ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

FAKULTA DOPRAVNÍ

Bc. Lukáš Čacký

DOPRAVNÍ A BEZPEČNOSTNÍ PŘÍSTUPY A OPATŘENÍ PRO KRITICKOU INFRASTRUKTURU

Diplomová práce

2020

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE
Fakulta dopravní
děkan
Konviktská 20, 110 00 Praha 1

K620 ..... **Ústav dopravní telematiky**

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení studenta (včetně titulů):

Bc. Lukáš Čacký

Kód studijního programu a studijní obor studenta:

N 3710 – IS – Inteligentní dopravní systémy

Název tématu (česky): **Dopravní a bezpečnostní přístupy a opatření pro kritickou infrastrukturu**

Název tématu (anglicky): Transport and security approaches and measures for critical infrastructure

Zásady pro vypracování

Při zpracování diplomové práce se řiďte následujícími pokyny:

- Analýza kritické infrastruktury a technických zařízení na dopravní síti pozemních komunikací.
- Bezpečnostní přístupy při řešení mimořádných událostí na kritické infrastruktuře.
- Technologická a technická odolonost systémů a zařízení využívaných při mimořádných událostech na kritické infrastruktuře.
- Návrh a ověření bezpečnostního opatření při vzniku mimořádné události na kritické infrastruktuře pomocí technických a technologických přístupů.
- Metodika a riziková analýza k technickému zabezpečení zařízení a ochraně kritické infrastruktury.

Rozsah grafických prací: dle požadavků vedoucího diplomové práce

Rozsah průvodní zprávy: minimálně 55 stran textu (včetně obrázků, grafů a tabulek, které jsou součástí průvodní zprávy)

Seznam odborné literatury: 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

Procházková D.: Bezpečnost kritické infrastruktury, ČVUT 2012, ISBN 978-80-01-05103-0

Vedoucí diplomové práce: **doc. Ing. Tomáš Tichý, Ph.D., MBA**

Datum zadání diplomové práce: **18. července 2019**
(datum prvního zadání této práce, které musí být nejpozději 10 měsíců před datem prvního předpokládaného odevzdání této práce vyplývajícího ze standardní doby studia)

Datum odevzdání diplomové práce: **18. května 2020**
a) datum prvního předpokládaného odevzdání práce vyplývající ze standardní doby studia a z doporučeného časového plánu studia
b) v případě odkladu odevzdání práce následující datum odevzdání práce vyplývající z doporučeného časového plánu studia

L. S.

Ing. Zuzana Bělinová, Ph.D.
vedoucí
Ústavu dopravní telematiky

doc. Ing. Pavel Hrubeš, Ph.D.
děkan fakulty

Potvrzuji převzetí zadání diplomové práce.

Bc. Lukáš Čacký
jméno a podpis studenta

V Praze dne 18.7.2019

Poděkování

Tímto bych rád poděkoval svému vedoucímu diplomové práce panu docentu Ing. Tomášovi Tichému, Ph.D., MBA za jeho odborné vedení, podporu a trpělivost v průběhu vypracování diplomové práce.

Prohlášení

Předkládám tímto k posouzení a obhajobě bakalářskou práci, zpracovanou na závěr studia na ČVUT v Praze Fakultě dopravní.

Prohlašuji, že jsem předloženou práci vypracoval samostatně a že jsem uvedl veškeré použité informační zdroje v souladu s Metodickým pokynem o dodržování etických principů při přípravě vysokoškolských závěrečných prací.

Nemám závažný důvod proti užívání tohoto školního díla ve smyslu § 60 Zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon).

V Praze dne 5.5.2020 .....

Bc. Lukáš Čacký

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

FAKULTA DOPRAVNÍ

DOPRAVNÍ A BEZPEČNOSTNÍ PŘÍSTUPY A OPATŘENÍ PRO KRITICKOU INFRASTRUKTURU

Diplomová práce

Červen 2020

Bc. Lukáš Čacký

Abstrakt

Předmětem předložené diplomové práce „Dopravní a bezpečnostní přístupy a opatření pro kritickou infrastrukturu“ je analýza kritické infrastruktury a technických zařízení na dopravní síti pozemních komunikací. Dále přehled bezpečnostních přístupů při řešení mimořádných událostí a analýza technologické a technické odolnosti využívaných systémů a zařízení. V praktické části se poté práce zabývá především rozborem fyzické bezpečnosti objektů a ve své poslední části také návrhem bezpečnostní analýzy prvku kritické infrastruktury.

Abstract

The subject of this diploma thesis "Transport and security approaches and measures for critical infrastructure" is analysis of critical infrastructure and technical equipment on the road transport network. Furthermore, an overview of security approaches in dealing with emergencies and an analysis of technological and technical resilience of the systems and equipment used. In the practical part, the work deals mainly with the analysis of physical security and in its last part also the design of security analysis of the critical infrastructure element.

Klíčová slova

kritická infrastruktura, ohrožení, most, tunel, bezpečnost, zabezpečení, silniční doprava

Keywords

critical infrastructure, danger, bridge, tunnel, safety, security, road transport

OBSAH

SEZNAM POUŽITÝCH ZKRATEK

KI kritická infrastruktura

EKI evropská kritická infrastruktura

ČR Česká republika

OSS organizační složka státu

V2X „vehicle to everything“ („vozidlo všemu“)

RVHP Rada vzájemné hospodářské pomoci

HZS Hasičský záchranný sbor

MV Ministerstvo vnitra

ŘSD Ředitelství silnic a dálnic

MÚK mimoúrovňová křižovatka

ADR Evropská dohoda o mezinárodní silniční přepravě nebezpečných věcí (z franc. **A**ccord européen relatif au transport international des marchandises **D**angereuses par **R**oute)

MZP mechanické zábranné prostředky

CCTV kamerový systém (z anglického **C**losed-**C**ircuit **T**ele**v**ision)

RFID identifikace na rádiové frekvenci (z anglického **R**adio-**F**requency **Id**entification)

ČSN česká technická norma (ze starého **Č**eskoslovenská **s**tátní **n**orma)

TP technické podmínky

GT dispečink dopravního řízení tunelů – úroveň oblasti

GG dispečink dopravního řízení – úroveň útvaru

GA dispečink technologického řízení tunelů – úroveň oblasti

CT hlavní řídící stanice a lokální dispečink tunelu

CS řídící stanice v tunelu (programovatelné automaty)

QR typ kódování dat (z anglického **Q**uick **R**esponse)

WAN Wide Area Network (počítačová sít pokrývající velice rozsáhlé území)

NFC technologie bezdrátové komunikace na krátkou vzdálenost (z anglického **N**ear **F**ield **C**ommunication)

FMEA typ rizikové analý zy (z anglického**F**ailure **M**ode and **E**ffects **A**nalysis)

FTA typ rizikové analý zy (z anglického**F**ault **T**ree **A**nalysis)

RPN indikátor závažnosti poruchy (z anglického **R**isk **P**riority **N**umber)

SCADA systém průmyslového dohledu na systém (z anglického **S**upervisory **C**ontrol **A**nd **D**ata **A**cquisition)

DCS systém průmyslového dohledu na systém (z anglického **D**ecentralized **C**ontrol **S**ystem)

PLC programovatelný logický automat (z **a**glického **P**rogrammable **L**ogic **C**ontroller)

SIL bezpečnostní standard průmyslových zařízení (z anglického **S**afety **I**ntegrity **L**evel)

PČR Policie České republiky

DoS typ softwarového útoku (z anglického **D**enial **o**f **S**ervice)

DDoS typ softwarového útoku (z anglického **D**istributed **D**enial **o**f **S**ervice)

POPV metoda určení pravděpodobnosti (**P**římý **O**ptimalizovaný **P**ravděpodobnostní **V**ýpočet)

FORM metoda určení pravděpodobnosti (z anglického **F**irst **O**rder **R**eliability **M**ethod)

SORM metoda určení pravděpodobnosti (z anglického **S**econd **O**rder **R**eliability **M**ethod)

ANN umělé neuronové sítě (z anglického **A**rtificial **N**eural **N**etwork)

NIS evropská směrnice pro bezpečnost informačních sítí a systémů (z anglického **N**etwork **I**nformation **S**ecurity)

1. Úvod

S vývojem potřeb společnosti a ekonomiky narůstají i všeobecné nároky na dopravní infrastrukturu, přičemž se do určité míry dá říci, že její vývoj a rozšiřování je s ekonomickým růstem přímo spojený. Zároveň s neustále se měnícím společenským klimatem přichází nejen pozitiva, ale i nové hrozby. Tyto hrozby mohou z různých důvodů, ať už náboženských, politických či ekonomický ch, růst negativně ovlivnit, případně ohrozit bezpečnost nebo narušit stabilitu v určitých oblastech.

Ekonomiky mnohých států jsou z velké části závislé na průmyslových subjektech. V České republice je to například automobilový průmysl a strojírenství. Při moderním trendu přistupovat k výrobě strategií „just in time“, kde jsou dodávky dílů optimalizovány bez nutnosti jejich nákladného skladování v místě kompletace výrobku, by mohlo snadno dojít k ohrožení vý roby (například přerušením silničního nebo železničního spojení a tím zamezení dodávek dílů). To by prakticky znamenalo kolaps vý robní linky a stím spojené značné škody.

Dopravní infrastruktura sehrává též významnou roli v úloze bezpečnosti. Například v případě války je možné využívat některé dálniční komunikace jako provizorní letiště pro vzdušné síly Armády České republiky, nebo je naopak využívat pro evakuaci lidí z ohrožených oblastí a podobně.

Pro zamezení negativních dopadů je tedy nutné zajistit dosažení co nejlepší připravenosti a vytvoření důkladných krizových plánů. Pro tyto účely je nezbytné analyzovat různá související opatření a poskytnout tak informace pro praktické řešení možných hrozeb, což je jedním z hlavních cílů této diplomové práce.

2. Infrastruktura pozemních komunikací a legislativa

Pod pojmem pozemní komunikace se ve znění zákona č. 13/1997 Sb. rozumí dopravní cesta určená k užití silničními a jinými vozidly a chodci, včetně pevných zařízení nutných pro zajištění tohoto užití a bezpečnosti. Dělení pozemních komunikací je v České republice následující. [28]

Dálnice

Dálnicemi se rozumí silniční komunikace určená pro rychlou dálkovou přepravu. Slouží k mezistátní i vnitrostátní přepravě a nevyskytují se na nich úrovňová křížení. Možnost napojení je omezena po určitých úsecích, jízdní pásy jsou oddělené fyzickou zábranou a jakožto jediná z pozemních komunikací má stanovenou nejnižší povolenou rychlost. Vozidla, která nesplňují podmínku rychlosti, tedy jejich maximální konstrukční nebo provozní rychlost je nižší než minimální povolená, nemají na komunikaci volný přístup. Dle určení a dopravního vý znamu se dělí na dálnice I. a II. třídy. Dálnice spadají do vlastnictví státu a jejich užívání je zpoplatněno. [28]

Rychlostní komunikace

Dřívějším typem silničních komunikací byly také takzvané „rychlostní komunikace“. Od 1.1.2016, kdy došlo k legislativní změně zákona zákona o pozemních komunikacích č. 13/1997 Sb., spadají pod dálnice II. třídy nebo silnice I. třídy. Termín rychlostní komunikace lze však stále spatřit ve statistických srovnáních, pokud se provádí srovnání s roky před rokem 2016. Jedno ze srovnání je možno spatřit na obrázku číslo 1. [6]

Silnice

Silnicemi se rozumí veřejně přístupná pozemní komunikace, určená k užití silničními a jiný mi vozidly a chodci. Silnice nemají narozdíl od dálnic minimální povolenou rychlost. Obdobně jako dálnice se dle svého určení a dopravního využití dělí na silnice I., II. a III. třídy. Silnice I. třídy jsou ve vlastnictví státu. Zbylé třídy II a III jsou ve vlastnictví krajů, na jejichž území se nachází (od 1. října 2001). [28]

Místní komunikace

Místními komunikacemi se rozumí veřejně přístupné pozemní komunikace, které slouží primárně k místní dopravě na území dané obce. Opět se rozdělují dle určení a dopravního významu na třídy. V tomto případě na I., II., III. a IV. třídu, přičemž vlastníkem je vždy obec, na jejímž území se nacházejí. Parametry rozdělení jsou stanoveny zvláštním prováděcím předpisem. [28]

Účelové komunikace

Jako účelové komunikace se označují komunikace, které slouží například ke spojení jednotlivých nemovitostí pro potřeby jejich vlastníků nebo spojení nemovitosti s ostatními pozemními komunikacemi a podobně. Jako jediný typ komunikace může být ve vlastnictví fyzické nebo právnické osoby. Přístup na účelovou komunikaci může být na základě rozhodnutí vlastníka omezen. [28]

	2010	2014	2015	2016	2017	2018
Délka silnic a dálnic celkem	***55 751,9***	***55 747,6***	***55 737,5***	***55 757,3***	***55 756,4***	***55 744,0***
z toho evropská silniční síť typu E	2 635,8	2 627,5	2 627,7	2 627,9	2 631,1	2 630,2
Dálnice v provozu	***733,9***	***775,8***	***776,0***	***1 222,7***	***1 239,8***	***1 251,7***
Rychlostní komunikace[1)2)]	***422,3***	***459,4***	***459,4***	***0,0***	***0,0***	***0,0***
Silnice	***55 018,0***	***54 971,8***	***54 961,5***	***54 534,6***	***54 516,7***	***54 492,3***
v tom silnice I. třídy	6 254,6	6 233,2	6 244,9	5 807,3	5 824,8	5 817,9
silnice II. třídy	14 634,8	14 577,5	14 586,7	14 592,7	14 588,5	14 587,1
silnice III. třídy	34 128,6	34 161,1	34 129,9	34 134,6	34 103,4	34 087,3
Místní komunikace	***74 919,0***	***74 919,0***	***74 919,0***	***74 919,0***	***74 919,0***	***74 919,0***

1) Délka rychlostních komunikací je obsažena v délce silnic I. třídy
2) Od 1.1.2016 změny v evidenci pozemních komunikací; většina rychlostních silnic byla změněna na dálnice II. třídy.

Obrázek 1: Infrastruktura silniční dopravy (km) [6]

2.1. Dopravní infrastruktura

Pod pojmem infrastruktura se rozumí prvek nebo soubor prvků přímo zajišťující fungování nějakého systému. Lze ji dělit do mnoha odvětví, která spadají do různých oborů lidské činnosti, kvůli čemuž se může v různých oborech definice drobně odlišovat, nicméně se obecně jedná o „spodní vrstvu“ systémů, která zajišťuje právě jejich funkčnost. Z pohledu moderní společnosti, jak ji známe dnes ve vyspělých zemích, lze jmenovat jako významnou infrastrukturu například inženýrské sítě, telekomunikace, energetiku nebo občanské vybavení měst. Žádná z nich by se však neobešla bez infrastruktury dopravní. Ta je z pohledu ekonomiky velice významná především z toho důvodu, že slouží k transportu surovin, zboží, lidí a zajišťuje spojení mezi subjekty v prostoru, čímž přímo ovlivňuje socioekonomický rozvoj oblasti. [2] [3]

Dopravní infrastrukturou se rozumí dopravní stavby a zařízení s tím spojená. Její kvalita se přímo odráží na možnostech vývoje a zvyšování úrovně národního hospodářství. Vývoj infrastruktury je nutný i z pohledu vývoje automobilového průmyslu, kde dochází ve velké míře k využívání moderních „chytrých“ technologií. Příkladem mohou být technologie V2X, díky kterým vozidlo komunikuje s okolím, které by mohlo ovlivnit jeho jízdu. Tedy i se samotnou dopravní infrastrukturou. [3] [4]

Obecně lze dopravní infrastrukturu v České republice dělit dle typů dopravy do pěti hlavních částí čítající silniční infrastrukturu, železniční infrastrukturu, potrubní infrastrukturu leteckou infrastrukturu a vnitrozemskou vodní infrastrukturu. Následující podkapitoly se věnují podrobněji silniční dopravě a její infrastruktuře. Železniční, letecká, vnitrozemská vodní a potrubní doprava zde zahrnuty nejsou, jelikož je práce zaměřena na pozemní komunikace. [7]

Silniční infrastruktura v České republice se dělí do kategorií dle typů pozemních komunikací. Hlavními jsou dálnice v provozu, silnice a místní komunikace. Čtvrtým typem jsou poté účelové komunikace. Do silniční infrastruktury patří i sítě trolejbusů, tramvají a metra. Zpravidla bývají označované jako „elektrické trakce městské hromadné dopravy“ a spadají pod místní komunikace. S součástí silniční infrastruktury jsou taktéž související bodové, plošné nebo liniové prvky, například tunely, mostní konstrukce a podobně. Na obrázku číslo 1 je možno spatřit skladbu a délku silniční infrastruktury v České republice. [5] [6] [7]

2.2. Národní kritická infrastruktura

Kritická infrastruktura státu se týká pouze vnitřních záležitostí státu, ovlivňuje pouze jeho ekonomiku a obyvatelstvo. Nemá žádný vliv na okolní státy. Je tvořena vybranými prvky nebo soubory prvků dané infrastruktury, u kterých by po narušení jejich funkce došlo k závažným problémům. Ty by se mohly týkat zajištění základních životních potřeb obyvatelstva, ohrožení života nebo zdraví velkého množství osob, případně by též mohlo dojít k dopadu na ekonomiku státu a podobně. Do kritické infrastrutury jsou zahrnuti i provozovatelé daných prvků. Gesčně spadá pod Hasičský záchranný sbor České republiky a její parametry stanovuje zákon č. 240/2000 Sb. (krizový zákon). [1] [9]

Určování prvků spadajících do kritické infrastruktury v České republice má v kompetenci Ministerstvo vnitra. Pokud je objekt shledán prvkem KI, na základě návrhů ostatních ministerstev, ústředních správních úřadů nebo ČBN, je povinností jeho provozovatele zpracovat „Plán krizové připravenosti subjektu kritické infrastruktury“, který identfikuje možná ohrožení prvků a stanovuje postupy k jeho ochraně. Přičemž platí, že pokud je provozovatel odpovědný za plnění opatření v plánu krizové připravenosti, musí do něj též zahrnout i zabezpečení úkolů, které zajišťuje. [1] [9]

Postup určování prvků kritické infrastruktury, jejíchž provozovatelem je OSS, je následující: [1]

I. Ministerstva a ústřední správní úřady a ČNB zasílají Ministerstvu vnitra návrhy prvků KI a EKI, jejichž provozovatelem je OSS (§ 9 odst. 3 písm. d) a §13 odst. 4 písm. c) krizového zákona),
II. Ministerstvo vnitra zpracuje seznam, který je podkladem pro určení prvků KI a EKI, jejichž provozovatelem je OSS (§ 10 odst. 1 písm. f) krizového zákona),
III. vláda usnesením určí prvky KI a EKI, jejichž provozovatelem je OSS (§ 4 odst. 1 písm. e) krizového zákona).

V případě, že prvek není provozován OSS, je postup následující: [1]

I. Ministerstva, ústřední správní úřady a ČNB určí opatřením obecné povahy prvky KI a EKI.
II. O určení neprodleně informují Ministerstvo vnitra.

Určování prvků probíhá za pomoci odvětvových a průřezových kritérií pro určení prvků kritické infrastruktury. [1] [9]

Odvětvová kritéria pro určení prvku kritické infrastruktury

Odvětvová kritéria jsou definována v nařízení vlády č. 432/2010 Sb. S platností od 30. prosince 2010 a účinností od 1. ledna 2011. Vzhledem k jejich rozsahu jsou však obsažena v příloze, nikoli v hlavním textu nařízení. Týkají se nejvýznamnějších odvětví, která zajišťují fungování státu. Níže lze spatřit redukovaný výčet bodu V. se zaměřením na silniční dopravu. Ostatní kritéria se zaměřují na oblast energetiky, zdravotnictví, nouzové služby a podobně. [10]

V. DOPRAVA

A. Silniční doprava

Pozemní komunikace, která je zařazena do kategorie dálnice a silnice I. třídy[2]), pokud pro ni neexistuje objízdná trasa

B. Železniční doprava

Definuje kritéria týkající se železniční dopravy a s ní spojených objektů.

C. Letecká doprava

Definuje kritéria týkající se letecké dopravy a s ní spojených objektů.

D. Vnitrozemská vodní doprava

Definuje kritéria tý kající se vnitrozemské vodní dopravy a s ní spojený chobjektů.

