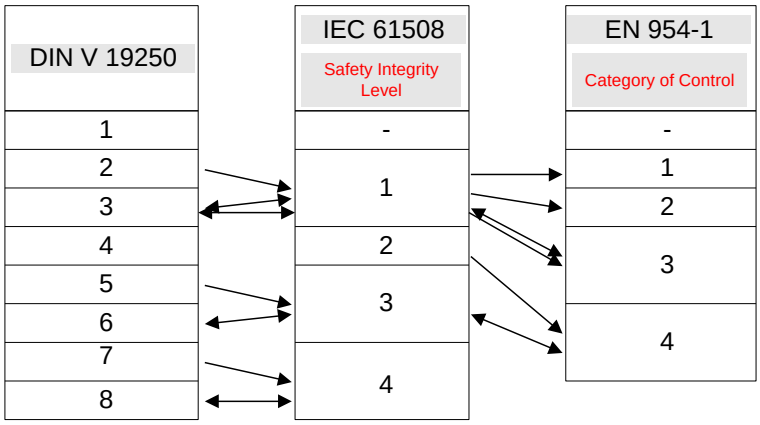
podle Tab. 2: Klasifikace bezpečnostně relevantních částí systému“ představují klasifikaci bezpečnostně relevantních částí řídicího systému s ohledem na jejich odolnost proti poruchám a též na jejich chování při výskytu poruchy.

Kat.	Požadavky (stručně)	Chování systému	Princip
B	Bezpečnostně relevantní části řídicích systémů a/nebo jejich bezpečnostní moduly a jejich prvky musí být navržené, konstruované, vybrané, instalované a vzájemně propojené v souladu s relevantními normami tak, aby byly odolné proti předpokládaným nepříznivým vlivům	Výskyt chyby může vést ke ztrátě bezpečnostní funkce.	Především výběr komponentů.
1	Požadavky jako v kategorii B. Je potřebné používat osvědčené prvky a osvědčené principy bezpečnosti.	Výskyt chyby může vést ke ztrátě bezpečnostní funkce, ale pravděpodobnost výskytu chyby je menší než v kategorii B.	
2	Požadavky jako v B spolu s aplikováním osvědčených principů bezpečnosti. Bezpečnostní funkce by měla být řídicím systémem ověřována v přiměřených intervalech	Výskyt chyby může vést ke ztrátě bezpečnostní funkce mezi dvěma následujícími kontrolami.	Především volba struktury.
3	Požadavky jako v B spolu s aplikováním osvědčených principů bezpečnosti. Bezpečnostně relevantní části by měly být navrženy tak, aby: - jednonásobné chyby libovolné části nezpůsobily ztrátu bezpečnostní funkce, - jednonásobné chyby byly detekovány, jak jen to bude možné	Po výskytu jednonásobné chyby musí byť bezpečnostní funkce zachována. Detekovaná je většina chyb, ne všechny. Seskupování nedetekovaných chyb může způsobit ztrátu bezpečnostní funkce.	
4	Požadavky jako v B spolu s aplikováním osvědčených principů bezpečnosti. Bezpečnostně relevantní části by měly být navrženy tak, aby: - jednonásobné chyby libovolné části nezpůsobily ztrátu bezpečnostní funkce, - jednonásobné chyby byly detekovány v průběhu nebo přednostně do následujícího požadavku na realizaci bezpečnostní funkce. Pokud to není možné, potom seskupování chyb nesmí vést ke ztrátě bezpečnostní funkce	Po výskytu jednonásobné chyby musí být bezpečnostní funkce zachována. Chyby jsou detekovány ve vhodném čase tak, aby se zabránilo ztrátě bezpečnostní funkce.	

Tab. 2: Klasifikace bezpečnostně relevantních částí systému

2.5.4 Úroveň integrity bezpečnosti SIL systému v normách

Při určování dosažené úrovně integrity bezpečnosti analyzovaného a/nebo navrhovaného systému je třeba respektovat filozofii relevantních norem, hlavně DIN V 19250, IEC 61508 a EN 954-1 ve vztahu k bezpečnosti (Tab. 3).



Tab. 3: Úrovně integrity bezpečnosti podle významných norem

Z porovnání hodnot z Tab. 3, která uvádí počet poruch za hodinu pro jednotlivé úrovně integrity vyplývá, že na systém se SIL 4 bude kladeno mnohem víc bezpečnostních požadavků než na SIL 1 a naopak. Přitom je třeba si uvědomit, že systémy s nejvyšší úrovní obsahují nejvíce bezpečnostních požadavků a funkcí a proto jejich řízení je pomalejší a ne tak efektivní, na druhé straně je však velmi bezpečné. Naopak, systémy s nejnižší úrovní jsou rychlejší, neboť neobsahují tolik bezpečnostních požadavků na systém a proto riziko, které se v systému se SIL 4 považuje za nebezpečné, je v jiném systému se SIL 2 ještě akceptovatelné. Tato úroveň se určuje na základě výsledků analýzy nebezpečí a rizik. Jestliže si ale uvědomíme riziko, s ohledem na které byl daný systém navržen v souladu se SIL 4, může tomuto požadavku vyhovět řekněme ve třetině svého technického života a ve zbytku bude vyhovovat už jen SIL 2. Proto pokud bychom dokázali identifikovat, že dané riziko se může objevit pouze v určité části celého života systému, mohl by tento systém být navržen tak, že bude pracovat jako systém s úrovní SIL 2 a jen v té části, kde se může objevit vyšší riziko, bude pracovat jako SIL4. Tak by se dalo zrychlit a zefektivnit řízení daného systému. Na to by bylo potřebné přesně definovat rozdíly mezi jednotlivými úrovněmi bezpečnosti podle relevantních norem a přesně analyzovat konkrétní systém, zda může pracovat s jednou úrovní integrity bezpečnosti v jednom časovém úseku svého života a s jinou ve zbývajícím úseku svého života.

3 SCÉNÁŘE PROVOZOVÁNÍ TUNELU POZEMNÍ KOMUNIKACE

Tato kapitola metodického pokynu poskytuje přehled o tom, které kategorie scénářů provozování tunelu mohou být považovány za kritické. Pojem kritický či bezpečnostně-kritický se v tomto případě vztahuje k uživatelům tunelu, tedy řidičům a dalším účastníkům silničního provozu. Neberou se v úvahu havárie, kdy třeba zborcení tunelu díky geotechnickým podmínkám vyvolá ztráty na povrchu.

V technických podmínkách TP154 „Provoz, správa a údržba tunelů pozemních komunikací“ jsou detailně popsány zvláštní a mimořádné stavy v tunelu i v předportálových úsecích a to z hlediska dopravních situací a i z hlediska výpadku technologií.

Úvaha, zda jsou vůbec v tunelu zařízení, jejichž výpadek může přímo ohrozit životy lidí nebo vyvolat značné materiálové škody, jako například porucha zařízení v atomové elektrárně vedoucí k její explozi, vede k závěru, že taková zařízení či systémy v tunelu nejsou.

Tunel je součástí pozemní komunikace a pro řidiče platí pravidla silničního provozu i při jízdě tunelem. Jinak řečeno, při výpadku základního i nouzového osvětlení se zvyšuje sice riziko excesů, ale vozidlo by mělo tunelem bezpečně projet s rozsvícenými reflektory. Technologická zařízení tunelu, respektive jejich dysfunkce obvykle samy nevyvolávají kritické situace, které by přímo způsobovaly ztráty na životech účastníků, ale jejich poruchy mohou být potenciálně zdrojem značného nebezpečí.

V případě požáru, hromadné nehody či exploze je situace jiná. Pokud selžou zařízení blokující vjezd do tunelu, jsou uživatelé tunelu, pokračující v jízdě k události, vystaveni bezprostřednímu ohrožení života, právě díky této poruše. V tomto smyslu je nutné přiřadit vybraná zařízení ovládající dopravu v tunelu do kategorie bezpečnostně-kritických. Stejně tak, pokud selže identifikace požáru, informování uživatelů o bezprostředním nebezpečí a třeba i ventilace, může to způsobit přímé ohrožení života.

3.1 Kategorie rizikových událostí

V následující tabulce jsou scénáře událostí uspořádány do kategorií: Nehoda a Požár. Vzhledem k zaměření metodického pokynu na kritické a bezpečnostně kritické procesy je sledovanou kategorií pouze nehoda a požár. Expozice toxickými nebo jinak nebezpečnými látkami, či teroristické napadení si vyžaduje speciální přístupy, které musí být zapracovány do provozní dokumentace dle doporučení v TP154. Další a detailnější úvahy o přepravě nebezpečného nákladu lze najít v dokumentech PIARC a nejsou také předmětem následujících úvah.

Při analýze situací, které mají vliv na bezpečnost pro účastníky provozu na pozemních komunikacích, jsou v následující Tab. 4 „Dělení události typu „nehoda“ a „požár“ brány v potaz excesy související s dopravním provozem, v Tab. 5: Příklad matice zařízení, jejichž výpadek může způsobovat nebezpečné situace pro účastníky provozu“ navíc přistupuje i hodnocení události vyplývající z různých kombinací výpadku technologií. Následující úvahy jsou omezeny na vlastní prostor tunelových trub. Jedná se tedy pouze o stavy „Zvláštní stav bez/s účastí dopravní policie“ a „Mimořádné stavy“ ve smyslu TP154.

V následující tabulce jsou děleny výše uvedené kategorie dle scénářů/událostí, které mohou v tunelu nastat. Zároveň je popsáno riziko, který tento stav přináší a bezpečnostní funkce, kterých se to týká.