Průřezová kritéria pro určení prvku kritické infrastruktury

Průřezová kritéria opět definuje nařízení vlády č. 432/2010 Sb., obdobně jako u odvětvových kritérií. Níže lze spatřit výčet hledisek, které musí prvek splňovat pro jeho zařazení do kritické infrastruktury. Pro jeho identifikaci jako součást kritické infrastruktury stačí, aby splňoval jen jedno z hledisek. [10]

a) hledisko obětí s mezní hodnotou více než 250 mrtvých nebo více než 2500 osob s následnou hospitalizací po dobu delší než 24 hodin
b) hledisko ekonomického dopadu s mezní hodnotou hospodářské ztráty státu vyšší než 0,5 % hrubého domácího produktu
c) hledisko dopadu na veřejnost s mezní hodnotou rozsáhlého omezení poskytování nezbytných služeb nebo jiného závažného zásahu do každodenního života postihujícího více než 125000 osob

2.3. Evropská kritická infrastruktura

Kritická infrastruktura, jejíž narušení by mělo významný dopad na Českou republiku a zároveň nejméně dva další členské státy Evropské unie, se označuje navíc přívlastkem „evropská“. Pro zařazení prvku nebo souboru prvků do úrovně evropské kritické infrastruktury je nejprve nutné, aby daný prvek nebo soubor prvků splňoval parametry pro národní kritickou infrastrukturu. [1] [12]

Podmínky pro zařazení prvku do EKI následně nestanovuje opět vláda, ale Rada Evropské unie. Nečiní tak však samovolně, ale vychází z návrhů Komise EU, stanovisek Evropského parlamentu a stanovisek Evropské centrální banky. V procesu se také bere v potaz smlouva o založení Evropského společenství (tzv. Římská smlouva z 25. března 1957), která politický m vývojem a několika konsolidacemi doznala podobu Smlouvy o fungování EU (tzv. Lisabonská smlouva z 3. prosince 2007). V současnosti se proces řídí směrnicí Rady 2008/114/ES ze dne 8. prosince 2008. [11] [12]

V případě, že prvek z národní kritické infrastruktury splňuje podmínky zařazení do evropské kritické infrastruktury, je členský stát EU povinen informovat o této skutečnosti všechny dotčené členské státy. S nimi poté jedná, ať už ve dvoustranných nebo vícestranný ch jednáních, o možných dopadech. V jednání se obdobně jako u národní kritické infrastruktury uplatňují průřezová a odvětvová kritéria. V případě, že se některý z členských států domnívá, že může být zasažen EKI na území jiného státu a nebyl přizván do jednání, může zažádat Komisi EU. Ta má poté za úkol neprodleně zajistit oznámení dotčeným státům a následně případně usnadnit jednání mezi jednotlivý mi stranami. [12]

V České republice byla jakožto evropská kritická infrastruktura identifikována pouze odvětví energetiky. V oblasti dopravy se v České republice nenachází žádné prvky natolik vý znamné, aby byly zařazeny do evropské kritické infrastruktury. [13]

2.4. Dokumenty kritické infrastruktury ČR

Hlavním legislativním dokumentem, týkajícím se kritické infrastruktury, je v České republice zákon č. 240/2000 Sb. a s ním související nařízení vlády č. 432/2000 Sb. Dalšími dokumenty, ne však již legislativního charakteru, pochází od Ministerstva vnitra – generálního ředitelství Hasičského záchranného sboru ČR. Jsou jimi například Národní program ochrany kritické infrastruktury, Koncepce ochrany obyvatelstva do roku 2020 s výhledem do roku 2030 nebo Komplexní strategie České republiky k řešení problematiky kritické infrastruktury. Následující podkapitoly se věnují právě těmto dokumentům.

Zákon č. 240/2000 Sb.

Celý názvem „Zákon č. 240/2000 Sb.: Zákon o krizovém řízení a o změně některých zákonů (krizový zákon)“ v platnosti od 9. srpna 2000 s účinností od 1. ledna 2001 je v současnosti již v jedenáctém znění dle novely 205/2017 Sb. v platnosti ode dne 14. července 2017 s účinností od 1. srpna 2017. V legislativě spadá do kategorií správního práva a ústavního práva. Součástí zákona je vymezení pojmů týkajících se krizových situací, pracovních povinností, ochranou kritické infrastruktury a podobně. Dále také vymezení pravomocí státních institucí, určení práv a povinností fyzických či právnockých osob v případech krizových situací. [13] [14]

Jakožto velice významnou novelu tohoto zákona lze jmenovat zákon č. 430/2010 Sb., kdy byla provedena úprava vnitrostátní legislativy zakomponováním evropské směrnice č. 2008/114/ES. Tím došlo k zavedení přesně definovaného postupu při určování kritické infrastruktury a společného přístupu k jejich ochraně i v rámci EKI. [13]

Nařízení vlády č. 432/2010 Sb.

Celým názvem „Nařízení vlády č. 432/2010 Sb.: Nařízení vlády o kritériích pro určení prvku kritické infrastruktury“ v platnosti od 30. prosince 2010 s účinností od 1. ledna 2011 prošlo ve své historii jednou novelizací a to sice dle nařízení vlády č.3015/2014 Sb. v platnosti od 19. prosince 2014 a účinností od 1. ledna 2015. [10]

Nařízení definuje odvětvová kritéria pro určování kritické infrastruktury dle typů odvětví. Jakmile dojde k určení prvku nebo souboru prvků do definovaných odvětví, jsou následně uplatněna průřezová kritéria, která slouží k finálnímu určení, zda daný prvek nebo soubor prvků spadá do kritické infrastruktury. [10]

Odvětvová kritéria se dělí do 9 skupin, přičemž jednotlivé skupiny se poté dělí na podskupiny a menší celky a detailně specifikují podmínky pro zařazení prvku do kritické infrastruktury. Jak již bylo zmíněno dříve v podkapitole 3.1, dopravě patří bod V. [10]

Komplexní strategie České republiky k řešení problematiky kritické infrastruktury

Dokument byl schválen 22. února 2010 s průběžnou platností a vychází z usnesení vlády ze dne 25. února 2008 číslo 170. Pojednává o kritické infrastruktuře v EU a NATO z pohledu vlivu na kritickou infrastrukturu v České republice. Dále obsahuje pricipy a cíle komplexní strategie České republiky k řešení dané problematiky a nakonec stanovuje místa a úlohy výzkumu a vzdělávání v oblasti ochrany kritické inftrastruktury. [17]

Národní program ochrany kritické infrastruktury

Dokument byl schválen taktéž 22. února 2010 s průběžnou platností, za účelem jasného vymezení konkrétních úkolů určených příslušným subjektům v případě krizové situace. Navazuje na dokument „Komplexní strategie České republiky k řešení problematiky kritické infrastruktury“. Zabývá se určováním odvětvových a průřezových kritérií a dále mimo jiné řeší i nahraditelnost a nenahraditelnost prvků. [15] [16]

Koncepce ochrany obyvatelstva do roku 2020 s výhledem do roku 2030

Dokument se ve své aktuální (třetí) podobě primárně zabývá ochranou civilního obyvatelstva České republiky, nicméně v jedné ze svých částech přímo pojednává i o problematice kritické infrastruktury. Konkrétně se jedná o podkapitolu 3.2.3 s názvem „Zvýšení odolnosti a ochrany prvků kritické infrastruktury proti možným rizikům a zajištění širšího zapojení subjektů kritické infrastruktury do procesu přípravy na mimořádné události a krizové situace a jejich řešení“. Jejím motivem je rozvíjet a zdokonalovat systém ochrany kritické infrastruktury na národní úrovni především z důvodu dosud nejasného dalšího postupu ze strany EU a snaha zachovat vývoj a řešení dané problematiky na národní úrovni. [18]

2.5. Unijní dokumenty evropské kritické infrastruktury

Vzhledem k tomu, že je Evropská unie společenstvím 27 různých států, snaží se oficiální unijní dokumenty sjednotit přístup pro řešení dané problematiky na evropské půdě. Cílem je zlepšit ochranu kritických infrastruktur a informovanost mezi jednotlivými členský mi státy, aby se zamezilo možným nežádoucím stavům a neinformovanosti. [12] [19]

Směrnice Rady č. 2008/114/ES

Směrnice byla vydána 8. prosince 2008, na základě žádosti Evropské rady na zasedání v červnu roku 2004. V účinnost vstoupila 12. ledna 2009 a členské státy byly povinny provést implementaci do národních legislativ do 12. ledna 2011 a jedná se o hlavní dokument dané problematiky. Žádostí bylo vypracování souhrnné strategie s cílem posílení ochrany kritický ch infrastruktur EU. Vydání proběhlo s ohledem na Smlouvu o založení Evropského společenství, návrh Komise, stanovisko Evropského parlamentu a stanovistko Evropské centrální banky. [12]

Mezi klíčové body směrnice patří určování a označování EKI, kde jsou opět uplatňována odvětvová a průřezová kritéria. Dále se jedná o plány bezpečnosti provozovatele, jejiž cílem je určení kritických prostředků EKI a stávajícího bezpečnostního řešení. V souvislosti na definování EKI směrnice udává povinnost zajištění styčného bezpečnostního úředníka, který má sloužit jako kontaktní místo mezi vlastníky nebo provozovateli EKI a příslušnými orgány.

Dále též udává povinnost předkládání zpráv v intervalech dvou let s povinností pravidelného přezkoumávání aktuálního stavu EKI na území příslušných států. [12]

Zelená kniha o Evropském programu na ochranu kritické infrastruktury

Tento dokument byl vypracován na základě zasedání Evropské rady v červnu roku 2004. Jeho cílem je především zapojení a sjednocení velkého množství subjektů ze státní i soukromé sféry do projektů ochrany kritické infrastruktury a získání konkrétních informací vhodný ch pro využití v daný chprojektech. Těmi jsou v současnosti dva EPCIP a CIWIN. O projektu EPCIP pojednává následující podkapitola. Projekt CIWIN se týká vybudování informační sítě pro předávání důležitých informací, týkajících se kritické infrastruktury a její ochrany, v rámci EU mezi členský mi státy.[21] [22]

Akční plán EPCIP

Podnět pro vytvoření akčního plánu EPCIP (celý názvem „Evropský program na ochranu kritické infrastruktury“) vzešel ze zasedání Evropské rady v červnu roku 2004. Plán je koncipovaný jakožto dokument pojednávající o předcházení, připravenosti a reakcích primárně na teroristické útoky na kritickou infrastrukturu. [20]

Mezi definovaný mizásadami, který mi se systémEPCIP má řídit patří: [20]

- subsidiarita – zaměření na kritickou infrastrukturu primárně z evropského pohledu, nikoli národního
- doplňkovost – snaha by měla doplňovat a navazovat na stávající řešení, nikoli je duplikovat
- důvěrnost – utajování informací tý kajících se kritické infrastruktury na unijní i národní úrovni
- spolupráce zainteresovaných subjektů – všechny subjekty zainteresované v dané kritické infrastruktuře budou spolupracovat, nebude docházet k upřednostňování státního aparátu nebo prostředků ze soukromé sféry
- proporcionalta – opatření budou navrhována pouze pro případy, kde byl zjištěn jejich nedostatek
- odvětvový přístup – kritická infrastruktura se bude dělit odborně dle odvětví a na jejich základě budou prováděny opatření pro zvýšení bezpečnosti

Sdělení Evropské komise Radě a Evropskému parlamentu o ochraně kritické infrastruktury při boji proti terorismu

Dokument slouží především jako shrutí dosavadního pokroku na poli ochrany kritické infrastruktury Evropské unie pro Evropskou radu a Evropský parlament. Ve své první části definuje hrozby, který m vsoučasnosti KI čelí a dále specifikuje evropskou kritickou infrastrukturu. Ve své další části pojednává o řízení bezpečnosti EKI a podává přehled o dosavadním pokroku v ochraně KI na úrovni EU. Na tuto část navazuje přehledem možného zvyšování schopnosti EU v rámci ochrany a v závěru se věnuje provádění Evropského programu na ochranu EKI. V úplném konci shrnuje budoucí cíle a ukazatele dosavadního pokroku. [23]

3. Technická zařízení a bezpečnostní opatření

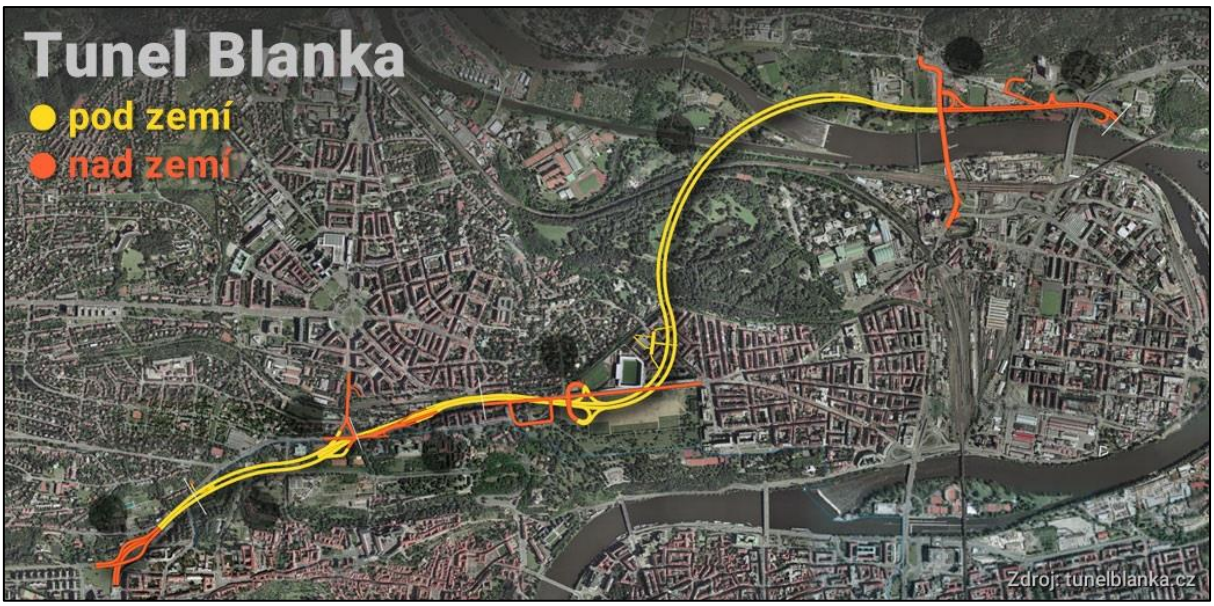
Technická zařízení na dopravní síti pozemních komunikací slouží k organizaci dopravy a pohybu dopravních prostředků“. Tedy v případě, že je potřeba vést komunikaci náročným terénem, například nad propastí, řekou nebo skrz vyvýšeniny, je nutné provést technická opatření, aby byl zajištěn bezpečný provoz. To vede k budování mostních nebo tunelový ch konstrukcí, železničních přejezdů a podobně. Tyto technická zařízení lze dělit do několika skupin podle jejich uspořádání. Následující kapitoly tedy pojednávají o prvcích bodových, plošných a liniový ch.[24]

3.1. Bodová technická zařízení

Do bodových prvků se zařazují technická zařízení, která na dopravní síti představují uzavřený celek. Díky povaze bodových prvků, které jsou zpravidla soustředěny na malé ploše, lze zajistit efektivní ochranu před možným nebezpečím. V následujících podkapitolách jsou podrobněji rozebrány vybrané bodové prvky. Nejedná se však o kompletní výčet a mohou mezi ně patřit i budovy s vazbami na konkrétní silniční infrastrukturu. [8] [25]

Tunely

Tunelem se na síti pozemních komunikací označuje liniový podzemní objekt, který m prochází pozemní komunikace. Jeho hlavní části jsou předportálový úsek, tedy část komunikace



Obrázek 2: Tunel Blanka [43]

navazující na portál tunelu. Portál je vstupní / výstupní část tunelu, která slouží pro vjezd / výjezd vozidel dle směru jízdy na komunikaci. Ten následně navazuje na tunelovou troubu, ta je opět zakončena portálem. Jízdní směry jsou odděleny v samostatných troubách a mohou být propojeny tunelovou propojkou. Provoz v tunelech je minitorován a regulován, přičemž může být omezen nebo úplně zapovězen některým vozidlům, která například přepravují materiály spadající do kategorie ARD, nebo jsou rozměrově nevyhovující a podobně. [29] [32] [62] [64]

V České republice je v současnosti nejdelším silničním tunelem pražský tunelový komplex Blanka. Ten tvoří na sebe navazující tunely Brusnický, Dejvický a Bunenečský scelkovou délkou 5 502 metrů. Na komplex následně navazuje tunel Mrázovka, Strahovský a Zlíchovský, které společně s Blankou tvoří téměř 9 km dlouhý úsek. [32]

Mosty

Pojmem most (mostní objekt) se rozumí objekt, který je součástí jedné nebo více komunikací a nahrazuje zemní těleso v místech, kde je v daném terénu potřeba překonat překážku přemostěním. Tyto objekty se světlostí do 2 metrů se označují jako propustky. Přímé označení most se využívá u objektů, jejichž světlost přesahuje 2 metry. Provoz na mostech může být omezen nebo regulován, například pro vozidla s hmotností přesahující určitou hranici nebo jsou rozměrově nevyhovující a podobně. Nejdelším mostem v České republice je v současnosti Radotínský most, který v celé své délce měří 2 281 metrů (uvádí se též 2 295 metrů). Celkový počet mostů je dle poslední zprávy z přehledu informačního systému ŘSD na silniční a dálniční siti v ČR 17 533 s celkovou délkou 407 365 metrů. [30] [33] [35]

Obrázek 3: Radotínský most [44]

Podjezdy

Jako podjezd se označuje stavba, která umožňuje průjezd dopravních prostředků pod již existující stavbou. Ze své podstaty se jedná o dodatečné řešení, které se využívá zpravidla ve městech, kde není možné jiné dopravní řešení. Jeho konstrukce je značně závislá na stabilitě konstrukce, která se nachází nad ním. [31]

Železniční přejezdy

Železničním přejezdem se rozumí místo, kde dochází k úrovňovému křížení pozemní komunikace a železniční dráhy. Podle vybavenosti se dělí přejezdy na zabezpečené a nezabezpečené. Zabezpečené přejezdy jsou vybaveny manuálním nebo automatický m zabezpečovacím zařízením, závorami a signalizací, která vizuálně i zvukově varuje řidiče před přijíždějícím vlakem. [28]

Nezabezpečené přejezdy jsou zpravidla vybaveny pouze výstražnými dopravními značkami. V některých případech se lze setkat s pojmem „přejezd zabezpečený výstražným křížem“. Toto označení je však značně zavádějící, protože se jedná o nezabezpečený přejezd. V daném místě se pouze nachází označení dopravní značkou, která řidiče informuje o přítomnosti přejezdu. [28]

Mimoúrovňové křižovatky

Mimoúrovňové křižovatky jsou stavby, ve kterých dochází ke křížení nebo stýkání různých pozemních komunikací ve dvou nebo více výškových úrovních a u kterých by nebylo z jejich povahy možné provést úrovňové křížení, tedy například dálnice. [34]

Ekodukty

Ekodukt je speciální mostní nebo tunelový objekt, který má za úkol zajistit bezpečnou možnost přesunu migrujících živočichů přes pozemní komunikace a zamezit jejich střetům s vozidly. Budování těchto staveb je prováděno z důvodu fragmentace krajiny. To znamená, že postavená pozemní komunikace prochází územím, které rozděluje na dvě nebo více částí, které již nemají plnohodnotné vlastnosti oproti původnímu celku. Tím zásadně ovlivňuje charakter krajiny a má přímý vliv na místní faunu i floru. [36] [37]

3.2. Plošná technická zařízení

V případě plošných prvků je nejprve nutné rozhodnout, pro jaký typ dopravy budou definovány. Podle typu dopravy lze některé prvky ze skupiny bodových zahrnout i do skupiny plošných, záleží zde na zvolené rozlišovací úrovni. [29]

Z pohledu železnice se do skupiny plošných prvků řadí železniční přejezdy s přejezdovým zabezpečovacím zařízením a železniční stanice se staničním zabezpečovacím zařízením. Analýza plošného prvku poté probíhá za pomoci kritérií kritičnosti liniových bodových prvků. Dále dle kritéria složitosti prvku a možnosti objezdu. [29]

To však nesouhlasí v případě přístupu z pohledu pozemních komunikací, kde v praxi nezáleží, zda přejezd má nebo nemá zabezpečovací zařízení a je obecně pouze bodem na síti pozemních komunikací. V tomto případě je tedy vhodnější jej řadit do prvků bodových. [25]

V případě pozemních komunikací se jeví jako možný vhodný příklad plošných prvků mimoúrovňové křižovatky. Ty svými proporcemi zabírají větší plochu v místě křížení a jsou soustavou několika samostatných bodů mimoúrovňového křížení. Opět by zde však záleželo na zvolené rozlišovací úrovni, jelikož je lze také považovat pouze za body na síti pozemních komunikací. Pro potřeby této práce jsou řazeny pouze jako prvky bodové.

3.3. Liniová technická zařízení

Liniové prvky lze definovat jako souvislou řadu více bodů. Na dopravní síti se typicky jedná o prvky spojující mezi sebou dva vybrané body, tedy pozemní komunikace a traťové úseky na železnici. Analýza liniových prvků se na železnici provádí na základě kritérií významu dráhy, výkonu dopravy, možnosti objezdu a rizika dráhy. Obdobný přístup lze aplikovat i v případě pozemních komunikací. [25] [26]

Z pohledu silniční dopravy lze jmenovat jako významné prvky silniční dopravy dálnice a silnice I. třídy, jejichž spravovatelem je Ředitelství silnic a dálnic a jak již bylo zmíněno, jsou ve vlastnictví státu. ŘSD, jakožto státní příspěvková organizace, zajišťuje výkon vlastnických práv státu k daným komunikacím, dále zabezpečení, údržbu, modernizaci a opravy. [27] [8]

3.4. Bezpečnostní opatření

Bezpečnostními opatřeními na kritické infrastruktuře se rozumí soubor opatření, jejichž úkolem je snížení možných rizik nebo jejich úplné odstranění. Konkrétní opatření mohou být vázána technické nebo organizační prostředky. [40]

Mezi důležité procedury v případě bezpečnostích opatření pro nestandardní situace na kritické infrastruktuře patří jejich standardizace. To znamená, že centrálně dochází k přesnému výběru a sjednocování postupů, reakcí a případně jejich kombinací tak, že jsou dané procedury následně prováděny předem určenými subjekty ve formě optimalizovaných variant. Cílem je především zamezení možných nežádoucích stavů při nutnosti kooperace více subjektů najednou, případně zvýšení efektivity a bezpečnosti prováděných postupů. Následující podkapitoly se zabý vajíjednotlivými skupinami bezpečnostních opatření podrobněji. [38]

3.4.1. Technická opatření

Do prvků technických opatření jsou řazeny fyzická zařízení pro zajištění monitorování daného prostoru, omezení vstupu do konkrétního prostoru nebo zajištění bezpečného provozu v případě nestandardního stavu. Při uplatňování technických opatření na konkrétním prvku KI lze prostor daného objektu klasifikovat na části podle významu. Tím se zajistí efektivnější uplatnění bezpečnostních opatření. Jeden z možných způsobů klasifikace je následující. [38] [39]

- Kontrolovaný prostor– požadavky na nejnižší úrovni zabezpečení, spojuje klíčová místa (například chodby)
- Chráněný prostor – požadavky na střední úroveň zabezpečení, prostor s důležitými místy, nikoli však klíčový mi pro funkci prvku KI
- Zvláště chráněný prostor – požadavky na nejvyšší úroveň zabezpečení, v daném prostoru se nachází fundamentální zařízení prvku KI, případně probíhá klíčová činnost pracovníků pro zajištění činnosti prvku

Monitorovací systémy

V případě monitorovacích systémů se typicky jedná o CCTV. Kamerový systém zajišťuje vizuální záznam, sloužící k dokumentaci pohybu dopravních prostředků a osob. Dále do této kategorie spadají systémy kontroly a evidence vstupu, dnes již standardně realizované pomocí RFID. [38] [39]

Mechanické zábranné prostředky

Úlohou mechanických zábranných prostředků je primárně vymezení chráněných zón objektu, omezení vjezdu vozidel nebo vstupu nepovolaných osob do konkrétních prostor a zabránění umístění nebezpečných předmětů v objektu nebo jeho okolí. Na příslušné technické řešení se vztahují ČSN normy pro jeho provedení. Následuje výčet typických zástupců MZP. [38] [39]

- betonová svodidla a kužely
- ocelová svodidla
- oplocení, bavolety
- dveře, turnikety, závory
- stavební konstrukce plášťů budov
- okna, mříže, zámky

Nouzové systémy

Jedná se o systémy, které v běžném provozu nejsou v aktivně zapojeny do fungování prvku KI a k jejich aktivací dochází v případě nestandardního stavu. Jejich úkolem je zmírnit dopad nestandardních stavů, zajistit alespoň částečnou funkčnost prvku a případně zajistit bezpečnou evkuaci osob, než dojde k nápravě. Jako zástupce lze jmenovat systémy nouzového osvětlení nebo záložní zdroje energie. [38]

3.4.2. Administrativní a režimová opatření

Administrativní opatření se týkají zajištění bezpečnosti dokumentů KI v papírové i elektronické podobě již od počátku jejich tvorby, následně nakládání s nimi a po vyřazení i postupu jejich likvidace. Důležitým prvkem je definování postupu a formy označování dokumentů, aby byla zajištěna jejich přesná identifikace a zpřístupnění oprávněným osobám. [39]

Režimová opatření jsou výsledkem kombinace opatření technických a administrativních. Slouží ke stanovení režimu a způsobu, kterým budou aplikována standardizovaná bezpečnostní opatření. Dále zajišťují vazby mezi technickými opatřeními a jeho uživateli. Souvisí tedy přímo s personálním obsazením daných objektů a činností jednotlivých pracovníků. [38] [39]

4. Odolnost systémů a druhy útoků

Odolnost systémů a zařízení KI představuje vlastnost odolávat působeních negativních vlivů a schopnost zajistit jejich fungování nebo, v případě poškození, schopnost se zotavit z následků nebezpečné události. Zajištění funkčnosti lze docílit rozličný mi způsoby, například flexibilitou činnosti, adaptací nebo obnovou funkce. [25] [41]

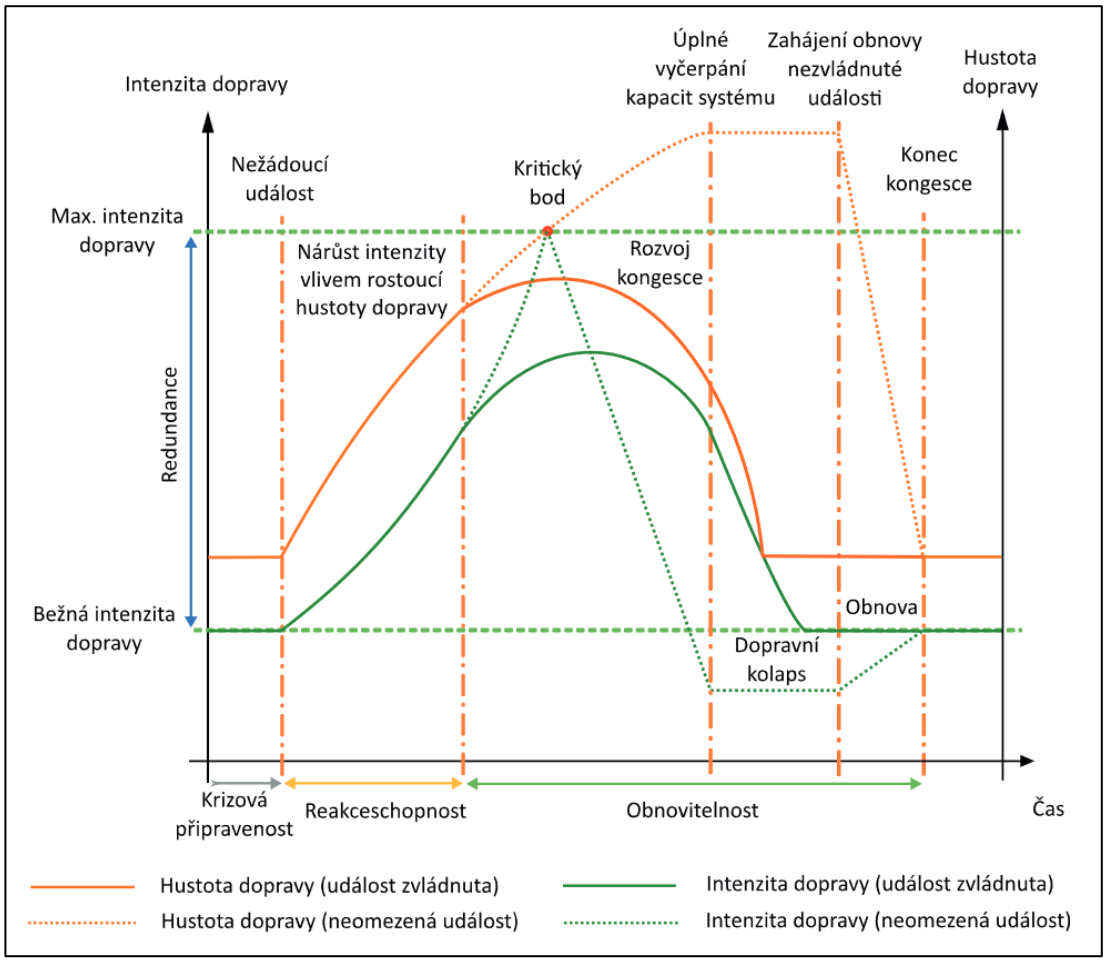
4.1. Principy hodnocení a ukazatele odolnosti

Proces hodnocení odolnosti prvku kritické infrastruktury lze provádět ze dvěma různými přístupy, interním a externím. Hlavní rozdíl mezi těmito dvěma způsoby je ten, že v případě externího hodnocení provádí hodnocení pozorovatel, který není součástí daného systému. V případě interního hodnocení lze provádět analýzu za pomoci vlastních zdrojů a vyhnout se tak vnějším subjektům. Následuje výčet principů, které se vyžívají při procesu hodnocení odolnosti. [25]

- Princip komplexnosti – při hodnocení odolnosti prvku je vhodné zahrnout všechny podstatné podněty, které zajišťují jeho cílovou funkci.
- Princip konkrétnosti – při hodnocení odolnosti prvku je vhodné využít co nejvíce dostupný ch údajů, týkajících se konkrétního prvku.
- Princip přiměřenosti – při hodnocení odolnosti prvku je vhodné zvolit vhodnou rozlišovací úroveň pro zajištění co nejlepší efektivity.
- Princip nestrannosti – při hodnocení odolnosti prvku je vhodné zajistit, aby hodnotitel nebyl zaujatý vůči činnosti, kterou má na starost. To lze dobře zajistit v případě externího hodnocení. V příapdě hodnocení interního je tento požadavek náročnější na realizaci.
- Princip odbornosti – při hodnocení odolnosti prvku je vhodné zajistit, aby hodnotitel byl odborníkem na danou problematiku a měl tedy i odpovídající zkušenosti a vzdělání.

V procesu hodnocení se využívá ukazatelů odolnosti prvků KI, na jejichž základě jsou poté prvky posuzovány. Následující přehled shrnuje základní ukazatele. [25]

- Robustnost – představuje stálost prvku při působení negativních vlivů a jeho schopnost zachovat si svou funkčnost bez významných degradací.
- Připravenost – představuje schopnost prvku odolávat předvídatelný m nestandardním situacím za pomoci předem vypracovaných opatření.
- Reakceschopnost – představuje schopnost prvku reagovat na nestandardní situaci. Její vyjádření je založeno na době mezi vznikem takové události a přijetím prvních opatření pro zajištění funkce prvku bez vý znamné degradacea následně jeho obnovy.
- Obnovitelnost – představuje schopnost prvku opět přejít do plně funkčního stavu po skončení nestandardní situace. Opět se zde využívá vyjádření za pomoci časového intervalu. Tektorát je však měřen od okamžiku, kdy bylo přijato první opatření pro zajištění funkčnosti, až po chvíli, kdy dojde k úplné regeneraci do původního stavu.



Obrázek 4: Dopad vysoké hustoty dopravního proudu na intenzitu dopravy [41]

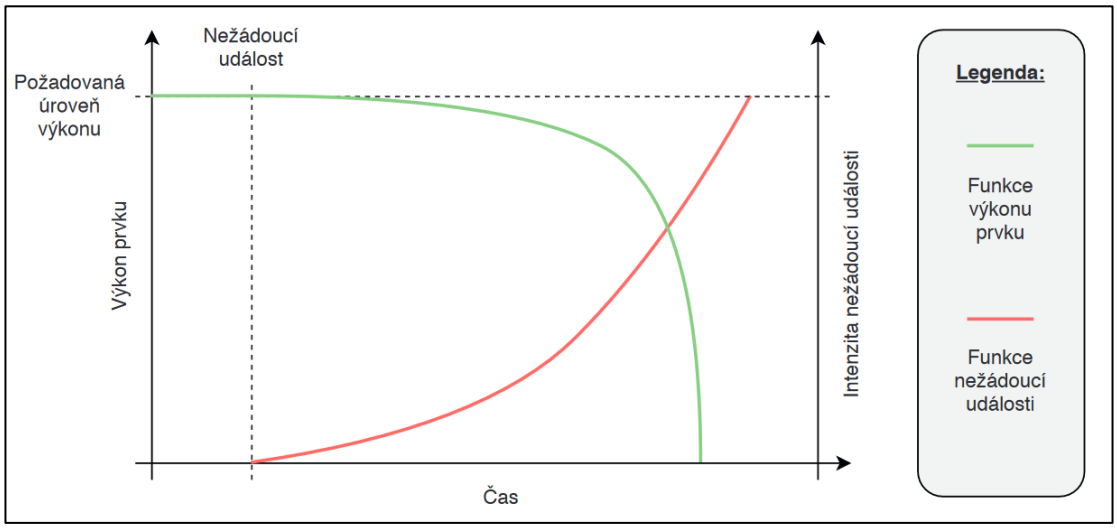
Na obrázku číslo 4 lze spatřit vztah intenzity dopravy a hustoty dopravního proudu v reakci na nestandardní událost. Na počátku diagramu lze spatřit, že výchozí stav dopravního proudu je rovnovážný s nízkou hustotou a nízkou intenzitou. Následně na dopravní proud působí nestandardní událost, kvůli které dochází k strmému nárůstu, avšak vozidla nejsou zatím příliš omezována, aby byla donucena snížit svoji rychlost. Dále dochází k dosažení kritického bodu a tím i vyčerpání robustnosti dané části infrastruktury a dochází k prudkému poklesu cestovní rychlosti při stálém nárůstu hustoty. Tento stav dopravního proudu se nazývá kongesce (někdy též „dopravní zácpa“) a typicky se projevuje maximální hustotou dopravy a minimální (až nulovou) cestovní rychlostí. Problematický je zejména ztoho důvodu, že se jedná o stabilní stav a k postupné obnově systému dochází až po výrazném poklesu hustoty dopravního proudu. Proces regenerace následně probíhá za stálého poklesu hustoty dopravního proudu, zvýšení intenzity až do stavu úplného obnovení. [41]

4.2. Hrozby a poruchy prvků

Při ochraně prvků kritické infrasktutury a vytváření krizových plánů je nutné definovat hrozby, který m mohou být prvky v provozu vystaveny. V případě, že je prvek vystaven hrozbám a nedisponuje dostatečnou odolností vůči danému typu hrozby, mohou se u něj začít projevovat poruchy, které zpravidla nejprve způsobí pokles výkonu a mohou mít až katastrofické následky na jeho funkčnost. Definicí hrozeb lze tedy zajistit vysokou efektivitu nouzový ch plánů a určité snížení nároků na lidský faktor, při jejich nasazení během nestandardní situace. Samotné hrozby lze dělit do pěti základních skupin, viz následující seznam. [41]

- meteorologické hrozby –způsobené zpravidla vlivem počasí, například povodně, požáry, vichřice a podobně.
- geologické hrozby –způsobené zpravidla podložím, na kterém se prvek KI nachází, například sesuvy půdy, zemětřesení a podobně.
- biologické hrozby – způsobené zpravidla činitelem virového nebo bakteriálního původu, působícím na živé organismy.
- technologické hrozby – způsobené zpravidla haváriemi technických zařízení. Jedná se například o úniky nebezpečných látek, nehody dopravních prostředků nebo havárie inženýrských sítí. Do této kategorie spadá i hrozba povodní, je-li způsobena poškozením uměle vytvořených vodních děl.
- kriminální hrozby – způsobené zpravidla lidskou činností. Jedná se například o národní i mezinárodní terorismus, ale i o obyčejnou kriminální činnost.

sDůsledky těchto hrozeb se následně projevují v podobě nežádoucích událostí, které vedou k různým poruchám a snížení výkonnosti. Dělení těchto událostí se odvíjí od typů hrozeb a jedná se o tří základní kategorie: *úmyslné antropogenní události* (důsledek kriminálních hrozeb), *neúmyslné antropogenní události* (důsledek technologických hrozeb) a *naturogenní události* (důsledek meteorologických, geologických a biologických hrozeb). [41]



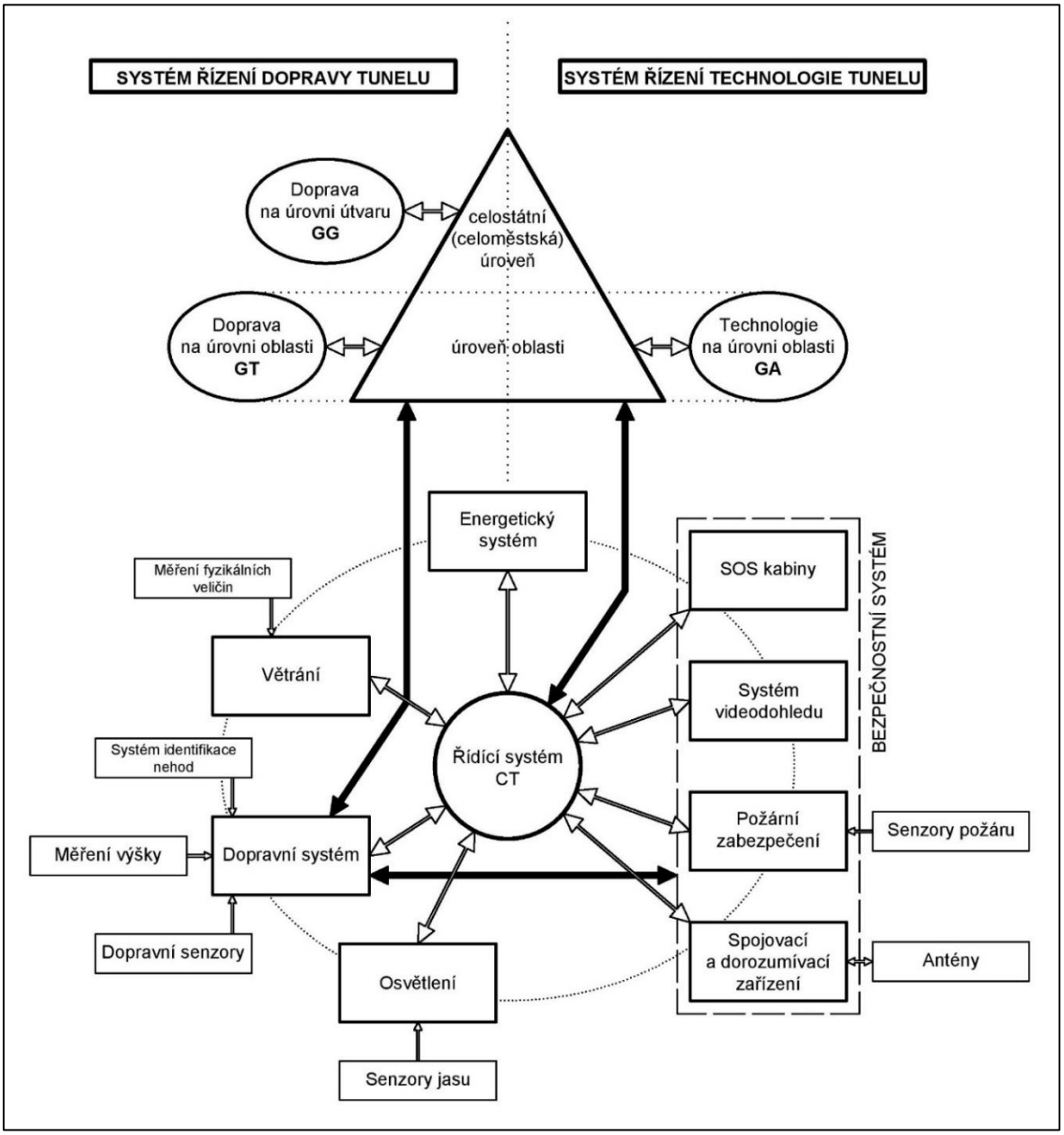
Obrázek 5: Narušení prvku KI [41]

Samotné poruchy se následně mohou v systému šířita způsobovat další nežádoucí stav a selhání. Dle typu šíření lze poruchy dělit do následujících kategorií. [41] [42]

- Kaskádní porucha – nastává selháním prvku nebo souboru prvků v jednom typu infrasktruktury, které následně ovlivní i další systémy jiný ch infrastruktur. Typicky se může jednat o poruchy v energetické infrastruktuře a následný dopad na dopravní infrastrukturu a podobně.
- Eskalační porucha – nastává v případě, že se vyskytnou dvě na sobě nezávislé poruchy v různých typech infrastruktury a kvůli jedné z nich dojde ke zhoršení situace na druhé infrastruktuře. Typicky se může jednat o závady na energetické infrastruktuře nebo na telekomunikačních sítích, které mají vazbu na dopravní infrastrukturu.
- Společná porucha – nastává v případě selhání více infrastrukturních prvků nebo skupin prvků vlivem jednoho činitele. Typicky se může jednat například o záplavy, které ovlivní jak dopravní infrastrukturu, tak energetickou infrastrukturu a mnoho dalších.

5. Druhy útoků

Útoky na slabá místa KI pozemních komunikací lze dělit do dvou základních kategorií podle způsobu provedení útoku. První kategorií by byly dálkové útoky softwarové povahy, například na hlavní řídící stanici tunelové stavby (CT) a jí nadřazenou řídící ústřednu (GG), viz obrázek číslo 6. Hlavní řídící stanice komunikuje s veškerým technickým vybavením tunelu a její ovládnutí by tedy útočníkovi defakto umořnilo přístup do všech systémů, kterými je stavba vybavena.



Obrázek 6: Systémy silničního tunelu (kreslil autor 2020 dle [47])

Druhou kategorií by poté byly útoky fyzické povahy přímo v místech dané infrastruktury. Například s cílem dostat se přímo ke zdroji nebo cíli komunikace (tedy GG, GT, GA, CT) a poté provádět záškodnickou činnost na místě. Následující podkapitoly pojednávají o dané problematice podrobněji.

5.1. Vzdálené útoky

Do podkapitoly vzdálených útoků patří typicky počítačové útoky. Jejich výhodou je zejména to, že se útočník nemusí fyzicky vyskytovat v místě daného prvku infrastruktury. Prakticky bez omezení se může nacházet kdekoli na světě, pokud dané místo poskytuje vhodné připojení k počítačovým sítím. Největší překážku poté představují pouze zabezpečení cílového software a použité komunikační standardy a jejich zabezpečení. V případě nezodpovědného přístupu správního subjektu je možné, že nepřímo usnadní útočníkovi práci užíváním starých verzí softwaru, na které již nemusí existovat podpora od výrobce. Úplnou ztrátou podpory se software stává zranitelnějším z toho důvodu, že již nevychází pravidelné aktualizace a záplaty chyb, které se v něm vyskytují.

Provedení těchto útoků je ovšem podmíněno otevřeností systému vnějšímu okolí, tedy například připojením elektroniky do sítě internetu. Pokud je systém oddělený od globálních sítí, nelze vzdálené útoky na zařízení provést. Lze však stále útočit na komunikaci jednotlivých zařízení mezi sebou. V případě tunelových staveb, jakožto prvku KI, je snaha zajistit co největší izolaci systému (viz obrázek číslo 6), počítače a začízení využívaná v řídících ústřednách tedy nejsou připojena k internetu ani neumožňují přístup cizích zařízení.