Kategorie	Název události	Důsledky	Riziko	Bezpečnostní zařízení a funkce
„Nehoda“	**Zastavení vozidla**		ohrožení dalších účastníků ⇒ vyvolané nehody s možností poškození zdraví	Rychlá identifikace události (senzory, videodetekce …) Informování řidičů (RDS-TMC, informační displeje …) Omezení/zastavení provozu (dopravní systém) Zajištění a spolupráce při odtahu (dispečeři, CCTV)
	Kolize bez zranění	Materiální škody: a) pro účastníka b) pro stavbu, zařízení	- vyvolané nehody - riziko vzniku požáru při nehodě - zastavení/omezení provozu	Rychlá identifikace události (senzory, videodetekce …) Informování řidičů (RDS-TMC, informační displeje …) Omezení/zastavení provozu (dopravní systém) Zajištění a spolupráce s IZS při likvidaci nehody (dispečeři, manuální řízení, CCTV)
	Kolize se zraněním, úmrtí	Škody na zdraví Materiální škody: a) pro účastníka b) pro stavbu, zařízení	- vyvolané nehody - riziko vzniku požáru při nehodě - zastavení/omezení provozu	Rychlá identifikace události (senzory, videodetekce …) Informování řidičů (RDS-TMC, informační displeje …) Omezení/zastavení provozu (dopravní systém) Zajištění a spolupráce s ITS při likvidaci nehody (dispečeři, manuální řízení, CCTV)
„Požár“	**Požár malého[3] rozsahu**	Škody na zařízení tunelu a škody na majetku účastníka Ohrožení zdraví účastníka	- vyvolané nehody - riziko rozšíření požáru - zastavení/omezení provozu	Rychlá identifikace požáru (videodetekce, senzory kouře, SOS skříně …) On-site hasební zásah (ruční hasící přístroje) Zajištění úniku osob (únikové východy, označení, osvětlení) Informování řidičů (RDS-TMC, informační displeje …) Zastavení provozu (dopravní systém) Zajištění a spolupráce s IZS při likvidaci nehody (dispečeři, manuální řízení, CCTV)
	Požár do 5 MW **Požár do 20 MW**	Škody na zdraví (teplem, kouřem) Úmrtí vlivem požáru a zplodin Materiální škody na stavbě a zařízení	- riziko rozšíření požáru - vyvolané nehody - zastavení provozu na delší dobu	Rychlá identifikace požáru (liniový hlásič, senzory kouře, SOS skříně …) On-site hasební zásah (ruční hasící přístroje) Zajištění úniku osob (únikové východy, označení, osvětlení) Ventilační zařízení Informování řidičů (RDS-TMC, informační displeje …) Zastavení provozu (dopravní systém) Zajištění a spolupráce s IZS při likvidaci nehody (dispečeři, manuální řízení, CCTV)
	Požár do 100 MW	- Velké škody na zdraví (teplem, kouřem) - Velký rozsah úmrtí vlivem požáru - Rozsáhlé materiální škody na stavbě a zařízení - Dlouhodobé omezení provozu		Rychlá identifikace požáru (liniový hlásič, senzory kouře, SOS skříně …) On-site hasební zásah (ruční hasící přístroje) Zajištění úniku osob (únikové východy, označení, osvětlení) Ventilační zařízení Informování řidičů (RDS-TMC, informační displeje …) Zastavení provozu (dopravní systém) Zajištění a spolupráce s IZS při likvidaci nehody (dispečeři, manuální řízení, CCTV)

Tab. 4: Dělení události typu „nehoda“ a „požár“

[3] Uhašen lokálně, na místě účastníkem nehody

3.2 Zařízení a systémy ovlivňující bezpečnost účastníků

Řada událostí je vyvolána uživateli tunelu (zastavení vozidla, nehoda, ztráta nákladu, požár apod.) a tyto události přímo technologie tunelu neovlivňuje, pokud je ve standardním stavu. Pokud však již takováto situace vznikne, je nutné ji bezprostředně identifikovat a učinit opatření, například aktivací světelného signálu „Stůj“, aby se do kritické situace nedostávali další účastníci provozu. Zde již hraje technologie klíčovou roli a to nejenom z hlediska obecné funkčnosti, ale i z hlediska spolehlivosti, že vykoná akci, na kterou je projektována.

3.2.1 Matice událostí

Následující tabulka ukazuje přehled událostí a to jak by měl systém reagovat, se zaměřením na význam aktorů a senzorů v bezpečnostním řetězci. Sloupce označené K/BK označují, zda dané zařízení má kritický (žlutá), bezpečnostně kritický (červená) význam pro zabránění škod na lidských životech i majetku. Pokud je označení zelené, selhání dané technologie neohrožuje bezprostředně životy či majetek.

Označení senzorů a aktorů je ve shodě s TP98 – pojem „světelný signál“ označuje signál dvojbarevné soustavy dle kap. 3.2.5.1; pojem PDZ B1 označuje zákazovou značku „Zákaz vjezdu všech vozidel“ nebo její modifikaci v obvyklém provedení s otočnými prizmaty; označení PDZ B20a označuje dopravní značku „Nejvyšší povolená rychlost“ v provedení světloemitujícím. Pojem „Zábrany“ je vysvětlen v kap. 3.2.3.7.

Stejně tak je terminologie a funkce senzorů přejímána z příslušných kapitol TP98.

Událost	Reakce systému	Senzory	K/BK	Aktory	K/BK
Zastavení, nehoda	– automatická identifikace v čase – bezprostřední omezení/ zastavení dopravy	dopravní detektory	K	světelná návěstidla,	BK
		úsekové měření	-	závory	K
		SOS boxy	-	PDZ B1	BK
Požár	– automatická identifikace v krátkém čase – bezprostřední zastavení dopravy – informování účastníků	videodetekce kouře	BK	ventilace	K
		liniový hlásič	BK	světelná návěstidla,	BK
		požární tlačítka	-	PDZ B1	BK
		SOS boxy	-	závory	K
				Nouzový zvukový systém	BK
Výpadek VZT s dlouhodobějším překročením koncentrací	zastavení dopravy	detektory CO, NOX	K	světelná návěstidla,	K
		opacity	K	PDZ B1	-
Výpadek VZT, ale hodnoty škodlivin jsou pod průměrem	žádná *Tento stav nepočítá s tím, že zrovna v této situaci může vzniknout požár*	detektory CO, NOX	K	světelná návěstidla,	-
		detektor opacity	K	závory	-
Výpadek osvětlení hlavní soustava	– automatický přechod na náhradní osvětlení – omezení rychlosti *Pokud by nesvítilo omezení rychlosti nutno zastavit provoz*	senzory škodlivin	K	světelné značky B20a	K
		dopravní detektory	K	PDZ B1	-
		CCTV	K	závory	-
Výpadek osvětlení náhradní nefunguje, ale svítí normální	*Není řešena situace, kdy zároveň vypadne i hlavní – nutno okamžitě zastavit dopravu*	senzory škodlivin	-	světelná návěstidla,	K
		dopravní detektory	-	PDZ B1	K
		CCTV	-	závora	K
Výpadek ovládání dopravních značek	*Stav je nebezpečný kdykoli je nutno omezit rychlost nebo zastavit provoz, např. při výpadku osvětlení, nehodě*	senzory škodlivin	-	světelná návěstidla,	K
		dopravní detektory	-	PDZ B1	K
		CCTV	-	závora	K
Výpadek napájení značek	*Značky jsou napájeny po sekcích, takže nehrozí nebezpečí*				
Výpadek ŘS ale lze zapnout ventilaci (funguje	*Při funkčním ovládání značek, signálů a závor*	požární senzory		světelná návěstidla,	BK
		senzory škodlivin		PDZ B1	BK

EPS, CCTV, SOS boxy a telefon)		CCTV		závora	K
				PDZ B20a	K
Výpadek ŘS nelze zapnout ventilaci (funguje EPS, CCTV, SOS boxy a telefon)	Požaduje se okamžité zastavení dopravy *BK aktory lze ovládat, pokud ne ⇒ přenosné zařízení*			světelná návěstidla	BK
				PDZ B1	BK
				závora	K
Výpadek EPS	Tunel se provozuje, musí fungovat měření škodlivin a CCTV	senzory škodlivin	K	světelná návěstidla	K
		CCTV	K	PDZ B1	K
		dopravní detektory	-	závora	K
Výpadek nouzového zvukového systému				Nouzový zvukový systém	BK
Celkový výpadek hlavního napájení	pracují UPS a záložní zdroj (generátor)	dopravní detektory	K	světelná návěstidla,	K
		CCTV	K	PDZ B1	K
		úsekové měření	-	závora	K
Výpadek UPS při funkčnosti hlavního napájení		dopravní detektory	K	světelná návěstidla,	-
		CCTV	K	PDZ B1	-
		úsekové měření	-	závora	-
Výpadek záložního zdroje při funkčnosti UPS	Při poruše hlavního i záložního zdroje nutné okamžitě zastavit provoz			světelná návěstidla,	BK
				PDZ B1	BK
				závora	K

Tab. 5: Příklad matice zařízení, jejichž výpadek může způsobovat nebezpečné situace pro účastníky provozu

Jak je z tabulky patrné, kromě kritických situací vzniku požáru nebo nehody se vyskytují i různé výpadky subsystémů či zařízení, při kterých je nezbytné, aby vyznačené senzory a aktory byly v provozuschopném stavu.