Komunikační standardy dle TP 98

Ke zjištění užívaných standardů při komunikaci jednotlivých uzlů prvku kritické infrastruktury byly využity Technické podmínky. Konkrétně se jedná o TP 98 (Technologické vybavení tunelů pozemních komunikací) z toho důvodu, že popisují doporučenou komunikaci mezi jednotlivými komunikačními uzly v procesu řízení. Pro dálkovou komunikaci doporučují pouze dvě možnosti, standardy ATM a X.25. Bylo taktéž kontaktováno několik společností, zabývajících se danou problematikou, dotazy však zůstalybez odpovědi. [45]

TP 98 byly publikovány v roce 2004 a od jejich publikace neproběhla žádná aktualizace týkající se komunikační části. Z právního hlediska se sice nejedná o závazný dokument, ale v České

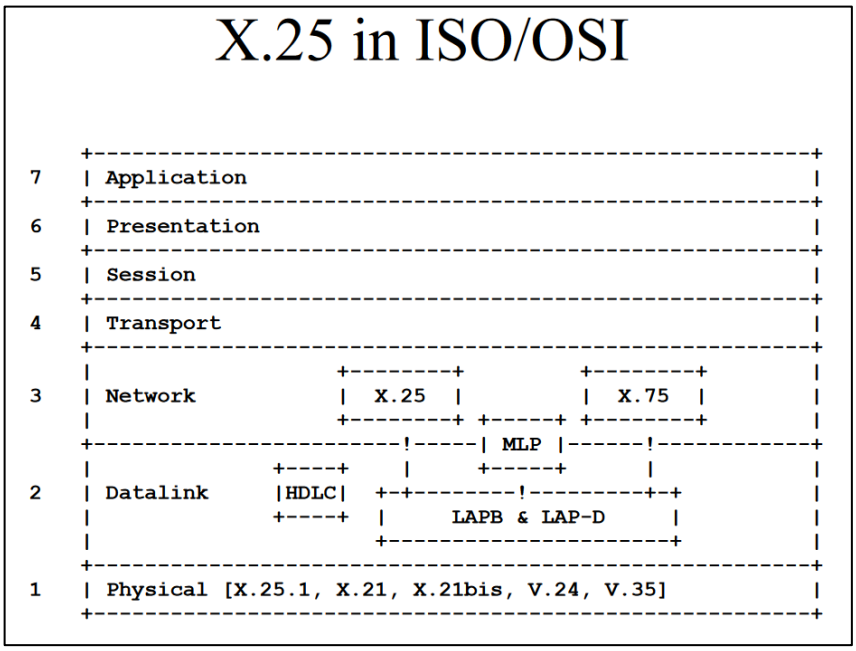
republice slouží jako respektovaný zdroj doporučení a varování při řešení problematiky pozemních komunikací. Nabízí se tedy opodstatněný důvod provést ověření, zda jsou dané standardy stále vhodné k doporučení a zda nedošlo k vývoji efektivnější a spolehlivější technologie. Několik autorů již přišlo s podněty týkajících se možných bezpečnostních rizik těchto standardů a po 16 letech lze očekávat, že dané technologie budou již překonané. [45] [53] [56]

Standard ATM

První z doporučených řešení pro dálkovou komunikaci na úrovni WAN je dle TP 98 standard ATM (z anglického **A**synchronous **T**ransfer **M**ode). Jedná se o vysokorychlostní standard pro přenos dat, definovaný ke konci osmdesátých let založený na metodě spojované komunikace (anglicky connection-oriented method). Pro přenos dat jsou využívány pakety s pevnou délkou, přičemž před samotným přenosem dat je nutné zajistit spojení mezi koncovými body. Tyto skutečnosti zajišťují, že je spojení spolehlivé a lze při něm využít složitějšího zabezpečení. [45] [46]

Standard X.25

Druhé z doporučených řešení pro dálkovou komunikaci na úrovni WAN je dle TP 98 standard X.25. Jedná se o technologii pocházející ze sedmdesátých let a byla vytvořena jako globální standard pro sítě s přepojováním paketů. Vzhledem k době vzniku a užití na metalických sítích,



Obrázek 7: X.25 ISO/OSI [53]

obsahují pakety velkou část informací sloužících k opravě chyb. To zajišťuje spolehlivost přenosu, avšak má za následek relativně nižší přenosovou rychlost. Na obrázku číslo 7 lze spatřit zařazení standardu X.25 v referenčním modelu ISO/OSI [45] [47]

Zabezečení ATM a X.25

Zabezpečení komunikačních standardů, nejen jmenovaných v TP 98, slouží k ochraně komunikace před zneužitím nebo útoky třetí strany. Mezi méně sofistikované útoky pak patří například odposlechy, rušení nebo zahlcení. Do sofistikovanějších by poté spadaly například úprava přenášených data, podstrčení falešných dat nebo doplnění o skrytý škodlivý software. [50]

Komunikační standard ATM využívá více způsobů zabezpečení. Patří mezi ně například šifrovaný přenos dat s využitím privátních/veřejných klíčů, kde oba konce mají svůj privátní klíč, jejímž odesílaná data zašifrují, a veřejný klíč, kterým si opačná strana obdržená data dešifruje. Dále se například využívá kontrola subjektů před započetím komunikace, autentizace integrity a původu dat a podobně. [49]

V případě standardu X.25 se opět využívá více způsobů zabezpečení. První z možností je princip koncového šifrování (anglicky „end-to-end encryption“), kdy komunikaci mohou rozšifrovat pouze koncoví účastníci a data jsou po celou dobu přenosu zašifrovaná. Dále existuje možnost kanálového šifrování (anglicky „link encryption“). V tom případě jsou odesílaná data zašifrována, ale na cestě k cíli musí být v každém uzlu dešifrována, aby se zjistila jejich následující destinace. Po jejím zjištění dochází k opětovnému zašifrování a odeslání a tímto způsobem data putují až do koncového bodu. Dalším způsobem ochrany je například aplikace hašovacích funkcí (z anglického „hash“), ověřování druhé strany před zahájením přenosu dat. [48]

Vzhledem k tomu, že je při elektronické komunikaci využíváno hašovacích funkcí, šifrování za pomoci klíčů, ověřování koncových uzlů a mnoha dalších způsobů zabezpečení, lze konstatovat, že je daný koncept bezpečný a možnost úspěšného útoku mizivá. Tato skutečnost ovšem platí s jistotou pouze v případě, že je využíván systém v aktuální verzi, nebyly prozrazeny privátní šifrovací klíče a jsou využívány aktuální šifrovací algoritmy, které nebyly překonány. Prozrazení klíčů by musel mít na svědomí člověk s přímým přístupem k hardwaru, jelikož je není možné získat běžnými postupy ani odposlechy. Šifrovací algoritmus je považován

za bezpečný v případě, že by jeho dešifrování trvalo značné množství času. To je u moderních algoritmů stovky i tisíce let.

5.2. Elektronické a softwarové hrozby

Mezi elektronické a softwarové hrozby se řadí činnosti, ve kterých je využito elektronických zařízení, ovšem vzhledem k uzavřenosti systému nejsou využity na dálku, ale přímo na místě prvku kritické infrastruktury. Útoky jsou značně omezené i díky oddělení systému od globálních sítí. Přímo souvisí s překonáním fyzického zabezpečení, které je rozebíráno v podkapitolách 5.3 až 5.6.

Provedení takového útoku je podmíněno přímým přístupem k fyzickému zařízení a může tedy být způsoben i samotným personálem. Nemusí se však vždy jednat o úmysl, může se jednat o obyčejnou nevědomou chybu neznalého uživatele, který například připojením vlastního infikovaného (USB a podobně) zařízení k pracovnímu počítači nakazí daný stroj škodlivým softwarem. Je tedy více než vhodné fyzicky omezit a zakázat využívání a připojování vlastních zařízení do síťových prvků, kterými jsou počítače, servery a podobně. Mezi tyto útoky a hrozby patří například následující.

Firewall

Pod pojmem firewall se rozumí síťové zabezpečení, které zajišťuje správu a monitorování odchozí a příchozí komunikace mezi zařízeními v síti na straně daného zařízení. V případě uzavřeného systému je nutné přesně nastavit, jaké porty se mohou při komunikaci zařízení využívat a všechny zbylé zakázat pro jakékoli jiné možné využití. Jedná se o základní ochranu, která však může být při správném nastavení velice efektivní. Nedovolí totiž zařízení komunikovat, jelikož porty, které jsou již přiřazené aplikacím nelze využívat více aplikacemi najednou a nezbývá tedy místo pro další komunikaci. Firewall může být jak softwarový, tak hardwarový, přičemž v případě využití na citlivých prvcích je vhodné využívat oba způsoby, čímž se docílí silnějšího zabezpečení. [77]

Malware

Pojmem malware se označuje škodlivý software, který může různým způsobem ovlivňovat elektronická zařízení v síti. Software může být do uzavřené sítě dopraven právě připojením cizího zařízení, jakým jsou USB flash disky, ale i počítačové myši a jakákoli další elektronika,

která je schopna komunikace s počítačem přes USB nebo jiný typ konektoru. Proto je důležité zamezit možnosti připojování vlastních uživatelských zařízení. Do skupiny patří například následující typy softwaru. [75] [76] [78]

- počítačové viry – typ softwaru, který může v síti škodit například ukončováním nebo blokováním důležitých procesů. Je schopný se šířit mezi zařízeními připojenými v síti a za krátkou dobu může infikovat i celou síť a začně ovlivnit její funkčnost.
- ransomware – typ softwaru, který zašifruje data silnou šifrou, kterou v některých případech ani nelze prolomit a následně vyžaduje výkupné za odblokování dat.
- spyware – typ softwaru, který sleduje činnost uživatele a jeho cílem může být například zisk přístupových hesel a podobně.
- keylogger – jedná se o program, který monitoruje a zaznamenává stisk tlačítek klávesnice a odesílá vytvořený záznam třetí straně.

SQL injekce

Jedná se o typ útoku zaměřený na SQL databáze které mohou sloužit k ukládání citlivých dat. SQL injekce principielně funguje tak, že se například v přihlašovacím okénku do databáze místo položky přihlašovací jméno vyplní SQL příkaz, který je následně zpracován systémem a pokud tato možnost není ošetřena, může mít za následek kritické poškození dané databáze včetně jejího kompletního smazání nebo zisku přístupových jmen, hesel a dalších citivých informací. [79]

DoS

Útok typu DoS funguje na principu zahlcení komunikační sítě. Lze jej provádět i za pomoci jednoho zařízení, což je značně nebezpečné i pro uzavřené sítě. Narozdíl od typu DDoS, pro jehož provedení je nutno využívat velké množství zařízení (například tisíce až desetitisíce zařízení), které v uzavřené síti vůbec nemusí být k dispozici a útočník by je musel na místo dopravit, což představuje značný logistický problém. Výsledkem takového útoku je nedostupnost napadený chzařízení právě z důvodu jejich přetížení. [74]

USB killer

Jedná se o eletronické zařízení, vizuálně podobné USB flash disku. Není ovšem vybaveno paměťovým úložištěm, ale kondenzátory. Ty se po připojení nabijí dokud nedosáhnou napětí v rozmezí -220 až -240V, které následně uvolní po datovém (komunikačním) vedení. Pokud

dané zařízení ustojí daný impulz, dojde následně ihned k opakování, dokud je zařízení v provozu a je schopno nabíjet kondenzátory. Pokud napadené zařízení není vybaveno ochranou proti tomuto typu útoku, dojde k jeho úplnému fyzickému zničení během velice krátké doby. [80]¨

5.3. Kybernetická bezpečnost

S elektronickými a softwarovými hrozbami přímo souvisí kybernetická bezpečnost. V České republice tuto problematiku řeší zákon č. 181/2014 Sb.: Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), na poli Evropské Unie následně evropská směrnice NIS a Evropská agentura pro kybernetickou bezpečnost (ENISA). [85] [86] [87]

Zákon o kybernetické bezpečnosti v tuto chvíli zmiňuje dopravu jakožto položku v §2 ohledně nutnosti zajištění zabezpečení základních služeb, jejichž narušení by mohlo mít vážné dopady na společenské nebo ekonomické činnosti v odvětví dopravy. Blíže se zaobírá řešením problematiky pouze kritické informační infrastruktury, nikoli jiný mi kritický mi infrastrukturami na území České republiky. [85]

Směrnice NIS je prvním evropským dokumentem, který řeší bezpečnost informačních systémů na úrovni sítí napříč všemi členskými státy EU. Hlavním cílem je vytvořit jednotné požadavky na státy v oblasti kybernetické bezpečnosti a jejich přístup k řešení této problematiky. [86]

Úkolem agentury ENISA, jakožto orgánu EU, je zajistit správnou a účinnou kooperaci členských států na poli kybernetické bezpečnosti. Toho má docílit za pomoci nového „aktu o kybernetické bezpečnosti“, který vstoupil v platnost v roce 2019. Agentura též řeší certifikace produktů a služeb v EU, což by mělo zajistit vyšší mezinárodní kompatibilitu a snížení nákladů. [87]

5.4. Útoky v místě prvku

K provedení fyzického útoku na kritickou infrastrukturu se útočník musí nacházet přímo v její lokalitě. Je tedy nezbytně nutné předvídat možné scénáře a přijímat bezpečnostní opatření fyzického charakteru, které zabrání proniknutí útočníka nebo skupiny útočníků do daného areálu, budovy nebo objektu a znemožnit přístup k citlivému vybavení.

Nelze se však spoléhat pouze na vnější zabezpečení budovy nebo areálu, je též nutné mít na paměti zabezečení vnitřních prostor. V případě, že by se útočníkovi podařilo překovat první úroveň zabezpečení, představující například vstupní dveře do budovy, jeho činnost značně zkomplikuje využití bezpečnostních zámků, dveří a dalšch prvků uvnitř samotného areálu a budov.

5.5. Fyzické zabezpečení objektů

Fyzické zabezpečení má za úkol zamezit vstupu nepovolané osoby do určitých prostor. Nejjednoduššími způsoby fyzického zabezpečení objektů jsou mechanické zámky. Ty taktéž tvoří základ všech dalších systémů, které mají za úkol bezpečně uzavřít konkrétní objekt a zajistit udržení tohoto stavu až do příchodu osoby způsobilé k jeho odemčení. Jejich praktická aplikace sahá od jednoduchých zámků na poštovních schránkách až po mnohem komplexnější systémy například u trezorových místností.

Vstup do objektu i v rámci objektu do jednotlivých místností lze řešit třemi základními způsoby. Výsledná volba provedení však přímo ovlivňuje celkové zabezpečení objektu a je nutné předem přesně definovat plánované využití daného místa. V praxi však může být značně limitována rozpočtem na realizaci.

5.5.1. Nezabezpečený vstup

Prvním způsobem vstupu je nezabezpečený vstup, případně pouze hlídaný za pomoci CCTV. Ten je ze své podstaty naprosto nevhodný pro prvky KI, protože umožňuje vstup doslova komukoli bez nutnosti jeho identifikace. V případě, že by fyzická ostraha, pracující se záznamem z kamer, měla na takovou situaci reagovat, nedá se s jistotou říci, že se jí podaří případného narušitele včas dostihnout a zajistit. Objekt je tedy v případě nezabezpečeného vstupu zcela otevřený okolí a jeho ochrana je značně náročná, ne li prakticky nemožná.

5.5.2. Vstup zabezpečený mechanický m zámkem

Jako první mechanické zámky jsou označovány uzly na provázcích, kterými byly v dávných dobách zajišťovány cennosti před odcizením. Ze své podstaty však neposkytovaly přílišné zabezpečení a sloužily spíše jako indikátor, zda s daným předmětem někdo interagoval bez vědomí majitele. Výskyt prvních mechanických zámků, kde byl využit koncept klíče,

se datuje do období starověkého Egypta (cca 4000 př.Kr.). K jejich výrobě se používalo dřevo a odemykání bylo založeno na základě použití čepů, které se musely vyzdvihnout do správné polohy zasunutím klíče. Tím došlo k uvolnění závorníku a bylo možné zámek otevřít. Metalické zámky se poprvé objevily ve starověkém Římě (cca 700 př.Kr.), kde byly využívány kovy jako je železo, bronz nebo měď. Technické řešení zámku za pomoci čepů se zachovalo do dnešních dní a stále patří mezi nejrozšířenější na světě, byť má již naprosto odlišnou podobu i použité materiály. [51]

Konstrukce moderních zámků čerpá především z vývoje materiálového inženýrství, moderních způsobů zpracování materiálu a při jejich výrobě se využívá výhradně kovů, například oceli nebo mosazi. Došlo též k fyzickému oddělení jednotlivých částí. Konkrétně se jedná o dvě základní části, které spolu interagují. První se nazývá cylindrická vložka a lze ji měnit dle potřeb, zpravidla vyšroubováním jistícího šroubů uvnitř dveřní konstrukce. Cylindrická vložka poté pracuje se střelkou a závorou, které tvoří jeden montáží celek, viz obrázek 8. Střelka slouží k zajištění zámku v uzavřené poloze a může být ovládána klikou. Závora slouží k uzamčení zámku do metalického protikusu vysunutím.

Mezi základní typy mechanických zámků patří následující:

- standardní mechanický – zámek zůstává ve stavu, do kterého je uveden za pomoci klíče
- samozamykací mechanický – zámek se po uzavření automaticky uzamkne
- mechanický sbezpečnostní střelkou – střelka zámku je dvojtá nebo je vybavena pojistkou, která slouží jako ochrana proti pokusům o otevření zámku zatlačením střelky při zasunuté závoře

Vstup zajištěný mechanickým zámkem tedy již má základní ochranu před vnikem cizích osob, protože je podmíněn držením konkrétního klíče. Není však vhodný pro místa s velkou intenzitou pohybu osob, protože odemykání zámku zabírá značné množství času. Je tedy nutné myslet na lidský faktor a neochotu vykonávat zdržující maličkosti. V případě užití mechanického zámku v místě s vyšší intenzitou pohybu osob by tedy mohlo docházet k situacím, že bude najednou procházet dveřmi více osob, aby si ušetřili čas a hledání klíčů k odemykání.

Nevýhodou je též to, že může docházet ke ztrátám klíčů nebo jejich poškození vlivem neopatrného zacházení. Pokud jsou klíče vystaveny hrubému zacházení, může dojít k deformaci odemykacích ozubů a jemná mechanika zámku s poškozeným klíčem nemusí správně fungovat. V případě, že se jedná o obyčejný klíč, lze jej snadno nahradit vyrobením nového. V případě bezpečnostního klíče, který je vázán na sériové číslo cylindrické vložky je situace složitější. Nelze jej totiž bezpodmínečně kopírovat a k výrobě kopií je nutné předložit příslušné doklady.

Typy mechanických klíčů

Jak již bylo zmíněno, existují dva základní typy mechanických klíčů. Prvním typem jsou standardní klíče, které lze běžně kopírovat v zámečnictví na základě volně dostupných polotovarů. Jejich výroba je podmíněná pouze předložením originálu a není nijak regulována. V případě, že je originální klíč ztracen, kopii lze též vyrobit na základě předložení samotné cylindrické vložky.

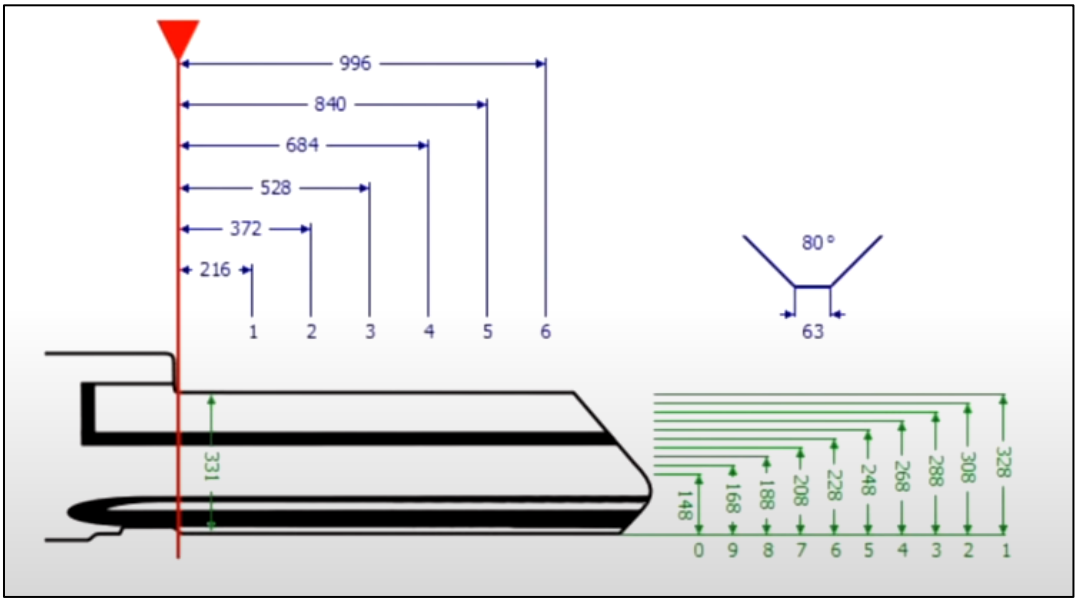
Druhým typem mechanických klíčů jsou bezpečnostní klíče. Polotovary bezpečnostních klíčů

Obrázek 8: Konstrukce zámku s cylindrickou vložkou (foto autor 2020)

nejsou běžně dostupné a jejich zakoupení je podmíněno prokázáním se kartou s výrobním číslem zámku. V některých případech je nutné polotovar objednat nebo nechat celý klíč zhotovit přímo u výrobce cylindrické vložky. Na kartě se též uvádí profil klíče a číselná kombinace použitých zubů (hloubek). Na obrázku číslo 9 na následující straně lze spatřit dva druhy bezpečnostních klíčů, přičemž klíč vpravo má na sobě vyražené sériové číslo.

Na obrázku číslo 9 je také možno vidět dva typy klíčů dle mechaniky cylindrické vložky. Rozměr klasických zubů je přesně definován výrobcema a identifikátor klíče, lze zapsat i číselně dle hloubky zubů. Stupnici takového číslování je možno spatřit na obrázku číslo 10, rozměry jsou uvedeny v tisícinách amerického palce. Konstukce levého klíče je však již značně odlišná, to především ztoho důvodu, že se jedná o klíč ke komplexnější cylindrické vložce, jejíž mechanika není volně k nahlédnutí.

Obrázek 9: Bezpečnostní klíče (foto autor 2020)



Obrázek 10: Rozměry klíčových zubů (tisíciny amerického palce) [55]

5.5.3. Vstup zabezpečený elektrický m zámkem

Elektronický zámek představuje další evoluční krok od klasického mechanického zámku. V tomto případě není uzamykací systém ovládán manuálně otočením klíče, ale za pomoci elektrického proudu. Oproti manuálně ovládaným zámkům mají velkou výhodu v různých možnostech odemykání a lze využívat jak kontaktních, tak bezkontaktních typů klíčů. Mohou, ale nemusí, bý tvybaveny cylindrickou vložkou pro nouzové případy otevření. [52]

Základní dělení dle ovládání pohyblivých částí zámku je následující: [54]

- elektromechanické – pohyblivý mechanismus zámku je zajištěn až po přivedení elektrického impulzu na elektromagnetickou cívku. V případě, že impulz nebyl udělen, klika je sice pohyblivá, ale není propojena s pohyblivý m mechanismem zámku a nelze jej otevřít.
- elektromotorické – pohyblivý mechanismus zámku je ovládán elektomotorem. Odemykání probíhá tak, že je nejprve elektromotorem zatažena závora a poté dochází k odblokování střelky.
- elektromagnetické – provedení elektromagnetických zámků může být vícero způsoby. Nejčastějšími jsou zámky bez střelky s elektromagnetick ovládanou závorou nebo zámky s pohyblivou, elektromagneticky ovládanou západkou (protikusem). Ta je v základní pozici nepohyblivá a po udělení elektrického impulzu dochází k vypnutí elektromagnetu, západka se stává pohyblivou a zámek lze otevřít.

Typy elektronických klíčů

Jak již bylo zmíněno, elektronické klíče lze dělit do dvou základních skupin – kontaktní a bezkontaktní. Následující seznam shrnuje základní přehled možných technických řešení.

- Kontaktní klíče – u klíčů je nutný fyzická interakce s čtecím zařízením a nelze s nimi odemknout zámky na jakoukoli větší vzdálenost než je přímý kontakt se zámkem.
    - kódové – typicky se jedná o alfanumerická hesla, která je nutno napsat do přístupové jednotky za pomoci klávesnice. Výhodou je, že nemají fyzickou podobu a nelze je kopírovat, pokud je jejich držitel sám někomu nesdělí nebo nezodpovědným jednáním vyzradí. Jejich nevýhodou však je, že je lze snadno zapomenout.
    - elektromechanické – jedná se o starší typ klíčů, kde je klíč tvořený například kartou s výstupky vurčitém uspořádání. Čtecí zařízení, například za pomoci optického snímače nebo elektromechanicky za pomoci elektrických kontaktů, rozpozná umístění výstupků a porovná je s dostupnou databází.
    - elektromagnetické – klíč je vybaven elektromagnetickým páskem, na kterým je zaznamenaný unikátní kód, snímaný magnetickým snímačem. Klíč na pásku může být šifrovaný.
    - elektronické – klíč je vybaven elektronickým čipem s vyvedenými kontakty na jeho povrch a pro čtení se musí vložit do snímače. Klíč může být šifrovaný a nelze jej přečíst jinak než, fyzickým spojením kontaktů se čtecí jednotkou. Tento typ se často využívá u platebních karet, viz obrázek číslo 9.
    - biometrické – princip biometrického typ klíčů je založen na čtení unikátních biologických rysů člověka. Zařazen je do obou hlavních skupin, protože záleží na jeho přesném provedení. V případě kontaktního řešení se jedná například o čtečky otisků prstů a obecně o zařízení, kde je nutná fyzická interakce osoby se zařízením.

- Bezkontaktní klíče – u bezkontaktních klíčů není nutná fyzická interakce se čtecí jednotkou. Jedná se tedy o uživatelsky pohodlnější řešení, které s sebou však může nést značná bezpečnosti rizika.
    - rádiové – klíč je vybaven radiovou vysílací jednotkou, která po stisku tlačítka vyšle do okolního prostředí v kulové vlnoploše kód, který je zachycen přijímačem ovládajícím zámek. Toto řešení má velkou nevýhodu v tom, že klíč lze zachytit odkudkoli v dosahu vysílače/klíče.

- infračervené – klíč je vybaven optickou vysílací jednotkou, která po stisku tlačítka opět vyšle kód okolním prostředím. V tomto případě je však částečná výhoda v tom, že signál není vysílán do celé kulové vlnoplochy. Je vyslán pouze v kuželové výseči ve směru od vysílače. Je tedy méně náchylný na zachycení třetí stranou, což však nic nemění na tom, že je stále možné jej zachytit.
- biometrické – jak bylo zmíněno dříve, principem založené na snímání biometrických rysů lidského těla. V tomto případě však snímání probíhá bezkontaktně, například oční duhovka nebo stavba obličeje.
- RFID – jedná se o elektronický čip, jehož provedení se dělí na dva základní druhy na základě funkce vysílače a přijímače. Pro svou funkci využívají převážně nosné frekvence 125 kHz a 13,56 MHz.
    - pasivní – RFID čip nevysílá do okolí žádný signál, jeho obvod je vybuzen elektromagnetickým polem jednotky s vysílačem a přijímačem. Tím dojde k aktivaci obvodu a odeslání předem nahraného kódu na velmi krátkou vzdálenost.
    - aktivní – systém je připojen ke zdroji elektrické energie a jeho součástí je i vysílač, který do okolí aktivně vysílá signál. Právě pro tento fakt však není vhodný jako přístupový prvek, protože by byl snadno zneužitelný.

- NFC – jedná se o formu komunikace na krátkou vzdálenost mezi elektronickými zařízeními, jenž podporuje šifrování a disponuje vyšší úrovní zabezpečení než RFID. Výhodou je, že identifikace není vázána na konkrétní předmět (jako například RFID klíčenka), ale lze ji využít u jakéhokoli zařízení, které disponuje touto technologií, jako jsou například mobilní telefony nebo náramky. Na obrázku číslo 11 vpravo lze spatřit obvod NFC čipu, jehož nejvýraznější částí je anténa. Ta se nachází po obvodu celé karty, za účelem co nejvyššího dosahu signálu.
- čárové kódy – kód pracující na základě poměru sekvence kontrastních svislých čar a mezer o různých tloušťkách. Informace je zde zakódována v jedné ose kódu kolmo na sekvenci čar a mezer.

- 2D kódy – jedná se o formu kódování dat do vizuálních obrazců a speciální podskupinu čárových kódů. Informace je zde zakódována ve dvou osách. Jejich velkou výhodou je velice nízká cena a reprodukce, jelikož je lze tisknout za pomoci obyčejné tiskárny.

Obrázek 11: Elektronická karta (foto autor 2020)

Tento benefit však s sebou nese i riziko snadného zneužití v případě, že se vzor dostane do nepovolaných rukou. Mezi nejčastější zástupce 2D kódů patří následující:

  - QR kód – čtvercový kód s pevně danými body v rozích s výjimkou pravého spodního rohu.
  - Data matrix – kód vizuálně podobný QR kódu, skládající se v základním provedení z bílých a černých čtverců. Nemá však pevně dané body v rozích JAKO qr KÓD a jeho charakteristickým znakem je spojitý levý a spodní okraj.

- Mobilní aplikace – trendem poslední doby jsou zámky typu „smart lock“a jejich ovládání je řešené za pomoci aplikace v mobilním telefonu. Komunikace se zařízeními zde probíhá za pomoci technologií Bluetooth, Z-Wave nebo Zigbee. Mezi výhody využití této technologie patří možnost udělení přístupu cizímu zařízení, odemknutí bez nutnosti dotýkat se dveří nebo odemknutí na dálku.

  Technologicky existuje více způsobů řešení. Jedním je instalace přímo elektronické zámkové jednotky, druhou poté zařízení, které se nasadí na stávající mechanický zámek sklíčem v cylindrické vložce. To poté za pomoci elektromotoru manipuluje s klíčem dle pokynů řídící jednotky.

Nevýhodou je naopak vysoká pořizovací cena, v opačném případě mizivá úroveň zabezpečení u levnějších modelů. Jedná se však o řešení vhodné spíše do domácností.

Pokud by mělo být využito na KI, bylo by nutné vybavit pracovníky mobilními telefony s vysokým stupněm zabezpečení a omezenými funkcemi, což by opět zvýšilo náklady. V případě, že by se pracovníkům povolilo využívat soukromé mobilní telefony, není jisté, že by bylo zajištěno zabezpečení daných zařízení, což by představovalo značné bezpečnostní riziko.

Další z nevýhod, v případě využití tohoto systému, je nejistota při pojistném plnění v případě vloupání. V České republice zatím nejsou tyto technologie příliš rozšířeny a je možné, že by se pojišťovací společnosti k pojistnému plnění při překonání tohoto typu zámku stavily zamítavě.

5.5.4. Konstrukce dveří

V případě využití bezpečnostního typu zámku v kombinaci s vhodnou bezpečnostní vložkou, nebo při využití elektrického zámku, je také nutné řešit problematiku samotných dveří a zárubní. Pokud by nesplňovaly určité požadavky, bylo by užití bezpečnostního zámku bezpředmětné. Dveře lze překonat i jinými způsoby, než přes mechaniku zámku – například přes zárubně nebo panty.

Slícování se zárubněmi

Slícování dveří se zárubněmi je důležité z několika důvodů. Pokud se jedná o dveře, které jsou z jedné strany vybaveny koulí a je nutné je odemknout, ale z druhé strany stačí otočit klikou, existuje zde riziko zneužití. To spočívá v tom, že lze mezerou mezi dveřmi a zárubněmi prosrtčit nástroj, kterým se zachytí klika dveří a stáhne se dolů. To platí ve všech případech instalace kliky u tohoto typu dveří. Nástroj lze prostrčit jak z boků, tak zespod nebo vrchem nad dveřmi.

Další riziko spočívá v tom, že je možné do místnosti skrze mezeru vehnat jakoukoli plynnou látku, která může ovlivnit elektronická čidla v místnosti nebo napáchat jiné škody. To platí zejména v případě, že jsou v objektu využita infračervená čidla, která lze ovlivnit prudkou změnou teploty v jejich okolním prostředí. A dále lze například mezerou mezi dveřmi a zárubněmi prostrčit nástroj, kterým se zachytí střelka zámku a manuálně se zatlačí do zámku. Této situaci lze zabránit využitím již zmiňovaných bezpečnostních střelek.

Všechny zmiňované metody průniku na základě špatného slícování dveří jsou metody nedestruktivní, nenechávají za sebou po sobě žádné stopy a neprodukují žádný hluk. Jejich nebezpečí tedy spočívá zejména v tom, že ani pracovníci, kteří se běžně pohybují v daných prostorách, by nemuseli zpozorovat nic podezřelého.

Panty a bezpečnostní kolíky

Vhodně zvolené umístění pantů je dalším z důležitých aspektů. Panty nesmí být umístěny na volně přístupné straně dveří, protože hrozí jejich odvrtání nebo vytlučení čepů. Dalším rizikem je taktéž vyražení dveří beranidlem nebo vypáčení páčidlem. Z tohodo důvodu je vhodné využívat dveře s bezpečnostními kolíky, které po jejich zavření zapadnou do otvorů v zárubni a dveře jsou tak jištěny na více místech najednou, než jsou jen panty a zámek. V případě odstranění pantů také nehrozí vypadnutí dvetí ze zárubně ven, protože jsou jištěny právě těmito kolíky. Metody vytloukání čepů a další zmiňované jsou však hlučné, destruktivní a jejich využití je značně omezeno okolním prostředím a denní dobou.

Bezpečnostní šrouby, vruty a nýty

V případě bezpečnostních dveří je vhodné, aby byla jejich konstrukce provedena bez viditelných výstupů spojovacího materiálu. Tím jsou myšleny hlavy šroubů, vrutů, čepů, nýtů a podobně. Pokud útočník neuvidí žádný takový spoj, jeho práce se značně ztíží v tom, že nebude mít ani náznak konstrukce dveří. V případě, že je toto řešení z jakéhokoli opodstatněného důvodu neproveditelné, je přínosné využívat alespoň bezpečností verze jmenovaného spojovacího materiálu. Těmi jsou například šrouby a vruty s hlavičkami ve tvarech, na jejichž povolení je nutné disponovat speciálními nástroji, nebo verze s proměnným stoupáním šroubovice, které se při pokusu o povolení protáčí. V případě šroubů a vrutů je také vhodné v některých případech upřednostnit nýty, jelikož jejich odstranění je proveditelné výhradně destruktivně. Takové odstranění za sebou zanechává stopy, které mohou upozornit na manipulaci a také produkuje hluk.

5.6. Překonávání zámků

5.6.1. Mechanické zámky

V případě překonávání mechanických zámků existuje mnoho různých metod překonávání, nedestruktivních i destruktivních. Hlavními výhodami nedestruktivních metod je především to, že zpravidla nezanechávají snadno viditelné stopy a případné překonání může zůstat bez povšimnutí, pokud nedojde k odcizení nebo poškození majetku. Existují i metody, které využívají běžně dostupných polotovarů klíčů. Ty poté ve správném provedení nezanechají stopy žádné. Destruktivní metody zde zmiňovány nejsou, protože se v praxi jedná o pouhé fyzické zničení zámku odvrtáním, vyříznutím a podobně.

Vyháčkování

Jedná se o nejznámější metodu překonávání zámků, kterou využívají i zámečníci ve svých profesních činnostech. Mezi základní nástroje patří napínák a planžety. Napínák slouží k udržování tlaku na vložku, což zajistí, že se stavítka uvnitř při manipulaci zachytí ve své odemykací pozici. Pro manipulaci se stavítky se využívají planžety. Těch existuje velké množství standardních druhů, přičemž lze snadno vyrobit i vlastní typ. Výhodami této metody je zejména bezhlučnost a nezanechávání okem viditelných stop. Nevýhodami pak časová náročnost v případě komplexnějších zámků a všeobecné povědomí o této metodě, které okamžitě vzbudí podezření protiprávního jednání. Na obrázku číslo 12 na následující straně lze vidět stopy po vyháčkování na stavítku cylindrické vložky.

Vyklepávání zámku

Při této metodě se využívá volně dostupných polotovarů klíčů, které se podle specifikací výrobce vybrousí na nejnižší možné hladiny, viz obrázek 10 na straně 37. Takto vzniklý klíč se označuje jako vyklepávací klíč nebo bumpkey z anglického jazyka. Na něj se následně nasune gumové těsnění, které slouží jako pružné médium, které vrací klíč do původní polohy. Vyklepávací klíč se zasune do cylindrické vložky na doraz ke gumovému těsnění a následně se provádí údery na jeho vystupující konec za stálého tlaku na klíč ve směru odemykání vložky dokud nedojde k odemčení zámku. Výhodou této metody je nezanechávání nestandardních stop opotřebení zámku při správném provedení. Mechanické namáhání vrchní části stavítek je totiž stejné jako při odemykání zámku klíčem. Při neodborném provedení však může dojít k poškození

vnější strany cylintrické vložky nebo dveří zejména z toho důvodu, že údery na klíč je nutné provádět kladivem.

Při vývoji této metody byl ve Spojených státech amerických vynalezen i speciální nástroj zvaný „snap gun“. Jedná se o nástroj ve tvaru pistole, kde je místo hlavně nasazená speciální planžeta, kterou ze dle potřeby a typu zámku měnit. Takový nástroj je poté společně s napínákem zasunuta do zámku. Napínák opět slouží k udržování tlaku na zámek ve směru odemykání a stiskem spouště je planžeta prudce vymrštěna k odpruženým stavítkům. Ty jsou nárazem planžety vystřeleny do zadních poloh a díky udržování tlaku napínákem jsou při cestě zpět do původní polohy zachyceny v odemykací poloze a dojde k odemčení zámku.

Obrázek 12: Planžetou poškrábané stavítko cylindrické vložky pod mikroskopem [57]

5.6.2. Elektrické zámky

Překovánání elektrických zámků je přímo závislé na typu jejich odemykání a konstrukci. Riziko se také odvíjí od použitého přístupového systému, kterého je zámek součástí. Následující typy útoků patří mezi nejjednodušší, avšak často používané v případě špatně zabezpečených nebo špatně zkonstruovaných elektrických zámků.

Útok „hrubou silou“

Tento útok lze provádět na zámcích zabezpečených přístupovým kódem, který lze zadat za pomoci klávesnice nebo bezdrátovou technologií. Jedná se o komunikaci elektronického zařízení s elektronikou zámku, kdy je na základě všech možných kombinací přípustných znaků odhadováno heslo. V případě, že je kód zadáván ručně, je nutné získat fyzický přístup k základní desce elektronického zámku, aby se bylo možné připojit přes konektor. To může v praxi představovat značnou překážku, zejména pokud jsou v jeho konstrukci využity bezpečnostní šrouby, nýty, fyzické zámky nebo detektory rozebírání zámku. Pokročilejší zámky již disponují ochranou „třikrát a dost“, když je po třetím neúspěšném zadání kódu spuštěn alarm.

Vystavení silnému magnetickému poli

Tento typ útoků ohružuje nejen zámky staršího data výroby ale i současnou produkci, kde je upřednostněna kvantita, nízká cena a atraktivní vzhled nad kvalitou a bezpečností. Existují dva základní způsoby, který mi lze odemknout takový zámek.

Prvním způsobem, jak ovlivnit takto zranitelný zámek je zapůsobení přímo na elektromagnetem ovládanou odpruženou závoru. Ve výchozí pozici je daná závora mechanicky tlačena do horní úvrati pružinou. Pro její odemčení je nutné zapnout elektromagnet, který přetlačí sílu pružiny a stáhne závoru do dolní úvrati, čímž dojde k odemčení zámku. Vystavení takové konstrukce dostatečně silnému magnetu ve vhodné pozici může přetlačit danou pružinu bez aktivace elektromagnetu. Závora je stažena do dolní úvrati a zámek lze otevřít i přesto, že elektronika zámku si myslí, že je uzamčený.

Druhým způsobem je ovlivnění relé, které slouží k ovládání elektromagnetu, jenž má stejnou funkci jako v předchozím případě. Zde však působením magnetického pole dojde k sepnutí relé, což umožní průtok elektrického proudu a tím dojde k zapnutí elektromagnetu. Nebezpečí tohoto

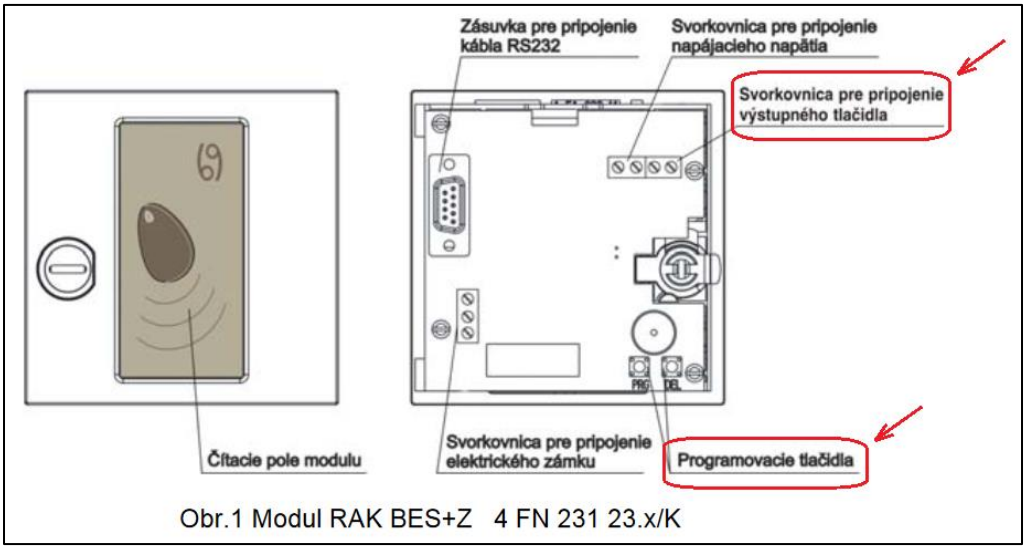
typu útoku spočívá zejména v tom, že zde vůbec nedochází k fyzickému kontaktu se zámkem a nezůstávají po něm tedy absolutně žádné stopy.

5.7. Přístupové systémy

Přístupovými systémy se rozumí elektronické zařízení nebo systém více propojených zařízení, které zajišťují čtení a ověřování elektronického klíče, ovládání elektrického zámku a ovládání poplachových zařízení v případě o pokus neoprávněného překonání zámku.