3.2.2 Shrnutí

Ve výše uvedené tabulce jsou uvedeny mimořádné a havarijní stavy a jsou vytipována zařízení, jejichž dysfunkce je kritická či dokonce bezpečnostně kritická a to ve vztahu k uživatelům tunelu. V zásadě leží na bezpečnostně kritické cestě zařízení a systémy, které musí neprodleně zabránit vjezdu vozidel do oblasti s krizí – vážnou nehodou, požárem či výbuchem. Jedná se o vybrané dopravní značení a jako ve všech případech řídicí systém, velmi záleží i na rychlosti identifikace události. V následujícím výčtu je proveden orientační komentář k jednotlivým technologiím.

3.2.2.1 Požár a vozidla mimo tunel

Dopravní značky: kritickou potřebou je za všech okolností zastavit vozidla a to světelnými signály S1a s červeným světlem „Stůj“. Z tohoto hlediska musí být řešeno jejich zálohované ovládání, dále (zálohované) napájení, vlastní spolehlivost světelných zdrojů a možnost identifikovat nesvícení. Z tohoto hlediska se zdá dobrou možností využívání LED světelných zdrojů, resp. je doporučeno červený signál zdvojovat, minimálně v oblasti portálů.

U zákazových značek typu B1 „Zákaz vjezdu všech vozidel“ je nutné napájení z oddělených sekcí, a redundantní ovládání. Dále zajištění identifikace nefunkčnosti a to i ve „studeném“ stavu. Vzhledem k mechanickému přestavování symbolů, jsou tyto značky náchylnější na poruchy a to zvláště v případě nepříznivých klimatických podmínek. Testování funkčnosti musí být prováděno pravidelně.

Pro zastavení provozu jsou významné i mechanické zábrany (závory), které lze také považovat za zařízení kritická.

Signály pro jízdu v pruzích S8a-e neslouží k zastavování provozu a nejsou tedy na kritické cestě.

Kombinace značek B1 a světelných signálů vytváří redundantní systém v kategorii BK a k nim ještě přistupují závory v kategorii K. Pokud je v provozu alespoň jedno ze dvou BK zařízení, neměla by být ohrožena bezpečnost uživatelů přijíždějících do místa s požárem či nehodou.

Řídicí systém: má zásadní důležitost, a proto jsou řídicí stanice CT u tunelů kategorie TA a TB v režimu „hot-stand_by“. Dále musí být rovněž redundantní komunikační vedení k podřízeným programovatelným automatům a jednotkám vzdálených vstupů a výstupů CS, více viz TP98, kap. 10. Doporučuje se i zálohovat stanice CT, které přímo řídí a ovládají vyjmenovaná BK zařízení.

Důležitým požadavkem vyplývajícím z kap. 2.3 „Bezporuchovost tunelových systémů“ je pravidelné ověření toho, že SW pracuje v požadovaném režimu.

Senzory požáru: pro automatizovanou identifikaci nejnebezpečnější události, požáru, se využívá celá řada různorodých systémů s různými funkčními vlastnostmi. Jsou to různé typy liniových hlásičů, videodetektory kouře nebo detektory plynů. Jejich funkční charakteristiky se liší dle typů, stejně jako se liší jejich spolehlivost a poruchovost.

Z tohoto hlediska je obtížné, resp. přímo nemožné uvažovat o zálohování zařízení se stejnou funkčností (dva liniové hlásiče apod.). Na druhé straně je požadováno navrhovat do tunelu kombinace různých systémů, liniový hlásič + videodetekce kouře apod. Dochází tedy k dílčí funkční redundanci systémových vlastností.

3.2.2.2 Požár a ohrožení účastníci v místě požáru

Požár je výjimečná situace, která se vztahuje nejenom k vozidlům přijíždějícím k události, ale také k uživatelům, kteří jsou v místě události a budou mít snahu uniknout. Zde má zásadní význam včasné varování nouzovým zvukovým systémem a činnost ventilačního systému.

Nouzový zvukový systém: pro automatizovanou identifikaci nejnebezpečnější události, požáru, se využívá celá řada různorodých senzorů, ale efektivní informování o požáru a bezprostřední nutnosti evakuace spočívá na nouzovém zvukovém systému. Protože může, až o minuty, urychlit únik osob je zařazen do kategorie BK zařízení.

Ventilátory: V prvních minutách po vypuknutí požáru je, z hlediska bezpečnosti osob, rozhodující optimální řízení ventilace, aby bylo dodrženo rozvrstvení (stratifikace) kouře. Ventilační systém je navrhován specificky, vždy pro dané podmínky konkrétního tunelu. Obvykle je tvořen více skupinami ventilátorů, napájených ze zálohovaných zdrojů. Vzhledem k tomu, že je šance se v prvních minutách po vzniku požáru zachránit evakuací únikovými východy i když ještě ventilace nepracuje je ventilační zařízení zařazeno do kategorie K. Dalším důvodem je, že ventilátorů je v tunelu více a tvoří vlastně vícenásobný redundantní systém

3.2.2.3 Výpadky různých technologických celků

V tunelu mohou vzniknout problémy, když vypadne osvětlovací soustava, energetický systém apod. Tyto situace přináší zvýšenou míru rizika pro uživatele tunelu, ale nic nebrání tomu, aby při dodržení pravidel silničního provozu tunel opustili. Pokud jsou výpadky technologií takového rázu, že by byla míra rizika příliš vysoká, je doprava v tunelu zastavena

Energetický systém: zásadně ovlivňuje funkčnost všech zařízení a systémů. Dle platných TP98 je napájení vícenásobně zálohováno, takže nehrozí to, že by systém byl bez napětí díky poruše napájení. Dokonce se zdá, že současný návrh dvojnásobného napájení ze dvou nezávislých rozvoden a další záloha agregáty a výkonnými UPS vede ke zbytečně vysokým investičním a provozním nákladům. Dosud nejsou a nebyly počítány pravděpodobnosti výpadků jednotlivých zdrojů napájení, například, zda se vůbec vyskytují výpadky rozvoden I. kategorie. Pro bezpečné opuštění tunelu by mělo postačovat napájení klíčových zařízení z UPS.

Osvětlení: Normální osvětlení je opět vícenásobně zálohováno náhradním a nouzovým osvětlením a jeho výpadek neleží na kritické cestě a neměl by vést k bezprostřednímu ohrožení života účastníků provozu.

Zatímco návrhu systému tunelu, jeho provedení a uvádění do provozu se věnuje značná pozornost, celý proces je popsán v technických podmínkách a je sledován různými účastníky procesu, je potom optimalizaci údržby a možnému prodloužení doby života zařízení věnována nepoměrně menší pozornost. Proto bude pozornost další části výzkumu zaměřena právě na tuto oblast.

4 SLEDOVÁNÍ ŽIVOTNOSTI ZAŘÍZENÍ – VZOROVÝ PŘÍKLAD

V této kapitole metodického pokynu je uveden vzorový příklad vedoucí k vytvoření systému pro sledování poruchovosti zařízení v tunelech a s tím spojené optimalizace údržby založené na hodnocení životnosti zařízení. Takovýto systém se stává základem pro řízení údržby na profesionální bázi založené na diagnostice zařízení. Preventivními zásahy či dílčími obměnami vadných dílů může významně přispět k prodloužení života zařízení a tím i ke zvýšení ekonomiky provozu.

Navržené postupy se týkají tunelů připravovaných k realizaci, případně by mohly být realizovány při zásadnějších modernizacích stávajících řídicích systémů a to v závislosti na ekonomických možnostech správce tunelu.

4.1 Příklad tvorby systému pro sledování životnosti

Vytvoření fungujícího systému je dlouhodobější záležitost, se kterou by se mělo počítat již při projektování a programování SCADA aplikace. Postup lze shrnout do následujících kroků, které budou dále komentovány:

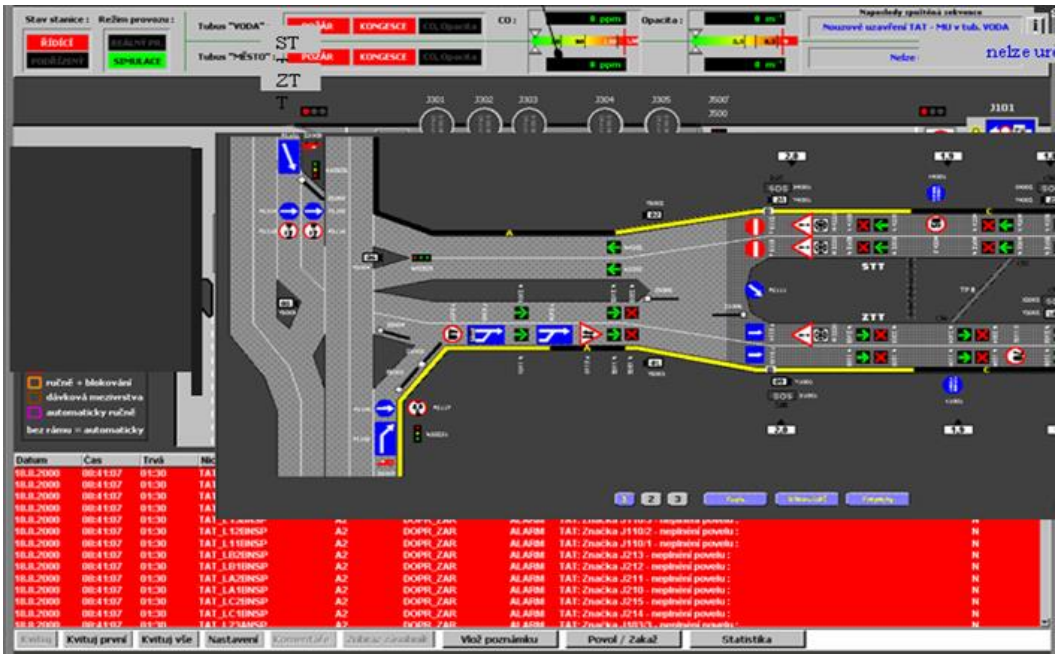
1. Extrakce událostních a poruchových dat v otevřeném formátu do specifické databáze;
2. Zavedení elektronických hlášenek poruch a jejich ukládání do databáze;
3. Expertní vytipování bezpečnostně-kritických a kritických zařízení;
4. Úprava a transformace měřených dat;
5. Analýza a vizualizace poruchových stavů;
6. Výpočty intenzity poruch a predikce zvýšení četnosti poruch nad stanovenou mez a odvození vanové křivky;
7. Expertní posouzení nutnosti preventivního zásahu údržby, či obnovu nebo výměnu tohoto zařízení.

4.1.1 Extrakce událostních a poruchových dat

Základním předpokladem pro realizaci této koncepce je, že tunel obsahuje SCADA systém ve smyslu TP98, kap. 1.2 „Tunel jako telematický systém“. SCADA systémy pro řízení tunelů mají různé formy tzv. poruchových deníků, ve kterých jsou zobrazovány poruchy či stavy vybraných technologii, které vybočují z normálu. Tyto stavy se automaticky ukládají do databáze řídicího systému. Poruchové deníky musí být součástí každého řídicího systému.

Na Obr. 18 je typický příklad, kde celý soubor poruch v červeném poli vyjadřuje povelování dopravních značek a to sice stav „Nepřijatý povel“.

Těchto hlášení mohou být tisíce a vůbec nemusí svědčit o poruchách zařízení souvisejících s životností, ale mohou být například vyvolány údržbou zařízení, špatným ovládáním, vytaženým kabelem, poškozením zařízení v důsledku dopravní nehody apod. Řídicí systém musí umožňovat export poruchových deníků do databázového systému mimo SCADA.



Obr. 18: Obrazovka řídícího systému s aktuálními poruchami (červené pole), příklad

Výstupem této etapy projektu je, že vybrané události (poruchové stavy, případně údaje o povětrnostních podmínkách a dopravě) jsou uspořádány v databázi analytického modulu.

4.1.2 Zavedení elektronických hlášenek poruch

Jak již bylo uvedeno, systém SCADA je schopen zachytit veškeré poruchy zařízení, která jsou na systém připojena a obsahují diagnostiku. Například při výpadku napájení pomocný kontakt stykače odpadne a identifikuje tuto poruchu. Na druhé straně existuje dosti velká kategorie poruch, které naopak nemůže zaznamenat řídicí systém, protože výstupy zařízení nejsou do řídicího systému zavedeny. V tomto případě se může jednat o znečištěnou značku, poškozený kryt závory, ale mohou to být i mnohem závažnější poruchy.

V tomto kroku řešení je vhodné zavést elektronické hlášenky. Ty jsou součástí programového balíčku, kdy dispečer zapíše závadu do elektronického formuláře a jeho vybraná políčka jsou propojena do databáze analytického modulu, takže se hlášenka ukládá jako databázový soubor.

HLÁŠENÍ O ZÁVADĚ

Dálnice/rychl.kom.: R1 Pořadové číslo hlášení: ŘSD: 19-2011
Místo: Lochkov ELTODO: 68/2011

Datum a čas zjištění závady: 14.1.2011 14:18
Závadu zjistil: dispečer tunelu
Telefonní kontakt: 725 472 251

Závada: **Akomodační osvětlení LTT Lochkov**

Stručný popis závady:

Výpadek komunikace akomodačního osvětlení LTT tunelu Lochkov. ŘS hlásí výpadek komunikace téměř u všech akomodačních světel světel.

Datum a čas předání hlášení o závadě ELTODO: 14.1.2011 15:05h
Hlášení za ŘSD zaslal: Hudec M.

Datum a čas přijetí hlášení o závadě servisní firmou: 14.1.2011 16:00
Hlášení přijal: hybš - dispečer servisu SOKP

Datum a čas opravy:

Popis opravy:
Předano na EDS
Odstraněno - nahodilá chyba

Oprava fakturována na ŘSD - č.faktury:
Oprava fakturována servisní firmou - č.faktury:

Hlášení vždy zasílejte na tyto e-mailové adresy: servis.sokp@eltodo.cz

Obr. 19: Příklad elektronického formuláře pro zápis závad dispečerem

4.1.3 Expertní vytipování bezpečnostně-kritických a kritických zařízení

V kap. 3 „Scénáře provozování tunelu pozemní komunikace“ je poskytnut přehled o tom, které kategorie scénářů provozování tunelu jsou kritické. Pojem kritický či bezpečnostně-kritický se v tomto případě vztahuje vždy k uživatelům tunelu, tedy řidičům a dalším účastníkům silničního provozu.

Tunel je součástí pozemní komunikace a pro řidiče platí pravidla silničního provozu i při jízdě tunelem. Jinak řečeno, při výpadku normálního i nouzového osvětlení se zvyšuje sice riziko excesů, ale vozidlo by mělo tunelem bezpečně projet s rozsvícenými reflektory. Zařízení, respektive jejich dysfunkce leží na kritické cestě a vyvolávají kritické situace, které přímo neohrozí životy účastníků, ale jsou potenciálně zdrojem značného nebezpečí.

V případě požáru, hromadné nehody či e+xploze je situace jiná. Pokud selžou zařízení blokující vjezd do tunelu, jsou uživatelé tunelu, pokračující v jízdě k události, vystaveni bezprostřednímu ohrožení života. V tomto smyslu je nutné přiřadit vybraná zařízení ovládající dopravu v tunelu do kategorie bezpečnostně-kritických. Stejně tak, pokud selže identifikace požáru, informování uživatelů o bezprostředním nebezpečí a třeba i ventilace jsou lidé v tunelu při požáru v přímém ohrožení života.

V kap. 3.2.1 „Matice událostí“ je tabulka, která přímo ukazuje, která zařízení jsou pro které scénáře událostí kritické. V následující tabulce je jenom příklad části matice pro situaci požár:

Událost	Reakce systému	Senzory	K/BK	Aktory	K/BK
Požár	– automatická identifikace v krátkém čase – bezprostřední zastavení dopravy – informování účastníků	videodetekce kouře	BK	ventilace	K
		liniový hlásič	BK	světelná návěstidla,	BK
		požární tlačítka	-	PDZ B1	BK
		SOS boxy	-	závory	K
				Nouzový zvukový systém	BK

Z ukázky je patrné, která zařízení mají kritický, či bezpečnostně-kritický vliv na životy účastníků provozu a na velké materiální škody. Jedná se o příklad pro konkrétní tunel, každý tunel je ale jiný.

V této etapě by měla být zpracována matice událostí a tak i stanoveny priority zařízení z hlediska údržby.

4.1.4 Úprava a transformace měřených dat

Architektura SCADA systému je/by měla být taková, že veškeré poruchy, které zaznamenává řídicí systém, jsou archivovány v deníku poruch ve formě specifické databáze. Takovýto soubor měl například za tři měsíce zkušebního provozu pro stavbu 514 (tunel Lochkov) 133 492 hodnot.

Obvykle platí, že data přímo poskytovaná senzory nejsou vhodná pro přímou analýzu. Cílem předzpracování dat je připravit data tak, aby mohla být použita v automatických vyhodnocovacích algoritmech na vyšších úrovních hierarchie řídicího systému. Důvodů pro předzpracovávání je celá řada:

- Data obsahují špatné údaje vzniklé chybami detektorů a přenosové trasy
  - typicky: chybějící data nebo duplicitní hodnoty
- Data v sobě obsahují náhodnou složku, nevhodnou pro další zpracování
- Data mají nestejnorodý obor hodnot, leží mimo toleranci měření …

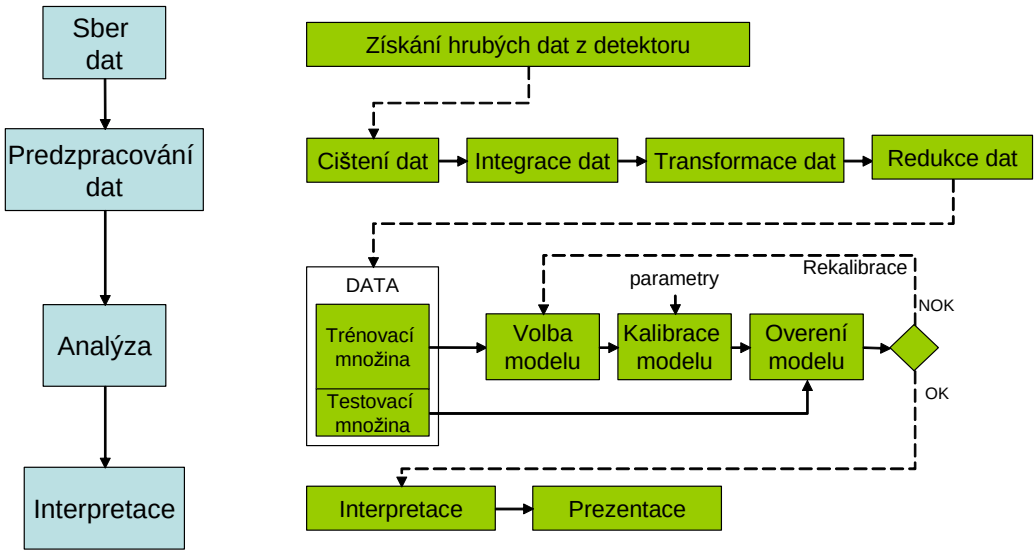
Přitom je nutné brát v úvahu, že se chyby mohou vyskytovat i ve formě náhodných poruch daných například rušením na trase. Proto, aby data byla vůbec využitelná, je nutné provést následující operace:

1. Efektivní extrakci surových dat z provozních dat SCADA systému a jejich předzpracování spočívající v:
   - čištění (kontrola oboru přípustných hodnot, náhrady chybějících hodnot (průměr, regrese apod.)
   - filtraci a agregaci hodnot (vyhlazování SMA, WMA, EMA, …)

- Integraci (mapování parametrů, slučování informací) a redukci (metody shlukování, transformace do jiné dimenze, …)

2. Analýzu dat a jejich transformaci na informace
3. Vizualizovat poruchy v uživatelsky příjemném prostředí;

Celý proces zpracování dat, až po jejich interpretaci a získávání informací o stavu technologie a informace pro údržbu lze shrnout do následujícího schématu, lit. [13], kap. 2:



Obr. 20: Obecné schéma při zpracování poruchových dat ze systému SCADA, lit.[13]

Pokud se data (poruchové stavy) zpracovávají dle výše uvedeného schéma, je vytvářena jejich interpretace ve formě modelu (vanová křivka) a lze predikovat jejich vývoj. V další kapitole je potom uveden příklad vizualizace a tím i interpretace dat.

4.1.5 Analýza a vizualizace poruchových stavů

Tento metodický pokyn dává návod, jak vytvořit systém pro sledování životnosti technologických systémů a zařízení v tunelu a to na obecné úrovni, neboť neexistuje univerzální návod, protože neexistuje univerzální tunel. Příklad návodu, jak postupovat, poskytují realizace toho systému u jiných již existujících tunelů.

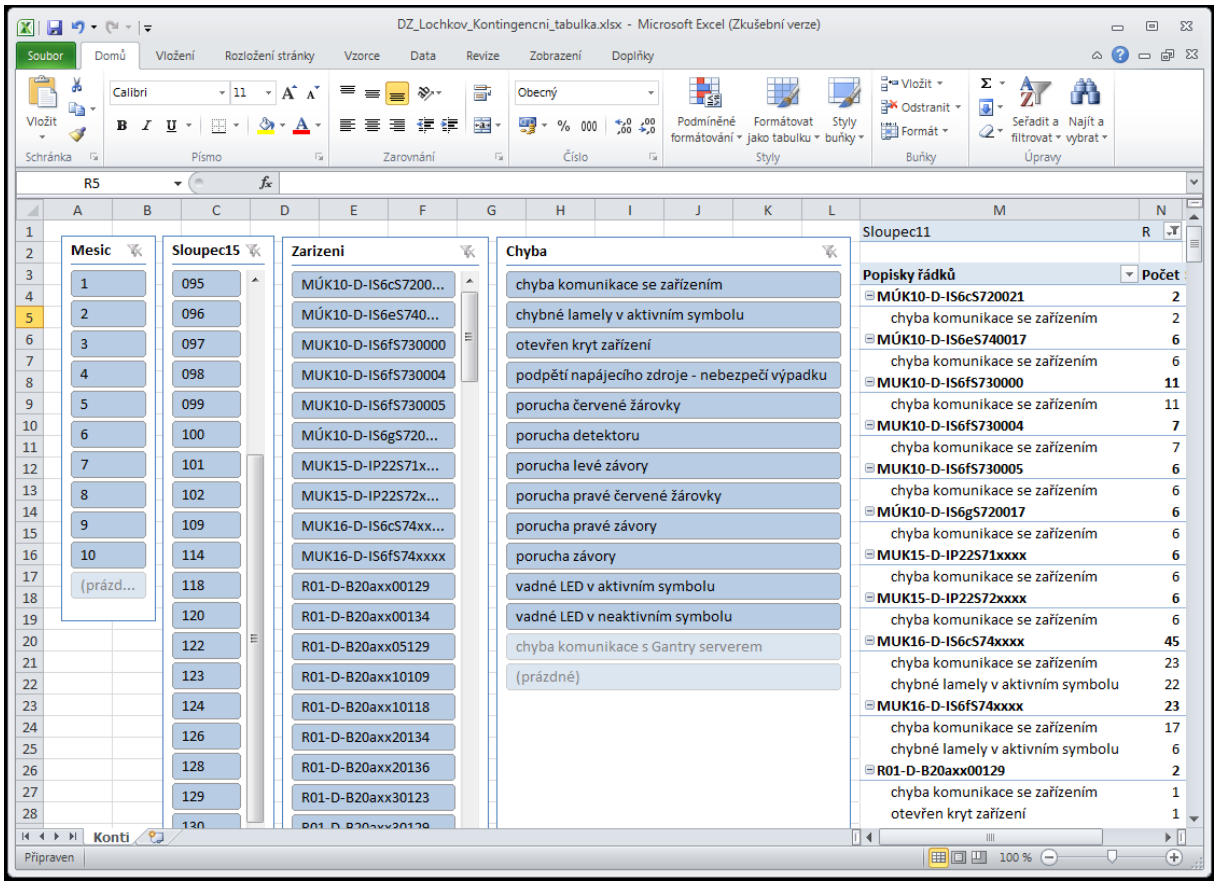
Datové soubory ze SCADA systému byly exportovány, viz kap. 4.1.1, do programového prostředí nazvaného FAILURE, které je zpracováno v programovém prostředí EXCEL a to proto, aby bylo dostupné pro každého uživatele, který potřebuje analyzovat závady v konkrétním tunelu. Touto metodikou je také doporučeno, aby se nejprve využíval všeobecně dostupný EXCEL na úkor více sofistikovaných programů typu MATLAB. Program využívá tzv. kontingenční tabulky, které umožní uživateli poměrně jednoduchou práci.

Vytvořený analytický program[4] byl testován a je využíván pro analýzu poruch v již existujících dopravních stavbách, přičemž data byla poskytnuta řídicím centrem. Na Obr. 21 je vidět hlavní okno. V prvním sloupci si uživatel volí měsíc/měsíce ve kterých chce analýzu provádět. Následuje polohopis zařízení, což byl specifický požadavek ŘSD. V dalším sloupci je kompletní seznam zařízení, která mohou být podrobena analýze. Ve sloupci „Chyba“ jsou typy poruch, které se mohou vyskytovat a poslední sloupec uvádí vlastní popis závady a množství, kolikrát se vyskytla.

V rámci této tabulky je možná kontrola a dohledání technologických dat pro jednotlivá zařízení. Jsou dohledatelná veškerá zařízení v řešené oblasti, která ve sledovaném období vykázala libovolnou chybu

[4] společností Eltodo, a.s.

nebo jinak zajistila log do registrů. Pro prohlížení kontingenční tabulky je díky použité technologii nutné využít MS Excel 2010 a vyšší.



Obr. 21: Náhled SW FAILURE s kontingenční tabulkou, zdroj Eltodo, a.s.

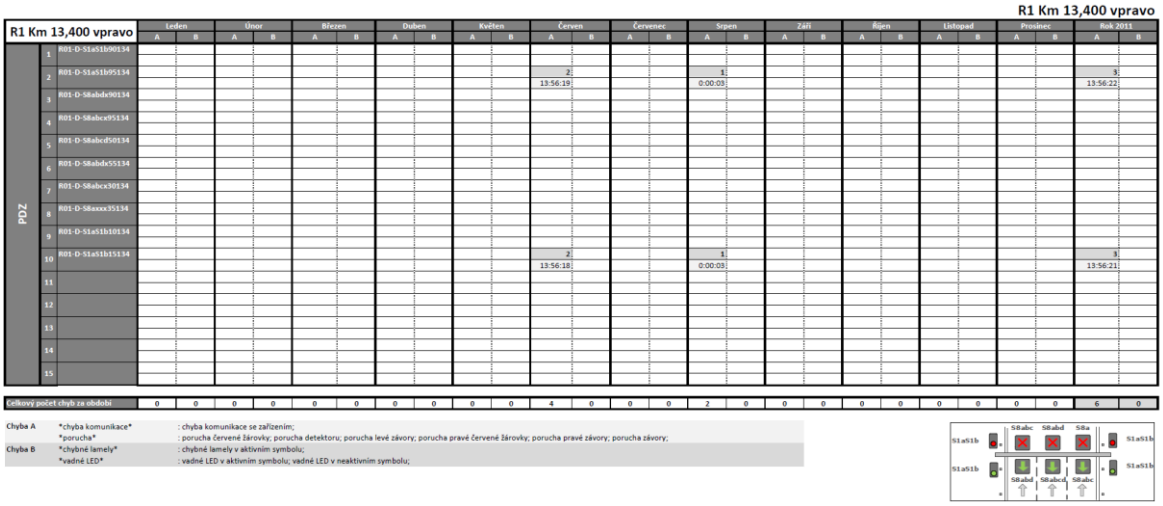
Pro jednotlivá zařízení je možné jednak vyhodnocovat počty chyb, které byly u těchto zařízení v daném měsíci evidovány a uloženy. K tomu je vyhodnocován a v přehledu uveden celkový čas trvání detekovaných chyb. Tento přehled je z pohledu vyhodnocení pravděpodobně důležitější, než absolutní číslo počtu chyb. Jsou případy, kdy jsou detekovány chyby komunikace, které ale mají dobu trvání v řádu sekund, nezřídka 0 s. Jedná se o chvilkový výpadek na komunikaci, který nemá zásadní vliv pro řízení a funkci systému LŘD. Oproti tomu jsou detekovány případy chyb, které mají trvání v řádu hodin. Takové výpadky již mohou mít významný vliv na správnou činnost a plnou funkcionalitu systému v dané oblasti.