5.7.1. Nezávislé systémy

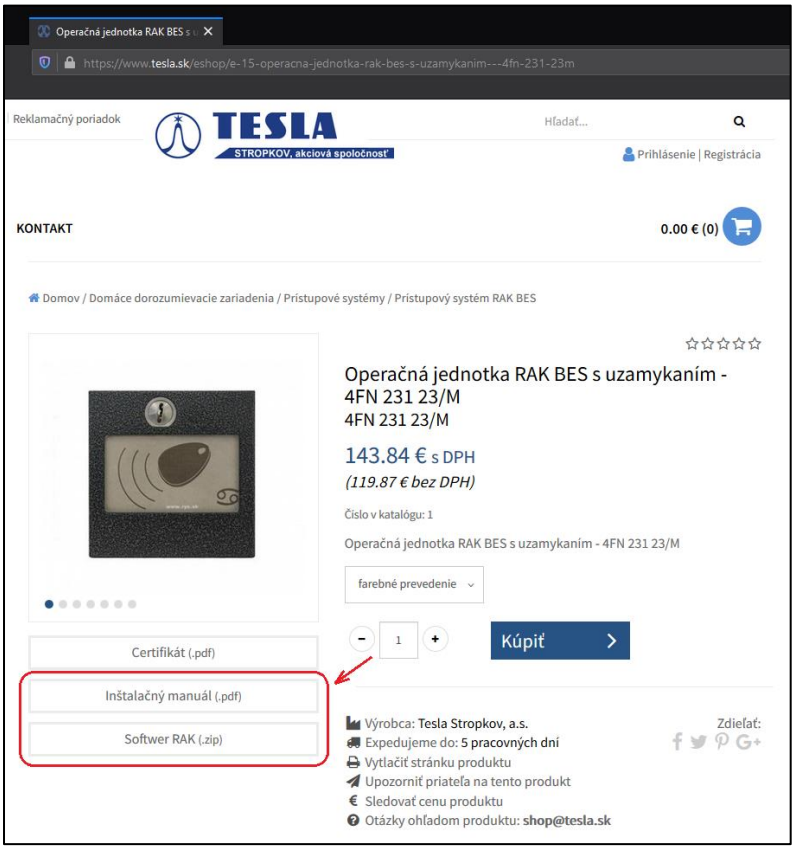
Do kategorie nezávislých systémů spadají systémy, které jsou umístěny v přístupových bodech u dveří s elektrický mi zámky a pracují jako samostatné jednotky bez kontaktu s jakoukoli další technikou. Nelze tedy monitorovat jejich aktuální stav v reálném čase a jakákoli změna identifikátorů musí být provedena na místě. Pro klíče zde mohou být využity všechny možnosti z kapitoly *12.4.1 Typy elektronických klíčů,* viz strana 38. Velkou nevýhodou těchto systémů a značným bezpečnostím rizikem je skutečnost, že ověření klíče, ovládání elektrického zámku a správa databáze identifikátorů probíhají přímo v jednotce uživateli na dosah. Systém se tak stává snadno napadnutelným i nejjednoduššími typy útoků, jaké byly například zmíněny v předchozí kapitole.



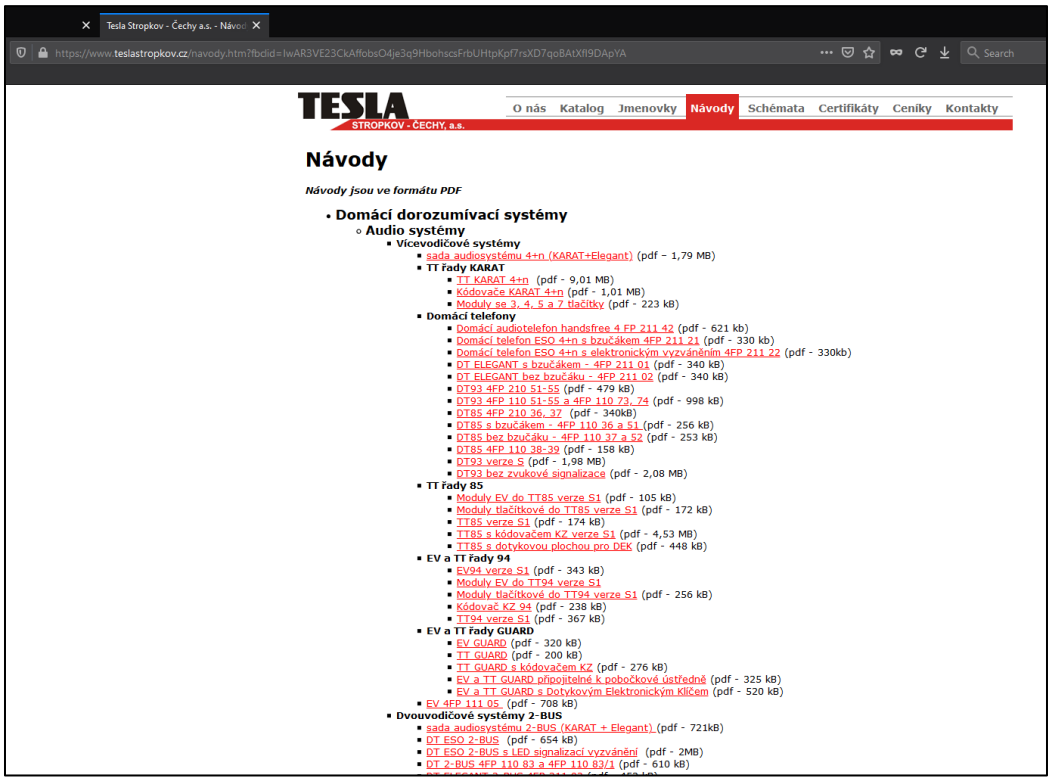
Obrázek 13: Ukázka z manuálu přístupového systému Tesla RAK BES [60]

Další bezpečnostní rizika vytváří přímo někteří výrobci sami tím, že na své internetové stránky umísťují volně k dispozici návody ke svým produktům. V návodech se totiž nachází schémata zapojení s detailním popisem jednotlivých prvků, včetně takových jako je výstupní tlačítko nebo programovací tlačítka, viz obrázek číslo 13. Jako příklad lze uvést slovenskou společnost TESLA STROPKOV, která navíc dává volně k dispozici i software k vytvoření databáze identifikátorů a její správu, viz obrázky 14 a 15 na následující straně. [60]

Na základě uvedených skutečností lze konstatovat, že nezávislé systémy jsou absolutně nevhodné pro aplikaci na prvcích kritické infrastruktury. Svou konstrukcí, ale i činností svých výrobců, nepředstavují v mnohých případech téměř žádnou překážku a jedná se spíše o prvek, který zrychluje otevírání dveří absencí fyzického klíče. Zabezpečení daného přístupového bodu s nezávislým systémem je v mnohých případech iluzorní. Využitím mechanické bezpečnostní cylindrické vložky v kombinací s dveřmi vhodné konstrukce lze zajistit vyšší stupeň ochrany při vynaložení stejných, ale i nižších finančních prostředků.



Obrázek 14: Ukázka z webových stránek TESLA STROPKOV [60]



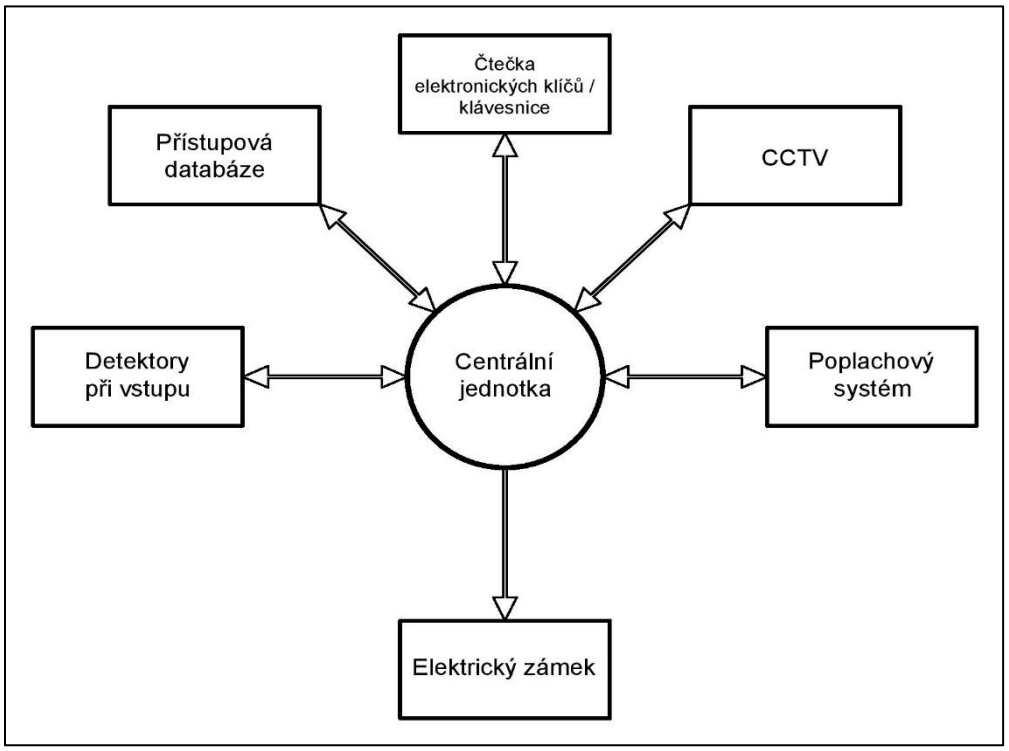
Obrázek 15: Ukázka z webových stránek TESLA STROPKOV – Čechy [61]

5.7.2. Distribuované systémy

Do kategorie distribuovaný ch systémů spadají systémy, jejichž struktura se skládá z více samostatný chprvků. Elektronická jednotka, která se nachází u elektrického zámku, slouží pouze ke čtení elektronických klíčů, případně k zadávání alfanumerického přístupového kódu. Narozdíl od nezávislých systémů tento koncept tedy poskytuje výrazně lepší zabezpečení, protože čtení a ověření identifikátoru, správa přístupové databáze ani manipulace s elektrický m zámkem neprobíhá v rámci jednoho zařízení.

Centrální jednotka, která slouží k ověřování identifikátorů, ani databáze identifikátorů nejsou uživateli přístupné a neexistuje tedy možnost jejího snadného zneužití. Pokud se při přenosu jaký chkoli informací vrámci tohoto typu přístupového systému využívá šifrované komunikace, nelze systém snadno napadnout. Velkou výhodou je též fakt, že správu elektronických klíčů lze provádět centrálně i pro více přístupových bodů najednou a není nutné nastavovat manuálně každý vstup. Na obrázku číslo 16 na následující straně lze spatřit schematické uspořádání jednotlivých prvků distribuovaného systému.

Na základě dříve uvedených důvodů lze konstatovat, že distribuované přístupové systémy jsou vhodné pro aplikaci na prvcích kritické infrastruktury. Jejich jednotlivé části mohou disponovat dodatečnou fyzickou ochranou a jeví se tedy jako značně robustní.



Obrázek 16: Schéma distribuovaného systému (kreslil autor 2020)

6. Metodiky vyhodnocování rizik

Pro vyhodnocování rizik v systémech se využívají nástroje známé jako rizikové analý zy. Jejich podoba může mít různou strukturu a vhodnost jejich užití se u konkrétních systémů liší. Princip analýz spočívá v rozboru procesů systému a identifikaci možných rizik s nimi spojených. Následně zhodnocení rizik a vyhodnocení, zda procesy z pohledu bezpečnosti vyhovují pro praktické nasazení v provozu daného systému. Ve všech případech by měla být snaha dosáhnout co nejdetailnějšího popisu systému, aby se zamezilo výskytu nečekaných situací v praxi. Obecně však nečekaným situacím naprosto zabránit nelze z různých důvodů. Zejména kvůli tomu, že i přes snahu dosáhnout co nepřesnějšího modelu systému a shody s reálný m provozem, nelze v praxi zaručit, že tomu tak skutečně bude. Analýzy jsou vypracovávány na základě předpokladů a mohou být založeny na expertním odhadu, který se může lišit na základě zkušeností vyhotovitele. Následující podkapitoly popisují vybrané metodiky rizikový ch analý z.

6.1. Brainstorming

Metoda brainstormingu je založena na diskuzi skupiny lidí, kteří prezentují své myšlenky a nápady ostatním, kteří na jejich základě přichází s dalšími možnosti. Nelze ji však správně provádět bez plánování a moderování. Pro její efektivní využití a poskytnutí užitečných výstupů je nejprve nutné zajistit, že lidé přizvaní k diskuzi mají zkušenosti a povědomí v oblastech, kterými se bude diskuze zabývat. Před započetím konverzace je nutné přesně definovat problematiku, která se bude rozebírat a dále je vhodné, aby se každý z účastníků připravil a utřídil si své myšlenky.

Vzhledem k tomu, že je metoda založena na konverzaci lidí, je důležité, aby bylo zajištěno, že bude efektivně postupovat vpřed a nezačne se ubírat pouze jedním směrem nebo odklánět od tématu. Tuto roli plní moderátor, který zároveň zajišťuje, aby se ke slovu dostali všichni zúčastnění.

Brainstorming lze provádět i individuálně, například se zapisováním myšlenek a přicházení s novými řešeními a možnostmi. Je však vhodnější jej provédět ve skupinách, jelikož lze těžit z více zkušeností, různých přístupů různých lidí a různých úhlů pohledu najednou.

6.2. FMEA

Jedná se o typ analýzy, který byl původně vyvinut pro vojenské použití. Metoda je založena na přístupu „krok za krokem“ pro zjištění všech možných příčin selhání prvků. Zabý vá se jak rozborem příčin selhání, tak dopadů selhání na uživatele. Cílem je nabízet řešení, jak možným selháním předejít nebo alespoň redukovat riziko jejich vý skytu. Aplikace této metody je možná jak při navrhování systému, tak při vylepšování systému nebo pravidelně, pro zajištění co nejvyšší efektivity a bezpečnosti systému. Na obrázku číslo 17 lze spatřit, jak může vypadat záznamový formulář. [65]

Prvek	Možná porucha	Možné následky poruchy	S	Možné příčiny poruchy	O	Stávající opatření	D	RPN	Doporučená opatření	Výsledky opatřední				
										Provedená/přijatá opatření	S	O	D	RPN

Obrázek 17: Ukázka formuláře FMEA (autor 2020)

Pro určení závažnosti poruch se využívá číslo RPN, které vychází z ohodnocení následků poruchy S, možných příčin poruchy O a ohodnocení stávajících opatření D. Vý sledek je poté určen součinem ohodnocení těchto tří položek $RPN = S \cdot O \cdot D$. Čím vyšší je výsledné číslo, tím vyšší prioritu má dané riziko při hledání řešení. Dále se v některých případech určuje i parametr kritičnosti, jehož výpočet je $C = S \cdot O$. Na základě těchto hodnot se navrhují protiopatření a následně provádí jejich opětovný výpočet jako ověření, zda došlo ke zlepšení situace.[65]

6.3. FTA

Jedná se o detailní metodu, ve které je prováděno hledání způsobů, kterými může dojít k určitému typu selhání vytvářením stromových grafů a následné navrhování zlepšujících opatření. Hlavním smyslem této metody je popsat možné řetězce vedoucí k selhání před tím, než k samotnému selhání dojde. Prvním krokem je definice hlavního selhání (například prasknutí pružiny) a následně je za pomoci technický ch znalostí problematiky vytvořen graf dílčích událostí, které mohou k danému hlavnímu selhání vést za konkrétních podmínek. Jednotlivé události mohou být doplněny o hodnoty pravděpodobností výskytu. [66]

V grafech událostí se užívají přesně definované znaky s jednoznačným významem, které lze spatřit na obrázku číslo 18. Díky grafickému zobrazení by měl být výsledný graf při znalosti použitých znaků přehledně srozumitelný. [66]

Event Symbol		Gate Symbol		Transfer Symbol	
Symbol	Meaning	Symbol	Meaning	Symbol	Meaning
	AND Gate		Basic event		Transfer-In
	OR Gate		Incomplete Event		
	Exclusive OR Gate		Conditional Event		Transfer-out
	Priority AND Gate		Normal Event		
	Inhibit Gate		Intermediate Event		

Obrázek 18: Symboly FTA [67]

6.4. PNH

Jedná se ty maticové analý zy, která vychází ze základů metody FMEA. Určování rizik a jejich stupňů probíhá za pomocí tří základních hodnot, kterými jsou pravděpodobnost vzniku rizika *P*, závažnost následků *N* a hodnota *H*, která popisuje subjektivní názor hodnotitele na vliv rizika a míru nebezpečí. Pro ohodnocení jednotlivý chparametrů se využívají stupnice o pěti hladinách a hodnoty mohou nabývat čísel 1 až 5 odstupňované po 1. Nejnižší hodnota, kterou tedy může riziko nabývat je 3 a nejvyšší je hodnota 125.

Výsledkem této analýzy je takzvaný ukazatel míry rizika R, jehož hodnota je určena výpočtem $R = P \cdot N \cdot H$. Výsledek výpočtu vyjadřuje naléhavost přijetí opatření ke snížení rizika a proritu přijetí bezpečnostních opatření. Na jeho základě lze také rozdělit rizika do pěti rizikových stupňů, viz obrázek číslo 19.

V případě, že metodu vyhodnucuje více hodnotitelů najednou, je vhodné pro parametr H, tedy subjektivní názory hodnotitelů, určit statistické veličiny jako je například směrodatná odchylka (data mají normální rozdělení). Při vysokých hodnotách směrodatné odchylky je zřejmé, že je

názor nejednotný a je tedy vhodné se danému riziku věnovat odděleně s důkladnějším rozborem. Stejné platí i pro zbylé parametry v případě, že jsou určovány například expertním odhadem nebo jiným způsobem subjektivně několika hodnotiteli a nevychází tedy z výsledků měření.

Tabulka 1: Stupně rizik PNH analýzy (upraveno dle [68])

Rizikový stupeň	Ukazatel míry rizika R	Míra rizika
I.	101 - 125	Nepřijatelné riziko
II.	51 - 100	Nežádoucí riziko
III.	11 - 50	Mírné riziko
IV.	3 - 10	Akceptovatelné riziko
V.	1 - 2	Bezvý znamné riziko

7. Riziková analý za

Pro zpracování rizikové analý zy byla zvolena maticová metoda „RPD“. Provedením se jedná o metodu podobnou PNH analý ze zpředchozí kapitoly. Pro vyhotovení byl zvolen modelový systém tunelu, který je standardně řízen na dálku z řídící ústředny.

7.1. Identifikace rizik

Rizika byla rozdělena podle původu do tří hlavních skupin. První skupinou jsou rizika vnitřní, která vycházejí z fungování samotného systému. Druhou skupinou jsou rizika vnější, která působí na systém z jeho blízkého okolí a ovlivňují jeho chod. Poslední skupinou jsou rizika globální, která pochází ze vzdáleného okolí systému. Následující tabulka 2 shrnuje identifikovaná rizika a podává u každého jeho definici.

Tabulka 2: Identifikace rizik

Příčiny vzniku		Rizikové faktory	Definice
Vnitřní	Personální	Nekvalitní personál	Personál neschopný zajistit správné a bezpečné fungování prvku.
		Únik informací	Zneužití přístupu k technickému vybavení prvku personálem.
		Nedostatečný personál	Nedostatečný počet pracovníků pro zajištění správného a bezpečného fungování prvku.
	Systémové	Monitorování stavu technického vybavení	Neefektivní využití a správa vybavení infrastruktury.
	Technické	Nevhodné zabezpečení přístupových bodů	Využití nedostatečně odolných bezpečnostních prvků v přístupových bodech.
		Nevhodné technické vybavení	Nedostatečné technické parametry, vybavení poskytující nekvalitní vý stup.

		Poškození technického vybavení vlivem neodborné manipulace	Zásah do technického vybavení infrastruktury neoprávněnou osobou.
Vnější	Legislativní	Nedostatečná legislativa a předpisy	Legislativa a předpisy opomíjející využití moderních přístupů.
	Politické	Nedostatečné financování infrastruktury	Udělení nedostatečných finančních prostředků pro údržbu a modernizaci infrastruktury.
	Technické	Dopravní nehody	Nehody vozidel v oblasti prvku infrastruktury.
		Ztráta dodávek elektrické energie	Vý padekpřívodu elektrické energie.
		Vjezd nevhodného typu vozidla	Vjezd nevhodného typu vozidla do oblasti prvku infrastruktury - například sklízecí mlátička.
Globální	Přírodní	Pandemie	Plošný výskyt onemocnění ohrožující zdravotní stav personálu.
		Živelné pohromy	Pohromy ohružující infrastrukturu a její vybavení - například povodně.
	Politické	Mezinárodní terorismus	Hrozba teroristických útoků.

7.2. Princip ohodnocení rizik

Následně byla rizika ohodnocena dvěma parametry *P1* a *D*. Parametr *P1* značí pravděpodobnost výskytu rizika a parametr *D* značí závažnost dopadu příslušného rizika. Pro číselné ohodnocení parametrů byly využity stupnice o pěti úrovních, které znázorňují jejich závažnost. Hodnoty jednotlivých úrovní jsou odstupňovány po 0,1 od 0,1 do 1. Lze je spatřit v tabulkách číslo 3 a 4 včetně jejich definice.