Obr. 21 uvádí příklad tabulky generované SW FALURE se zpracovanými daty o činnosti PDZ v tunelu. Tabulky mohou být zpracovány po jednotlivých řezech, přesné označení se staničením řezu se nalézá v pravém i levém horním rohu tabulky. Každému zařízení na řezu je definováno unikátním kódem, dle požadavků na systém, značení provozních celků a elektrických zařízení na dálnicích, rychlostních silnicích, tunelech a jiných objektech ve správě Ředitelství silnic a dálnic ČR: PPK-ZAR, verze 06/2006. Pod tímto kódem je zařízení uvedeno v levé části tabulky.

Vedle seznamu kódů zařízení se nalézají k nim příslušné řádky, které zobrazují počet příslušných chyb v měsíci a celkový čas trvání těchto chyb. Zapisované chyby (4 typy) byly pro potřeby vyhodnocení shrnuty do dvou kategorií. Jedná se o chyby typu A a typu B, kdy chyby A jsou chyby komunikace se zařízením, porucha červené žárovky a další poruchy. Do kategorie chyb typu B byly zařazeny chyby lamely proměnné značky v aktivním symbolu, vadné LED v aktivním symbolu a vadné LED v neaktivním symbolu.

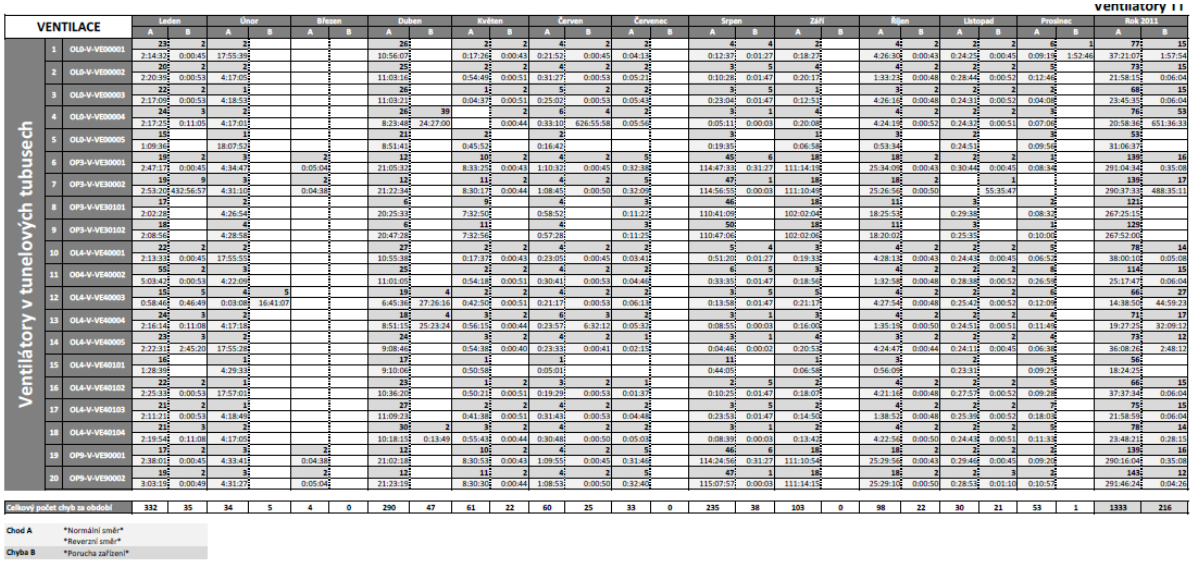
V pravé spodní části pod tabulkou se nalézá grafické ztvárnění řezu, kterému přísluší v tabulce vyhodnocovaná zařízení. Grafické ztvárnění je aktuální pro daný řez a reflektuje jak počet pruhů, tak

i případnou unikátnost řezu. Jednotlivá zařízení jsou označena zkrácenými kódy dle výše uvedené specifikace PPK-ZAR.



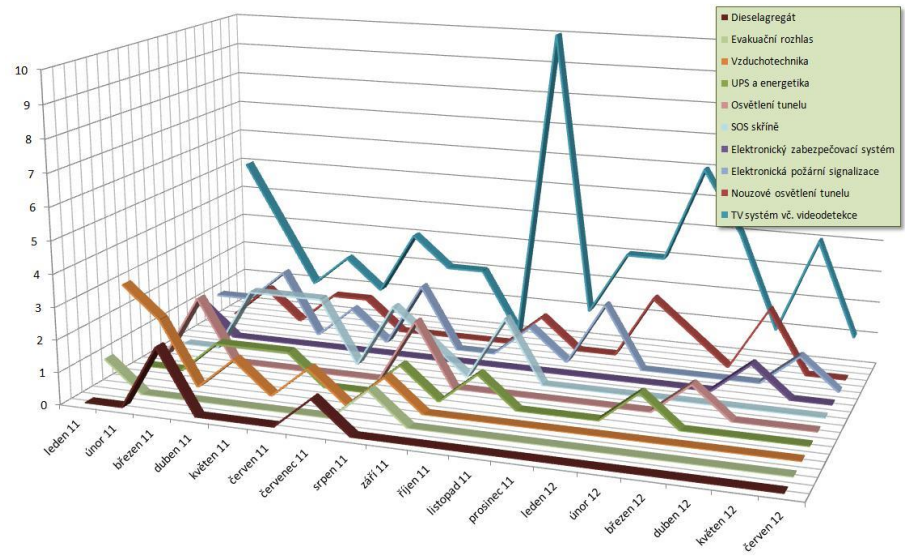
Obr. 21: Náhled tabulky zpracování činnosti telematických zařízení, zdroj Eltodo, a.s.

Další výstup programu umožňuje například sledovat celkovou dobu činnosti všech ventilátorů v tunelu, což je vhodný nástroj pro ekonomické analýzy.



Obr. 22: Výstupní sestava zachycující celkovou dobu činnosti všech ventilátorů po jednotlivých měsících

Pomocí analytického programového nástroje je možné generovat a vizualizovat sestavy hlášenek pro různé provozní soubory a tím usuzovat na tendence spolehlivosti jejich provozu. Na obrázku níže jsou jako názorný příklad zpracovány hlášenky tunelové stavby Cholupice (včetně hlášenek týkajících se dispečinku nebo řídicího systému, které jsou společné se stavbou 514 tunelu Lochkov). Hlášenky jsou pro přehlednost tříděny do 20 kategorií.



Obr. 23: Rozdělení všech hlášenek DT (z tunelu Lochkov) – prvních 10 z 20 skupin, zdroj Eltodo, a.s.

V následujícím výčtu je jako příklad komentováno šest zařízení z celkem dvaceti, která byla analyzována pracovníkem zodpovědným za analýzu poruch:

- Dieselagregát

  Za celé období ZP byly zaznamenány 3 hlášenky DT v rámci sledování dieselagregátu na tunelové stavbě Cholupice. Dvě hlášenky se zabývaly únikem oleje a poruchou frekvenčního měniče.
- Nouzový zvukový systém

  Za celé období ZP byly zaznamenány 2 hlášenky DT v rámci sledování nouzového zvukového systému tunelové stavby Cholupice. Jednalo se o poruchy ve vybraných sekcích.
- Vzduchotechnika

  Za období ZP dispečeři technologie zaznamenali 8 hlášenek za tunelovou stavbu Cholupice z oblasti vzduchotechniky. Nejčastěji byla hlášena porucha regulačních a provětrávacích klapek.
- UPS a energetika

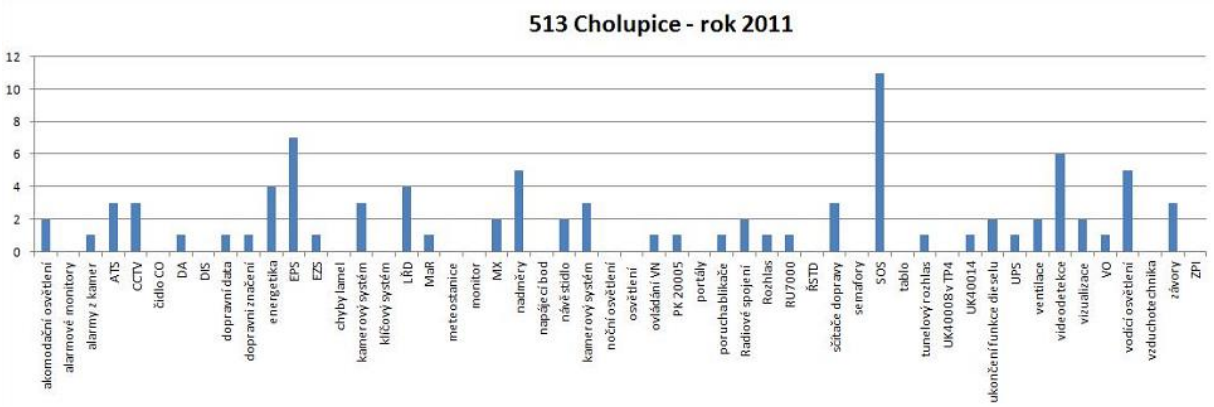
  Za období ZP dispečeři technologie zaznamenali 6 hlášenek za tunelovou stavbu Cholupice z oblasti UPS a energetiky. Jedna se týkala signalizace UPS, další údajů o spotřebě elektrické energii a přepálených pojistek.
- Osvětlení tunelu

  Za období ZP dispečeři technologie zaznamenali 5 hlášenek za tunelovou stavbu Cholupice z oblasti osvětlení tunelu. Z větší části se týkaly výpadků osvětlení, případně špatné logiky svícení v propojkách.
- SOS skříně

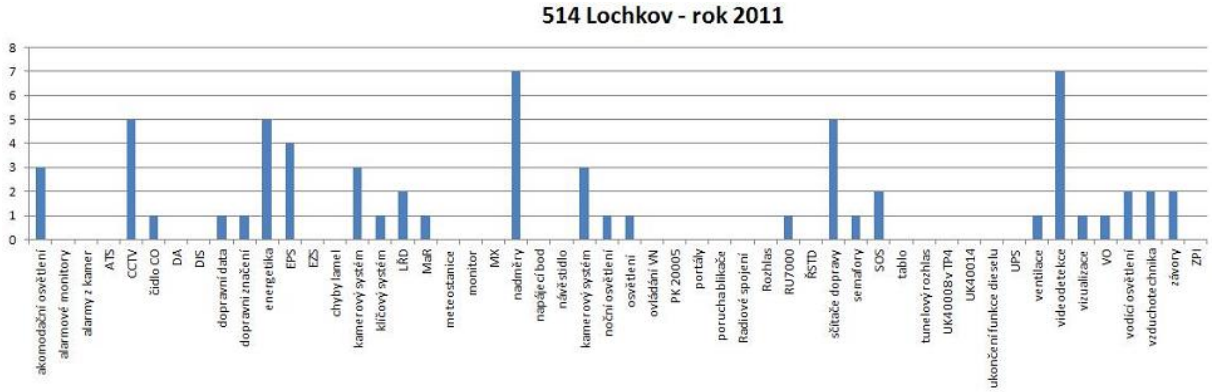
  Za období ZP dispečeři technologie zaznamenali 11 hlášenek za tunelovou stavbu Cholupice z oblasti SOS skříní. Poruchy byly rozdílné, nelze mezi nimi nalézt významnější opakující se příčinu.

Export dat

Analytický nástroj s databází dat umožňuje realizovat i další grafické interpretace, které významně pomáhají analyzovat případné problémy. Sumární přehled o všech typech závad evidovaných systémem a dispečery je na následujících obrázcích.



Obr. 24: Celkový přehled nahlášených poruch za tunel[5] Cholupice, zdroj Eltodo, a.s.



Obr. 25: Celkový přehled nahlášených poruch za tunel Lochkov, zdroj Eltodo, a.s.

Na závěr lze konstatovat, že i z uvedených příkladů je patrné, jak může být analýza poruch názorným nástrojem pro jejich sledování.

4.1.6 Výpočty poruch

V tomto kroku jsou počítány základní vlastnosti pro vybraná zařízení: bezporuchovost a životnost. Vstupem jsou předzpracovaná data z analytického modulu, která minimálně udávají četnost poruch v závislosti na čase. Výpočty a analýzu provádí analytik poruch dle platných vztahů. Ty jsou v dalším popsány pouze obecně, protože existuje více přístupů vedoucích ke stejným či podobným výsledkům.

Ukazateli bezporuchovosti, které by měly být počítány zvláště pro BK a K zařízení, jsou:

- Pravděpodobnost bezporuchového provozu $R(t1,t2)$ - pravděpodobnost, že systém může plnit požadovanou funkci v daných podmínkách a v daném časovém intervalu.
- Střední čas do poruchy MTTF (*Mean time to failure*) - očekávaný čas výskytu poruchy systému.
- Střední doba provozu mezi poruchami MTBF - očekávané doba provozu mezi poruchami
- Intenzita poruch $\lambda(t)$ – limita poměru podmíněné pravděpodobnosti, že časový okamžik vzniku poruchy objektu T padne do časové podmínky intervalu $(t, t + \Delta t)$ v délce časového intervalu, kde $\Delta t \rightarrow 0$.

Právě sledování intenzity poruch λ v závislosti na čase dokáže odhalit konec životnosti nebo poskytne informace pro preventivní údržbu či obnovu dílčích částí zařízení či systémů.

[5] tunelem jsou myšleny i předportálové úseky

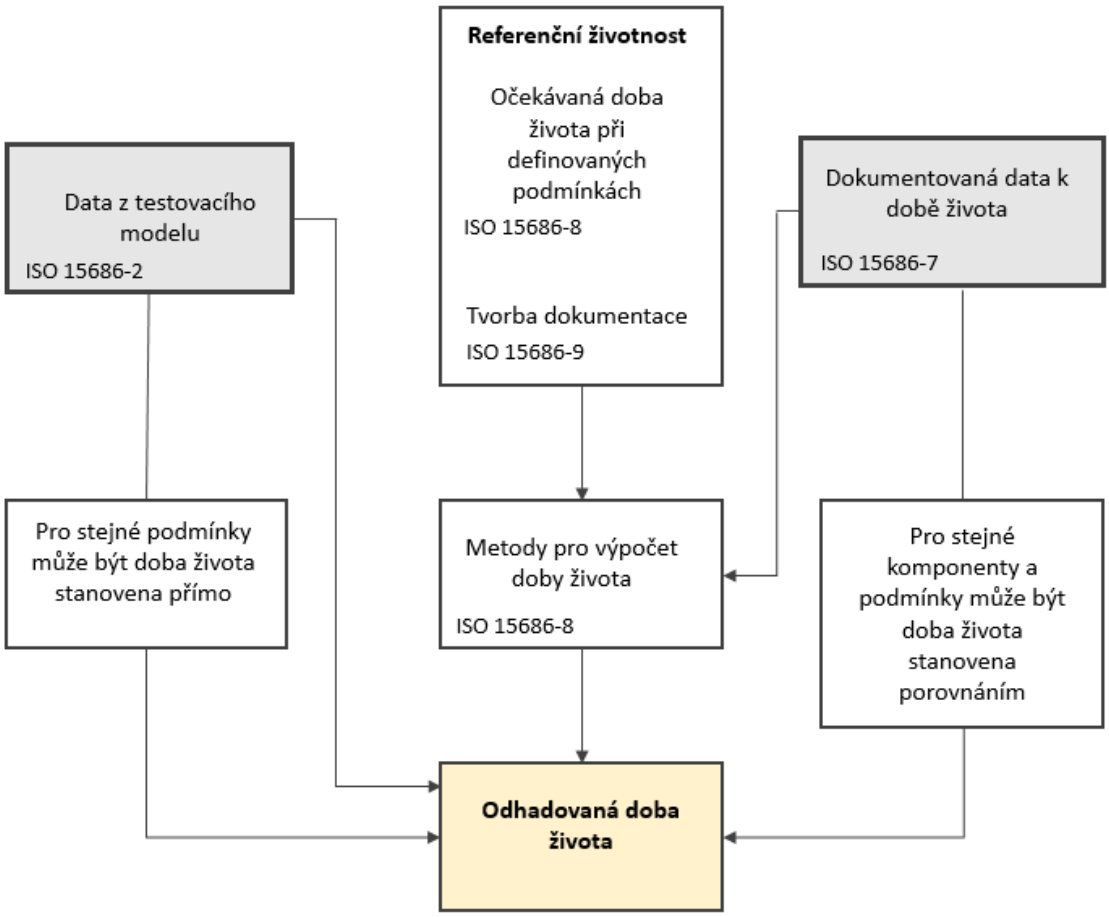
4.1.7 Expertní posouzení nutnosti preventivního zásahu údržby, obnovy či výměny tohoto zařízení

Analytický softwarový nástroj poskytuje tedy možnost analyzovat vývoje poruch a jejich závažnost, kap. 4.1.5. V předchozí kapitole byl vznesen požadavek na kvalitativní ohodnocování bezporuchových stavů. Přesto je obtížné najít nějaký univerzální nástroj, který by automaticky upozorňoval či dokonce doporučoval kdy a jaké zařízení preventivně udržovat či vyměnit jeho dílčí části.

Tento proces zatím musí provádět skupina expertů, kterou tvoří minimálně analytik a zástupci provozovatele a správce.

V budoucnosti je nutné se zaměřit na software na podporu rozhodování DSS (Decision Support System), který bude obsahovat explicitně zadané parametry pro údržbu. DSS by generoval požadavek na údržbu na základě zadaných parametrů, buď jenom dob provozu zařízení, nebo i jiných podmínek. Kromě těchto předem známých požadavků by obsahoval modul pro vyhodnocování poruch, který by, na základě předem daných a dohodnutých pravidel doporučoval požadavek na údržbu i v jiných, než dobou provozu, daných termínech.