Tabulka 3: Dělení pravděpodobnosti výskytu rizik P1

Úroveň	Pravděpodobnost rizika	Číselné vyjádření	Definice
1	Zanedbatelná	0.1 - 0.2	téměř se nevyskytuje
2	Malá	0.3 - 0.4	vyskytuje se pouze výjimečně
3	Střední	0.5 - 0.6	může se vyskytnout
4	Závažná	0.7 - 0.8	pravděpodobně se vyskytne
5	Kritická	0.9 - 1.0	vyskytne se téměř vždy

Tabulka 4: Dělení významu dopadů rizik D

Úroveň	Vý znam dopadu	Číselné vyjádření	Definice
1	Zanedbatelný	0.1 - 0.2	neovlivňuje znatelně fungování systému
2	Malý	0.3 - 0.4	ovlivňuje pouze dílčí aktivity
3	Střední	0.5 - 0.6	znatelně ovlivňuje fungování systému
4	Závažný	0.7 - 0.8	vede k újmě na majetku či zdraví osob
5	Kritický	0.9 - 1.0	vede ke ztrátám na majetku nebo na životech

7.3. Vyhodnocení závažnosti rizik

Číselné hodnoty parametrů *P1* a *D* lze spatřit v následující tabulce číslo 5. Jejich výše byla určena na základě expertního odhadu.

Tabulka 5: Vyhodnocení závažnosti rizik před protiopatřeními

Příčiny vzniku		Rizikové faktory	Pravděpodobnost vzniku rizika P1	Vý znam dopadu rizika D
Vnitřní	Personální	Nekvalitní personál	0.5	0.7
		Únik informací	0.2	0.3
		Nedostatečný personál	0.6	0.5
	Systémové	Monitorování stavu technického vybavení	0.6	0.6
	Technické	Nevhodné zabezpečení přístupových bodů	0.7	0.6
		Nevhodné technické vybavení	0.4	0.4
		Poškození technického vybavení vlivem neodborné manipulace	0.3	0.3
Vnější	Legislativní	Nedostatečná legislativa a předpisy	0.6	0.6
	Politické	Nedostatečné financování infrastruktury	0.6	0.3
	Technické	Dopravní nehody	0.7	0.7
		Ztráta dodávek elektrické energie	0.3	0.6

		Vjezd nevhodného typu vozidla	0.2	0.5
Globální	Přírodní	Pandemie	0.2	0.6
		Živelné pohromy	0.4	0.7
	Politické	Mezinárodní terorismus	0.1	0.9

Hodnota parametru závažnosti *R1* je následně určena výpočtem $R1 = P1 \cdot D$. Čím vyšších hodnot parametr závažnosti nabývá, tím vyšší prioritu má dané riziko při pozdějším řešení protiopatření. Dalším parametrem, který je v tabulce uveden, je „Klíčové riziko“. Za klíčové riziko je považováno takové riziko, jehož hodnota parametru R1 přesahuje nebo je rovna 0,35. Parametr tedy může nabý vat pouze dvou hodnot „ano“ a „ne“.

Tabulka 6: Vyhodnocení rizik před protiopatřeními

Příčiny vzniku		Rizikové faktory	Úroveň rizika R1	Klíčové riziko
Vnitřní	Personální	Nekvalitní personál	0.35	ANO
		Únik informací	0.06	NE
		Nedostatečný personál	0.30	NE
	Systémové	Monitorování stavu technického vybavení	0.36	ANO
	Technické	Nevhodné zabezpečení přístupových bodů	0.42	ANO
		Nevhodné technické vybavení	0.16	NE
		Poškození technického vybavení vlivem neodborné manipulace	0.09	NE

Vnější	Legislativní	Nedostatečná legislativa a předpisy	0.36	ANO
	Politické	Nedostatečné financování infrastruktury	0.18	NE
	Technické	Dopravní nehody	0.49	ANO
		Ztráta dodávek elektrické energie	0.18	NE
		Vjezd nevhodného typu vozidla	0.10	NE
Globální	Přírodní	Pandemie	0.12	NE
		Živelné pohromy	0.28	NE
	Politické	Mezinárodní terorismus	0.09	NE

Jako klíčová rizika byla indentifikována následující:

- Nekvalitní personál – nekvalitní personál může být následkem nevhodného výběrového řízení do pozic zaměstnanců zajišťujících chod systému.
- Monitorování stavu technického vybavení – vybavení tunelu a vybavení řídící ústředny je nutné po uplynutí doby provozní životnosti udávané výrobcem obměnit, aby se zajistila správná a spolehlivá funkce.
- Nevhodné zabezpečení přístupových bodů – v rámci ekonomických úspor mohou být využity nevhodné zabezpečovcí prvky, které nebudou poskytovat dostatečnou ochranu před narušiteli.
- Nedostatečná legislativa – s vývojem moderních technologií může dojít ke stavu, kdy nebude legislativní vývoj dostatečně rychlý a bude zaostávat za moderními přístupy a technologiemi.
- Dopravní nehody – dopravní nehody jsou rizikem, které se vyskytuje na všech silničních komunikacích, na nichž jsou dopravní prostředky ovládány lidskou obsluhou.

V následující tabulce číslo 7 je možné spatřit grafické zobrazení rozložení rizik. Zeleně jsou zvýrazněny nízká rizika, žlutě střední rizika a červeně vysoká rizika. Počty rizik v daných kategoriích jsou uvedeny vpravo za lomítkem, celkem bylo tedy 5 rizik vyhodnoceno jako nízkých, 7 jako středních a 3 jako vysoká.

Tabulka 7: Maticové zobrazení závažnosti rizik před protiopatřeními

Matice rizik		Dopad				
		Žádný	Malý	Střední	Závažný	Kritický
Pravděpodobnost	Kritická	5/0	10/0	15/0	20/0	25/0
	Závažná	4/0	8/0	12/1	16/1	20/0
	Střední	3/0	6/1	9/3	12/1	15/0
	Malá	2/0	4/2	6/1	8/1	10/0
	Žádná	1/0	2/1	3/2	4/0	5/1

7.3.1. Metody určení pravděpodobností

Jak bylo zmíněno, konkrétní hodnoty pravděpodobnosti vzniku jmenovaných rizik byly určeny na základě expertního odhadu autora práce. Tato metoda byla zvolena z toho důvodu, že v některých případech nebylo možné určit rozdělení pravděpodobnosti jmenovaných rizik na jejichž základě by bylo možné určit konktrétní hodnoty. V případě, že by rozdělení byla k dispozici, lze využít některé z následujících metod.

Simulační metody

Do simulačních metod spadají metody, které jsou založeny na využití opakované realizace simulací funkce náhodných proměnných. Jsou založeny na simulaci Monte Carlo, kterou lze aplikovat všeobecně, avšak vyžaduje vyšší množství simulací a s tím spojený velší výpočetní čas než metody, které z ní vycházejí. Mezi ty patří skupiny stratifikovaných simulačních metod a zdokonalených simulačních metod. [82] [83]

Aproximační metody

Jako základní zastupitele aproximačních metod lze jmenovat metody FORM a SORM, které využívají při pravděpodobnostním výpočtu analytické aproximace. Mezi další podskupiny poté patří metody plochy odezvy, perturbační techniky nebo ANN. [81] [83]

Numerické metody

Jako zástupce numetických metod lze jmenovat například metodu POPV, jejíž vývoj započal v roce 2002. Algoritmus, kterým slouží k výpočtu této metody, je přesně dán pro každou řešenou úlohu a k řešení dochází pouze numericky bez použití simulačních nebo aproximačních technik. [83]

7.4. Návrh protiopatření

V této části analýzy dochází k navržení možných protiopatření pro rizika, která byla identifikována jako kritická. Pro ostatní rizika, která jako kritická identifikována nebyla, jsou určena protiopatření v tabulce poslední podkapitole 14.4.6 Ostatní rizika.

7.4.1. Nekvalitní personál

Pozice pracovníků majících na starosti technický chod systému a práci s elektrotechnickým vybavením je nutné obsazovat na základě výběrového řízení, které prokazatelně potvrdí, že je uchazeč vhodný pro danou pozici. V případě práce s elektrotechnickým vybavením musí uchazeč prokázat splnění kvalifikace pro §6 vyhlášky č. 50/1978 Sb. o odborné způsobilosti v elektrotechnice, v případě působení na vedoucích pozicích následně §7 téže vyhlášky a v případě provádění revizních prací splnění kvalifikace pro §9.

Pracovnící zajišťující monitorování stavu dopravy v tunelových troubách musí být prokazatelně proškoleni v ovládání systému a schopnosti řešení krizových situací v psychicky náročném nasazení. Zároveň je nutné udržování jejich schopností a kvalifikace, kde se jako vhodným prostředkem jeví například tunelový trenažer TOMMS od společnosti Eltodo a.s. [69] [89]

Princip trenažeru spočívá v simulovaném operátorském pracovišti, kde probíhá simulace provozu v tunelové stavbě a přivození krizové situace. Školitel má k dispozici různé scénáře, může simulovat selhání různých částí vybavení a má detailní přehled o prováděných úkonech školeného pracovníka. Úkolem pracovníka je řešit danou situaci na základě nabytých znalostí a schopností, přičemž má k dispozici i simulovaný 3D pohled kamerových systémů. [69]

Nespornou výhodou takového systému trénování je zejména možnost prakticky neomezeného ověřování schopností pracovníků řešit krizové situace i v době, kdy již proběhly zkoušky tunelu

před uvedením do ostrého provozu a je tedy nemožné je opakovat. Další výhodou je také časová i finanční úspora oproti školení v reálné stavbě.

7.4.2. Nevhodné zabezpečení přístupových bodů

Pro přístupové body prvků kritické infrastruktury se důrazně nedoporučuje využití nezávislých přístupových systémů z důvodu jejich mizivé bezpečnosti a velice nízké úrovně zabezpečení. V případě využití elektrinických přístupových systémů by se mělo jednat o systémy distrubuované, kde má uživatel přístup pouze ke čtečce elektronického klíče. Ověření klíče a ovládání elektronického zámku musí být uživateli skryto, vzdáleno a řádně zabezpečeno, aby se zabránilo jeho zneužití.

V případě využití mechanických zámků se rozhodně nedoporučuje využívat standardní mechanické vložky, ale bezpečností typy s ochranou proti nedestruktivním technikám překonání. Vnější přístupové body dále by měly splňovat požadavky na třídu RC4 dle ČSN 1627, vnitřní poté alespoň RC 3 dle využití daných prostor. [63] [73]

7.4.3. Monitorování stavu technického vybavení

Životnost technického vybavení je na základě průzkumu společnosti PIARC zjištěna v rozmezí 10 až 25 let a není u všech systémů sjednocena. I v případě pravidelného provádění revizí existuje možnost selhání prvku, například z důvodu dlouhých intervalů mezi jednotlivými údržbami. Prohlídky také nejsou optimalizované na základě dat z terénu, ale plánované v předem stanovených intervalech. Protokoly o servisních zásazích mohou bý t zaznamenávány ručně a hodnoty získávané během údržby mohou bý todečítány z analogovýc měřících zařízení, kde hrozní provedení špatného záznamu přehlédnutím, z nepozorností a podobně. Kontroly také nelze provádět u všech systémů ve standardní provozní dobu a v některých případech musí bý t plánovány na dobu s menším nebo žádným zatížením systému. [70]

Tuto situaci by mohlo pomoci zlepšit využití systémů SCADA nebo DCS, případně TUBIS. Existuje zde však riziko otevření systému okolí a proto musí být prokazatelně zajištěno, že k takovému stavu nedojde. Následující část pojednává o jednotlivých systémech konkrétněji. [88] [89]

SCADA

SCADA systémy představují kombinaci softwarových nástrojů a hadrwarového vybavení pro dohled a řízení procesů v systému. Jejich velkou výhodou je zejména to, že nejsou vázány na konkrétní hardwarové vybavení a jsou založeny na otevřených standardech. Jejich nasazení tedy lze realizovat na hardwarovém vybavení různých výrobců. [88]

Dále umožňují uchovávání provozních dat o jednotlivých prvcích, za jejichž pomoci lze následně plánovat údržby, obměnu konkrétního vybavení s dosluhující provozní životností nebo provádět predikci možných poruch. Narozdíl od současných systémů také SCADA systémy umožňuji ovládání a monitorování vybavení online v reálném čase, což značně usnadňuje a zrychluje možné reakce na nežádoucí stavy a mohou pomoci docílit nižších provozních nákladů. [88]

DCS

Systémy DCS jsou velice podobné systémům SCADA, nejsou však natolik flexibilní. Mezi jejich hlavní specifika patří to, že výrobce DCS systému poskytuje jak softwarovou část, tak hardwarovou část intergrovanou do jednoho celku bez možnosti změny využití hardwaru nebo softwaru od jiného výrobce. K dispozici jsou předem definované funkce, které stačí dle nasazení pouze specificky upravit. Zpravidla se jedná o uzavřený systém, který využívá pro komunikaci interní síť. Nevýhodou však je, že pracuje o něco pomaleji, než předchozí SCADA a vyžívá výhradně proprietární prvky. [88]

V případě, že v kontrolovaném systému (tunelový komplex) je využito velké množství PLC pro řízení různých prvků, jeví se využití systému DCS jako vhodné, protože zamezuje možným chybám v kompatibilitě softwaru a hardwaru řídícího systému. Systém je také uzavřený vstupům z vnějšího okolí, což zaručuje jeho vyšší bezpečnost [88]

TUBIS

Systém TUBIS od společnosti Eltodo je navržen jako doplněk pro SCADA systémy. Jeho úkolem je analyzovat dlouhodobé záznamy o provozu technických zařízení tunelu, umožňovat prediktiví diagnostiku jednotlivých komponent a umožnit zpracování záznamů o servisních zásazích v elektronické podobě. Systém se orientuje především na údržbu a období konce životnosti zařízení, které je charakteristické výskytem většího počtu poruch a nutností zvýšené údržby. Výhodou nasazení takového systému by tedy bylo možné snížení nákladů na údržbu z důvodu

efektivnějšího plánování a zisk přesnějších dat přímo z konkrétních zařízení a systémů v tunelu. [89]

7.4.4. Nedostatečná legislativa a předpisy

Vývoj legislativy a předpisů pro různé technické a technologické vybavení nemusí vždy aktuálně korespondovat s úrovní moderních technologií a přístupů k problematice bezpečnosti.

V případě technologických zařízení se jeví jako vhodné využívat bezpečnostní certifikace prvků, která doposud není nikde obsažena. Konkrétně se jedná o bezpečnostní standardy SIL, které přesně definují nároky na maximální počet selhání, odolnost proti vadám a podobně. Dle mezinárodního standardu jsou definovány čtyři úrovně SIL, viz následující přehled. [71]

- SIL1 – Nízký stupeň garance, že bude výrobek plnit svou funkci nepřetržitě.
- SIL2 – Nízké statistické riziko neznámého selhání prvku.
- SIL3 – Schopnost prvku provádět měření redundantně, narozdíl od SIL2.
- SIL4 – Velice vysoké nároky na spolehlivost a nízkou chybovost.

V případě využití této certifikace v tunelových systémech se jeví jako vhodné, aby prvky splňovaly nároky dle úrovně SIL3. Případně by také bylo přínosné zavést tyto nároky na funkční bezpečnost zařízení do aktualizace Technických podmínek TP98 (Technologické vybavení tunelů pozemních komunikací), která proběhla naposledy v roce 2010. [72]

7.4.5. Dopravní nehody

Za účelem snížení dopravní nehodovosti je nutné neustále monitorovat dopravní proud a reagovat na příslušnou dopravní situaci regulováním maximální povolené rychlosti v tunelu, omezením vjezdu do tunelu, v případě zastavení vozidla jeho odstraněním do zálivů, případně uzavřením jízdního pruhu. Dále jeho co nejrychlejším odstraněním z oblasti tunelové trouby. Tyto skutečnosti jsou však již uvedeny v praxi.

Dalším možným snížením nehodovosti by bylo využití autonomních vozidel. Bylo by však nutné zajistit jejich plný podíl vdopravním toku. V případě jejich částečnému nasazení současně k vozidlům řízeným lidskou posádkou by mohlo docházet k nestandardním situacím například na základě předpokladů a očekávání „lidské reakce“. Současné technologie, ekonomická a společneská situace však takové řešení zatím nepřipouští.

7.4.6. Ostatní rizika

Následující tabulka číslo 8 pojednává o protiopatřeních pro ostatní rizika, která nebyla vyhodnocena jako kritická.

Tabulka 8: Návrhy protiopatření pro ostatní rizika

Příčiny vzniku		Rizikové faktory	Způsob snížení a eliminace rizika
Vnitřní	Personální	Únik informací	Elektronické a výpočetní zařízení nesmí být vybaveno běžnými uživatelskými vstupy typu USB a podobně. Dále je vhodné zavést přsný zákaz fotografování ve vnitřních a provozních prostorách kritické infrastrutkury.
		Nedostatečný personál	Obsazování pracovních míst na kritické infrastruktuře musí být prioritou a je tedy vhodné vytvářet atraktivní pracovní podmínky a benefity. Dále například v případě řídící ústředny, která je pro dohled a řízení spravována PČR je vhodné zajistit dostatečný počet personálu převelením policistů z jiných útvarů.
	Technické	Nevhodné technické vybavení	Technické vybavení infrastruktury musí zajišťovat dostatečnou kvalitu zaznamenaných dat pro jasnou interpretaci lidské obsluze.
		Poškození technického vybavení vlivem neodborné manipulace	Musí být zřízen a pracovníci musí být seznámeni s využíváním systému ohlašování závad a jejich odstraňování musí mít na starosti pouze odborný personál.
Vnější	Politické	Nedostatečné financování infrastruktury	Vhodné zajistit financování nejen ze státních, ale I evropských zdrojů financí.

	Technické	Ztráta dodávek elektrické energie	Nutnost zajistit možnost nouzových dodávek energie. Tím mohou být například naftové generátory elektické energie.
		Vjezd nevhodného typu vozidla	Nutnost monitorovat dostatečnou vzdálenost příjezdových komunikací v okolí prvku inftastruktury a zastavit dané vozidlo před jeho příjezdem do oblasti prvku kritické infrastruktury.
Globální	Přírodní	Pandemie	V případě potvrzení výskytu v České republice musí bý t pracovníci vybaveni ochranný mi pomůckami, které sníží riziko šíření nemoci mezi personálem a kontaminaci vybavení pracovišť.
		Živelné pohromy	Elektronická zařízení infrastruktury musí mít zajištěno vhodné krytí dle ČSN EN 1627. Technické místnosti musí mít zajištěno vhodné krytí proti působení vnějších živlů podle příslušných stavebních norem.
	Politické	Mezinárodní terorismus	Kritické body infrastruktury musí bý t vybaveny prvky odolnými proti vloupání dle ČSN EN 1627 alespoň třídy R3 nebo R4. Vhodné je také jejich nepřetržité monitorování kamerovým systémem a podobně. [63] [73]

7.5. Ověření protiopatření opětovným vyhodnocením

Ověření navrhovaných protiopatření bylo provedeno opětovným výpočtem parametru úrovně rizik *R2* za pomoci stejného postupu, jako v kapitole 14.3. Následující tabulky číslo 9, 10 a 11 shrnují možné změny v úrovních posuzovaný ch rizikpo navrhovaný chprotiopatřeních.

Tabulka 9: Vyhodnocení závažnosti rizik po protiopatřeních

Příčiny vzniku		Rizikové faktory	Pravděpodobnost vzniku rizika P1	Vý znam dopadu rizika D
Vnitřní	Personální	Nekvalitní personál	0.2	0.7
		Únik informací	0.1	0.3
		Nedostatečný personál	0.4	0.5
	Systémové	Monitorování stavu technického vybavení	0.3	0.6
	Technické	Nevhodné zabezpečení přístupových bodů	0.3	0.6
		Nevhodné technické vybavení	0.2	0.4
		Poškození technického vybavení vlivem neodborné manipulace	0.1	0.3
Vnější	Legislativní	Nedostatečná legislativa a předpisy	0.3	0.6
	Politické	Nedostatečné financování infrastruktury	0.4	0.3
	Technické	Dopravní nehody	0.7	0.7
		Ztráta dodávek elektrické energie	0.3	0.6
		Vjezd nevhodného typu vozidla	0.2	0.5

Globální	Přírodní	Pandemie	0.2	0.6
		Živelné pohromy	0.3	0.7
	Politické	Mezinárodní terorismus	0.1	0.9

Tabulka 10: Vyhodnocení rizik po protiopatřeních

Příčiny vzniku		Rizikové faktory	Úroveň rizika R1	Klíčové riziko
Vnitřní	Personální	Nekvalitní personál	0.14	NE
		Únik informací	0.03	NE
		Nedostatečný personál	0.2	NE
	Systémové	Monitorování stavu technického vybavení	0.18	NE
	Technické	Nevhodné zabezpečení přístupových bodů	0.18	NE
		Nevhodné technické vybavení	0.08	NE
		Poškození technického vybavení vlivem neodborné manipulace	0.03	NE
Vnější	Legislativní	Nedostatečná legislativa a předpisy	0.18	NE
	Politické	Nedostatečné financování infrastruktury	0.12	NE
	Technické	Dopravní nehody	0.49	ANO
		Ztráta dodávek elektrické energie	0.18	NE

		Vjezd nevhodného typu vozidla	0.1	NE
Globální	Přírodní	Pandemie	0.12	NE
		Živelné pohromy	0.21	NE
	Politické	Mezinárodní terorismus	0.09	NE

Tabulka číslo 11 níže zobrazuje posun závažnosti rizik po protiopatřeních do přijatelnější oblasti, pod ní se opakuje tabulka před opatřeními pro lepší názornost. Pouze riziko dopravních nehod je stále vysoké, to je však důsledkem působení lidského prvku v řízení vozidel. Oproti původnímu stavu, kde byla rizika vyhodnocena jako nízká / střední / vysoká v poměru 5 / 7 / 3, bylo 6 rizik vyhodnoceno jako nízký ch,8 jako středních a 1 jako vysoké.