Takovýto přístup má podporu i v normách, viz následující obrázek:



Obr. 26: Blokové schéma pro návrh DSS systému, lit. [5]

4.1.8 Závěr ke zkoumání poruchovosti

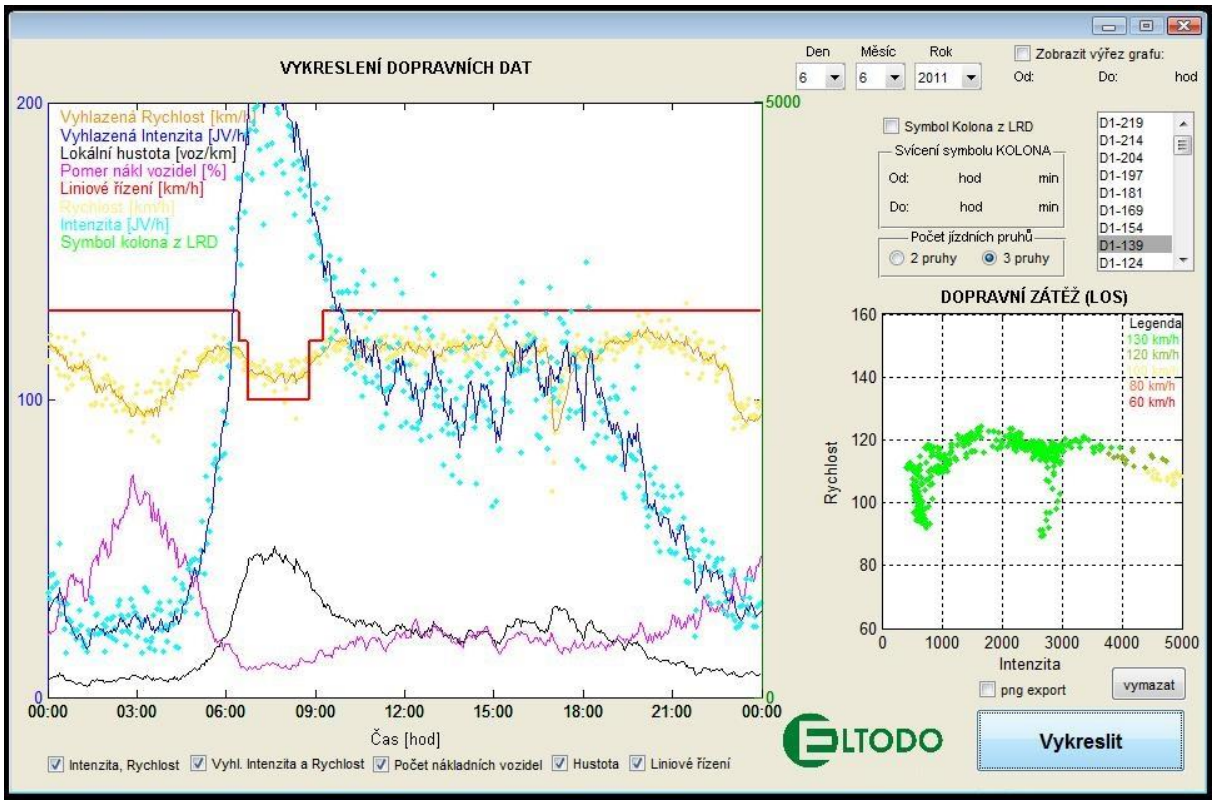
Zatímco návrhu systému tunelu, jeho provedení a uvádění do provozu se věnuje značná pozornost, celý proces je popsán v technických podmínkách a je sledován různými účastníky procesu, je potom optimalizaci údržby a možnému prodloužení doby života zařízení věnována nepoměrně menší pozornost. Tento metodický pokyn navrhuje v obecné rovině postupy, které by měly vést i ke zvládnutí této komplexní problematiky.

5 VYHODNOCOVÁNÍ DOPRAVNÍCH A FYZIKÁLNÍCH DAT

Výskyt poruch zařízení a doba jejich života je dílčím způsobem svázána s dopravou v tunelu, respektive kvalitou dopravy a samozřejmě také s fyzikálními podmínkami, kterými jsou zařízení vystavována. Proto je logické, a tímto metodickým pokynem se doporučuje, při analýze závad, sledovat dlouhodobě i hlavní dopravní a fyzikální parametry. Často právě propojení závad zařízení s dopravními a fyzikálními poměry odhalí skryté problémy, a proto je nutné tato data také zahrnout do systému vyhodnocování.

Jako příklad lze uvést prohlížeč dopravních dat, který byl testován a verifikován pro data z již existujících dopravních staveb. Po spuštění prohlížeče je možné procházet dopravní data z jednotlivých dnů pro vybrané řezy liniového řízení dopravy na vjezdech do tunelu, vybírat jednotlivé veličiny, které budou zobrazeny nebo definovat výřez dne pro lepší vizualizaci dopravních dat například během mimořádných situací.

V levém větším okně prohlížeče jsou zobrazeny hodnoty veličin jako měřená intenzita a rychlost, vyhlazená intenzita a rychlost, poměr nákladních vozidel v dopravním proudu, hustota dopravy a rychlostní značení automaticky aktivované modulem harmonizace dopravy pomocí snížení rychlosti. Pravé menší okno graficky zobrazuje stupně dopravní zátěže porovnáváním rychlosti a hustoty dopravního proudu. Obsah okna je možno exportovat do *.png souboru tak, aby mohl být použit jako samostatný materiál.



Obr. 27: Náhled okna DATAviewer_TUNEL se zobrazenými veličinami

Stejným způsobem jsou zobrazována fyzikální data.

6 ZÁVĚR

Předložený dokument vychází z úvah, kterými se zabývá v několika posledních létech mezinárodní silniční organizace PIARC, resp. její výbor C.3.3 „Road Tunnel Operation“, ve kterém pracují špičkoví zahraniční odborníci na problematiku silničních tunelů. Související výzkumné práce a množství statistických dat potvrzují, že cesta řízení údržby a obnova zařízení na základě analýzy poruch systému mohou vést k prodloužení života zařízení.

Realizace komplexního systému údržby, založeném na principu sledování životnosti zařízení, by mělo být postupně zahrnováno do strategických plánů všech správců a provozovatelů tunelů. Tento metodický pokyn představuje návod, s jakým cílem by měly být zpracovávány příslušné prováděcí předpisy.

Seznam použité literatury:

[1] SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY 2004/54/ES ze dne 29. dubna 2004 o minimálních bezpečnostních požadavcích na tunely transevropské silniční sítě; http://eur-lex.europa.eu

[2] NV č. 264/2009 Sb. o bezpečnostních požadavcích na tunely pozemních komunikací; částka 79/2009

[3] TP98 „TECHNOLOGICKÉ VYBAVENÍ TUNELŮ POZEMNÍCH KOMUNIKACÍ“, Eltodo EG, Praha, 2004, ISBN 80-239-0110-9, str. 106

[4] TP154 „PROVOZ, SPRÁVA A ÚDRŽBA TUNELŮ POZEMNÍCH KOMUNIKACÍ“, Eltodo EG, Praha, 2009, ISBN 978-80-254-4193-0

[5] „LIFE CYCLE ASPECTS OF TUNNEL EQUIPMENT“, PIARC WG1 „Improve tunnel operation and maintenance“, July 2010, pp. 31

[6] „RECOMMENDATIONS FOR ORGANISATIONAL STRATEGIC TUNNEL SAFETY MANAGEMENT“, PIARC WG1, March 2011, pp. 49

[7] Přibyl P., Janota A., Spalek J.: „ANALÝZA A ŘÍZENÍ RIZIK V DOPRAVĚ – TUNELY NA POZEMNÍCH KOMUNIKACÍCH A ŽELEZNICÍCH“, BEN, Praha, 2008, ISBN 978-80-7300-2140-0, str. 527

[8] Přibyl P., Spalek J., Krajčír D., Přikryl J.: „VÝZKUM BEZPEČNOSTNĚ KRITICKÝCH PROCESŮ A ŽIVOTNOSTI ZAŘÍZENÍ V TUNELU“, VZ351, Projekt ZET TA01030020, Eltodo EG, 2012, str. 48

[9] DIN V 19 250: „GRUNDLEGENDE SICHERHEITSBETRACHTUNGEN FUR MSR, SCHUTZEINRICHTUNGEN, CONTROL TECHNOLOGY“, Berlín, 1994

[10] CSN/EN 61 508: „FUNCTIONAL SAFETY OF ELECTRICAL/ELECTRONIC/PROGRAMMABLE ELECTRONIC SAFETY-RELATED SYSTEMS (E/E/PES)“, IEC, 2002

[11] IEC 61 511 „FUNCTIONAL SAFETY; SAFETY INSTRUMENTED SYSTEMS FOR THE PROCESS INDUSTRY SECTOR“, oborová implementace normy IEC 61508, CENELEC, 2000

[12] „PROJEKTOVÁNÍ DOPRAVNĚ TELEMATICKÝCH APLIKACÍ“, Metodický pokyn, Fakulta dopravní ČVUT, Praha, 2010, ISBN 978-80-01-04385-1, str. 130

[13] Přibyl P., Přibyl O.: „INTELIGENTNÍ DOPRAVNÍ SYSTÉMY A DOPRAVNÍ TELEMATIKA II, ČVUT FD, Praha, 2007, ISBN 978-80-01-03648-8, str. 254

Název:	**Životní cyklus technologií v tunelech pozemních komunikací**
Určení:	Metodický pokyn
Vydal:	MD ČR
Zpracovatel:	ČVUT Fakulta dopravní, Eltodo, a.s., Fakulta elektrotechnická Žilinské Univerzity v rámci Společné laboratoře tunelových systémů
Autoři:	prof. Ing. Pavel Přibyl, CSc.
Vydání:	první
Náklad:	neuveden
Počet stran:	45
Distribuce:	ELTODO, a.s., Novodvorská 1010/14, 142 01 Praha 4
ISBN:	
	prosinec 2013