Tabulka 11:Maticové zobrazení závažnosti rizik po protiopatřeních

Matice rizik		Dopad				
		Žádný	Malý	Střední	Závažný	Kritický
Pravděpodobnost	Kritická	5/0	10/0	15/0	20/0	25/0
	Závažná	4/0	8/0	12/0	16/1	20/0
	Střední	3/0	6/0	9/0	12/0	15/0
	Malá	2/0	4/1	6/5	8/1	10/0
	Žádná	1/0	2/3	3/2	4/1	5/1

7.6. Dílčí závěr

Závěrem provedené analýzy jsou zejména doporučení na protiopatření pro rizika, která byla určena jako nejvýznamnější. Ostatním rizikům, která nebyla vyhodnocena jako kritická je věnována kapitola 7.4.6.

Pro zajištění kvalitního personálu je nutné, aby byly pozice obsazovány na základě výběrových řízení a byla posuzována praxe a schopnosti uchazeče o dané pracovní místo. Taktéž je nutné zajistit, aby byl zajištěn dostatečný počet personálu a nedocházelo k jeho přetěžování vlivem přesčasů nebo navýšení počtu směn. To by se mohlo projevit na poklesu pracovní morálky, vyšší chybovosti a nepozornosti, což by mohlo mít až katastrofické následky v případě dopravních nehod nebo jiných nestandardních stavů. Pro udržování kvalifikace operátorů řídících ústředen tunelových staveb se doporučuje pravidelné školení a ověřování schopností na simulátorech, který mimůže být například zmiňovaný TOMMS od spolednosti Eltodo a.s.. [69] [89]

Pro monitorování stavu technického vybavení je doporučeno využívat moderní systémy typu SCADA nebo DCS dle komplexnosti systému a požadavků na zabezpečení. V případě, že by byly využívány i systémy typu TUBIS od společnosti Eltodo a.s. je vhodné, aby takové společnosti splňovaly podmínky dle zákona č. 412/2005 Sb.: Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti §4 Stupně utajení odrážka d) Vyhrazené. To zejména z toho důvodu, že by se jednalo o přístup vnějšího prvku do uzavřeného systému, což hrozí bezpečnostním rizikem. [84] [88] [89]

Z důvodu uzavřenosti systémů vůči okolí je velice důležité dbát na důkladné fyzické zabezpečení objektů kritické infrastruktury. Při zajištění kvalitního fyzického zabezpečení se znatelně snižuje riziko ovlivnění nebo poškození systému, protože potenciální útočník nebude schopen překonat fyzické překážky, aby se dostal k technickému vybavení nacházejícím se uvnitř staveb. V případě využití elektronických přístupových systémů pro přístup se důrazně nedoporučuje využívat nezávislé systémy, protože neposkytují dostatečnou ochranu. Veškeré kritické prvky takovýchto systémů, jako jsou databáze klíčů nebo ovládání elektrického zámku a další, jsou uživateli přímo na dosah a tím pádem snadno a rychle ovlivnitelné. Někteří výrobci také volně poskytují na internetu návody a schémata konstrukce elektronických jednotek včetně detailního popisu bezpečnostních prvků, čímž defakto poskytují návod pro překonání daného zařízení. [60] [61]

V případě legislativy a technických předpisů na národní úrovni je vhodné zvážit využívání mezinárodního standardu IEC 61508 pro funkční bezpečnost elektronických zařízení a její rozdělení do čtyř úrovní SIL. Taktéž se doporučuje provést aktualizaci Technických podmínek TP 98, které jsou již v dnešní době překonané. Od roku jejich publikace (2004) proběhla pouze jedna změna v roce 2010, která však upřesňovala a doplňovala pouze některé části, nikoli dokument jako celek. Například část 10.5 Komunikační síť, která pojednává o komunikačních standardech využívaných v tunelový ch systémech.[45]

8. Závěr

Předmětem diplomové práce je problematika, týkající se bezpečnosti a s ní spojená opatření na kritické infrastruktuře pozemních komunikací. Lze ji rozdělit do dvou hlavních částí, přičemž do první spadají kapitoly 1 až 4 a do druhé spadají kapitoly 5 až 7.

V úvodu práce je čtenář obecně seznámen s problematikou kritické infrastruktury pozemních komunikací a v následujících podkapitolách se může dočíst o konkrétním definováním druhů pozemních komunikací v České republice a dopravní infrastruktuře, do které spadají nejen pozemní komunikace, ale i budovy související s jejich provozem a správou. Práce dále pojednává o kritické a evropské kritické infrastruktuře a legislativními dokumenty, které jsou s ní spojeny.

Ve druhé části se práce věnuje druhům útoků, kterým mohou prvky kritické infrastruktury čelit. Nejpodrobněji je poté rozebrána stránka fyzické bezpečnosti objektů a možnosti řešení přístupových bodů na infrastrukturních prvcích. Zejména z toho důvodu, že se na prvních kritické infrastruktury pozemních komunikaci uplatňují uzavřené systémy, ke který m nemají přístup žádná cizí zařízení, která by nebyla součástí systému. A také z toho důvodu, že sám autor práce byl v minulosti několikrát svědkem snadného překonání nevhodných řešení fyzického zabezpečení bezpečnostně vý znamný ch budov.

Ve své poslední části práce obsahuje rizikovou analý zu, z jejíchž výsledků lze konstatovat, že při vhodném návrhu protiopatření lze snížit možná rizika, kterým mohou prvky kritické infrastruktury v praxi čelit, na přijatelnější úroveň a zajistit tak bezpečnější fungování systémů na kritické infrastruktuře.

9. ZDROJE

[1] *Hasičský záchranný sbor České republiky* [online]. Generální ředitelství Hasičského záchranného sboru ČR, 2019 [cit. 2020-02-17]. Dostupné z: https://www.hzscr.cz/

[2] *Infrastruktura (Infrastructure)* [online]. ManagementMania.com, 2016 [cit. 2020-02-17]. Dostupné z: https://managementmania.com/cs/infrastruktura-infrastructure

[3] *Dopravní infrastruktura - Centrum investic, rozvoje a inovací Regionální rozvojová agentura Královehradeckého kraje* [online]. CiriHK, 2013 [cit. 2020-02-17]. Dostupné z: https://www.cirihk.cz/doprava.html

[4] *What is V2X communication? Creating connectivity for the autonomous car era* [online]. CBS Interactive, 2020 [cit. 2020-02-17]. Dostupné z: https://www.zdnet.com/article/what-is-v2x-communication-creating-connectivity-for-the-autonomous-car-era/

[5] *Infrastruktura silniční dopravy v ČR a kraji k 1.1.2016* [online]. Český statistický úřad, 2015 [cit. 2020-02-28]. Dostupné z: https://www.czso.cz/csu/xc/infrastruktura-silnicni-dopravy-k-1-1-2016

[6] *Ročenka dopravy 2018* [online]. Systém dopravních statistik, 2019 [cit. 2020-02-28]. Dostupné z: https://www.sydos.cz/cs/rocenka-2018/rocenka/htm_cz/cz18_321000.html

[7] *Infrastruktura* [online]. Vláda České republiky, 2012 [cit. 2020-02-28]. Dostupné z: https://www.vlada.cz/assets/ppov/udrzitelny-rozvoj/dokumenty/Infrastruktura--web-compressed.pdf

[8] *Souhrn způsobů hodnocení kvality a odolnosti infrastruktury: Závěrečná zpráva k veřejné zakázce Úřadu vlády ČR* [online]. Ostrava: Fakulta bezpečnostního inžený rství, Vysoká škola báňská – Technická univerzita Ostrava, 2016 [cit. 2020-03-06]. Dostupné z: https://www.vlada.cz/assets/ppov/udrzitelny-rozvoj/dokumenty/Infrastruktura--web-compressed.pdf

[9] *KRITICKÁ INFRASTRUKTURA* [online]. Město Jindřichův Hradec, 2011 [cit. 2020-02-28]. Dostupné z: https://m.jh.cz/filemanager/files/98510.pdf

[10] *Nařízení vlády č. 432/2010 Sb.* [online]. AION CS, 2020 [cit. 2020-02-28]. Dostupné z: https://www.zakonyprolidi.cz/cs/2010-432

[11] *Euroskop.cz - Zakládající smlouvy* [online]. Vláda České republiky, 2020 [cit. 2020-02-28]. Dostupné z: https://www.euroskop.cz/8917/sekce/zakladajici-smlouvy/

[12] *SMĚRNICE RADY 2008/114/ES ze dne 8. prosince 2008: o určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu*. In: . Úřední věstník Evropské unie, 2008.

[13] *Evropský program na ochranu kritické infrastruktury* [online]. Generální ředitelství Hasičského záchranného sboru ČR, 2020 [cit. 2020-03-02]. Dostupné z: https://www.hzscr.cz/clanek/evropsky-program-na-ochranu-kriticke-infrasruktury.aspx

[14] *Zákon č. 240/2000 Sb.: Zákon o krizovém řízení a o změně některých zákonů (krizový zákon)* [online]. AION CS, 2000 [cit. 2020-03-02]. Dostupné z: https://www.zakonyprolidi.cz/cs/2000-240

[15] *Národní program ochrany kritické infrastruktury*. GŘ HZS ČR / Ministerstvo vnitra, 2010 [cit. 2020-03-02]

[16] *DATABÁZE STRATEGIÍ: Portál strategických dokumentů v ČR* [online]. Ministerstvo pro místní rozvoj ČR, 2010 [cit. 2020-03-02]. Dostupné z: https://www.databaze-strategie.cz/cz/mv/strategie/narodni-program-ochrany-kriticke-infrastruktury

[17] *Komplexní strategie České republiky k řešení problematiky kritické infrastruktury a Národní program ochrany kritické infrastruktury (2010)* [online]. Portál krizového řízení JmK, 2018 [cit. 2020-03-02]. Dostupné z: http://krizport.firebrno.cz/dokumenty/komplexni-strategie-ceske-republiky-k-reseni-problematiky

[18] *Koncepce ochrany obyvatelstva do roku 2020 s výhledem do roku 2030*. Praha: MV - generální ředitelství Hasičského záchranného sboru ČR, 2013. ISBN 978-80-86466-50-7

[19] *Všechny členské státy EU ve zkratce* [online]. Oficiální internetové stránky Evropské unie, 2020 [cit. 2020-03-04]. Dostupné z: https://europa.eu/european-union/about-eu/countries/member-countries_cs

[20] *Document 52006DC0786* [online]. Brusel: EUR-Lex Access to European Union Law, 2006 [cit. 2020-03-04]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=celex:52006DC0786

[21] *ZELENÁ KNIHA: O EVROPSKÉM PROGRAMU NA OCHRANU KRITICKÉ INFRASTRUKTURY* [online]. Brusel: KOMISE EVROPSKÝCH SPOLEČENSTVÍ, 2005 [cit. 2020-03-04]. Dostupné z: http://krizport.firebrno.cz/dokumenty/zelena-kniha-o-evropskem-programu-na-ochranu-kriticke

[22] *Critical Infrastructure Warning Information Network (CIWIN)* [online]. European Commission [cit. 2020-03-04]. Dostupné z: https://ec.europa.eu/home-affairs/what-we-do/networks/critical_infrastructure_warning_information_network_en

[23] *Document 52004DC0702* [online]. Brusel: EUR-Lex Access to European Union Law, 2004 [cit. 2020-03-04]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:52004DC0702

[24] *Databázové systémy GIS: Kapitola 15. Geografie dopravy* [online]. Plzeň: Západočeská univerzita, Fakulta aplikovaných věd, Katedra matematiky, 2004 [cit. 2020-03-04]. Dostupné z: http://old.gis.zcu.cz/studium/dbg2/Materialy/html/ch15.html

[25] LUKÁŠ, Luděk. *Metodika hodnocení odolnosti vybraných prvků a systému prvků kritické infrastruktury*. Zlín: Univerzita Tomáše Bati ve Zlíně, 2013

[26] SLIVKOVÁ, Simona. *Určování kritických prvků v oblasti železniční dopravy*. Ostrava: Vysoká škola báňská –Technická univerzita Ostrava, 2018

[27] *Ředitelství silnic a dálnic* [online]. Ředitelství silnic a dálnic ČR, 2020 [cit. 2020-03-06]. Dostupné z: https://www.rsd.cz/wps/portal/

[28] *Zákon č. 13/1997 Sb.: Zákon o pozemních komunikacích* [online]. AION CS, 1997 [cit. 2020-03-06]. Dostupné z: https://www.zakonyprolidi.cz/cs/1997-13

[29] *Tunely: Definice, předpisy, základní požadavky* [online]. Ostrava: Fakulta bezpečnostního inženýrství, Vysoká škola báňská – Technická univerzita Ostrava, 2013 [cit. 2020-03-06]. Dostupné z: https://fbiweb.vsb.cz/safeteach/images/pdf/Prezentace/Tunely_definice.pdf

[30] *Základy navrhování mostů: 133RBZS* [online]. Praha: Fakulta stavební ČVUT v Praze, 2016 [cit. 2020-03-06]. Dostupné z: http://people.fsv.cvut.cz/www/foglamar/Download/RBZS/RBZS-mosty_sylabus.pdf

[31] FIALKA, *Jindřich. Ottův slovník naučný: Devatenáctý díl.* Praha: J. Otto, 1902.

[32] *Tunelový komplex Blanka* [online]. Metrostav, 2020 [cit. 2020-03-09]. Dostupné z: https://www.metrostav.cz/cs/obory-pusobnosti/podzemni-stavby/reference/55-tunelovy-komplex-blanka

[33] *Víte, že ... délka nejdelšího mostu v České republice, tzv. Radotínského mostu přesahuje 2 kilometry?* [online]. Czregion.cz, 2020 [cit. 2020-03-09]. Dostupné z: https://www.czregion.cz/vite-ze-delka-nejdelsiho-mostu-v-ceske-republice-tzv-radotinskeho-mostu-presahuje-2-kilometry

[34] *KŘIŽOVATKY POZEMNÍCH KOMUNIKACÍ* [online]. Vysoká škola báňská – Technická univerzita Ostrava, 2006 [cit. 2020-03-09]. Dostupné z: http://fast10.vsb.cz/krajcovic/!kombinovane/!dopravni_a_vodni_stavby/pomucky_k_reseni/pdf/KRIZOVATKY_PK_KOMBI.pdf

[35] *Přehledy z informačního systému o silniční a dálniční síti ČR: stav k 1.7.2019* [online]. Ředitelství silnic a dálnic ČR, 2019 [cit. 2020-03-09]. Dostupné z: https://www.rsd.cz/wps/wcm/connect/d4f00eed-e6d7-4488-bac4-233113763473/prehledy_2019_7_cr.pdf?MOD=AJPERES

[36] *Ekodukt* [online]. MeziStromy.cz, 2020 [cit. 2020-03-09]. Dostupné z: https://www.mezistromy.cz/slovnik/ekodukt

[37] *Fragmentace krajiny* [online]. MeziStromy.cz, 2020 [cit. 2020-03-09]. Dostupné z: https://www.mezistromy.cz/les-a-stromy/fragmentace-krajiny/odborny

[38] ŘEHÁK, David, Jaroslav CÍGLER, Pavel NĚMEC a Libor HADÁČEK. *KRITICKÁ INFRASTRUKTURA ELEKTROENERGETIKY: určování, posuzování a ochrana*. Ostrava: Sdružení požárního a bezpečnostního inženýrství v Ostravě, 2013. ISBN 978-80-7385-126-2

[39] *Metodika zajištění ochrany kritické infrastruktury v oblasti výroby, přenosu a distribuce elektrické energie* [online]. Česká republika: Deloitte, 2012 [cit. 2020-03-16]. Dostupné z: https://www.mvcr.cz/cthh/clanek/ochrana-kriticke-infrastruktury-ochrana-kriticke-infrastruktury.aspx

[40] *Bezpečnostní opatření* [online]. EBOZP, 2015 [cit. 2020-03-16]. Dostupné z: http://ebozp.vubp.cz/wiki/index.php/Bezpe%C4%8Dnostn%C3%AD_opat%C5%99en%C3%AD

[41] ŘEHÁK, David, Martin HROMADA a Pavel ŠENOVSKÝ. *RESILIENCE KRITICKÉ INFRASTRUKTURY: Teorie, principy, metody*. 2019. Sdružení požárního a bezpečnostního inženýrství. ISBN 978-80-7385-224-5

[42] RINALDI, S. M. a James P. PEERENBOOM. *Identifying, understanding, and analyzing critical infrastructure interdependencies: IEEE control systems*. 2002. DOI: 10.1109/37.969131

[43] *Tunel Blanka* [online]. SATRA, spol., 2019 [cit. 2020-03-29]. Dostupné z: https://www.tunelblanka.info/

[44] *Radotínský most* [online]. TN.cz / Jakub Deml, 2019 [cit. 2020-03-29]. Dostupné z: https://tn.nova.cz/clanek/zpravy/galerie/galerie-nej-mosty-a-tunely-ceska.html/?imageId=2022436#2022436

[45] PŘIBYL, Pavel. *Technologické vybavení tunelů pozemních komunikací: Technické podmínky TP 98*. Třetí, upravené. Praha: MD ČR - OPK, 2004. ISBN 80-239-0110-9

[46] *Asynchronous Transfer Mode (ATM) - Network encyclopedia* [online]. Network Encyclopedia, 2020 [cit. 2020-04-08]. Dostupné z: https://networkencyclopedia.com/asynchronous-transfer-mode-atm/

[47] *X.25 - Network encyclopedia* [online]. Network Encyclopedia, 2020 [cit. 2020-04-08]. Dostupné z: https://networkencyclopedia.com/asynchronous-transfer-mode-atm/

[48] LABUSCHAGNE, Frans a Jan ROOS. *Computers & Security: Data security in X.25 networks*. Elsevier, 1993, 469 - 475. DOI: 10.1016/0167-4048(93)90068-G

[49] PEYRAVIAN, Mohammad a Thomas D. TARMAN. *IEEE Network: Asynchronous Transfer Mode Security*. IEEE, 1997, 34 - 40. DOI: 10.1109/65.587048

[50] *KYBERNETICKÉ ÚTOKY* [online]. Praha: JUDr. Jan Kolouch [cit. 2020-04-09]. Dostupné z: https://csirt.cesnet.cz/_media/cs/documents/kyberneticke_utoky.pdf

[51] *History of Keys and Locks* [online]. 2020 [cit. 2020-04-10]. Dostupné z: http://www.historyofkeys.com/

[52] *Alex Young: What Are Electric Door Locks and How Do They Work?* [online]. Safewise, 2020 [cit. 2020-04-10]. Dostupné z: https://www.safewise.com/home-security-faq/electric-door-locks/

[53] *Raoul Chiesa: X.25 (in)SECURITY in year 2005: What, Why, When, Who, HowOR...(not anymore) uncovered data networks,(yet) covered targets.: [real life & field experiences on an underestimated and still actual security issue]* [online]. Kuala Lampur (MY), 2005 [cit. 2020-04-11]. Dostupné z: https://dl.packetstormsecurity.net/hitb05/BT-Raoul-Chiesa-X25-Security.pdf?fbclid=IwAR2YW5DkP6tpybCreu28pdNXNl0Gr93yeURudCAvoucYKo66TSdwCp_Th8g

[54] *Elektrické zámky | fab-shop.cz* [online]. fab-shop.cz, 2015 [cit. 2020-04-11]. Dostupné z: https://www.fab-shop.cz/c-elektricke-zamky

[55] *SARGENT® Manufacturing Company* [online]. 2020 [cit. 2020-04-12]. Dostupné z: https://www.sargentlock.com/en/

[56] VARADHARAJAN, Vijay, Rajan SHANKARAN a Michael HITCHENS. Security Issues in Asynchronous Transfer Mode. *Lecture Notes in Computer Science*., 1997, 76-89. DOI: 10.1007/BFb0027945

[57] *Deviant Ollam: Copying Keys from Photos, Molds & More* [online]. Wild West Hacking Fest 2018 [cit. 2020-04-15]. Dostupné z: https://wildwesthackinfest.com/

[58] *Lock Picks Australia: Locksmith Supplies* [online]. Lock Picks Australia, 2020 [cit. 2020-04-15]. Dostupné z: https://www.lockpicksaustralia.com.au/product/australian-bump-key-set-small/ [59]

[60] *TESLA STROPKOV, a.s.: zásuvka, vypínač, ISO, nástrojáreň, objímka, húkačky, húkačka | Úvod* [online]. 2020 [cit. 2020-04-18]. Dostupné z: https://www.tesla.sk/

[61] *Tesla Stropkov - Čechy a.s. - Návody* [online]. 2017 [cit. 2020-04-18]. Dostupné z: https://www.teslastropkov.cz/navody.htm

[62] PŘIBYL, Pavel, Aleš JANOTA a Juraj SPALEK. *Analýza a řízení rizik v dopravě: Tunely na pozemních komunikacích*. Praha: BEN - technická literatura, 2008. ISBN 978-80-7300-214-5

[63] *Klíčové centrum* [online]. Klíčové centrum, 2020 [cit. 2020-05-05]. Dostupné z: https://www.klicovecentrum.cz/bezpecnostni-tridy-vyznate-se-v-nich/

[64] PŘIBYL, Pavel, Aleš JANOTA a Juraj SPALEK. *Analýza a řízení rizik v dopravě: Tunely na pozemních komunikacích*. Praha: BEN - technická literatura, 2008. ISBN 978-80-7300-214-5

[65] *What is FMEA? Failure Mode & Effects Analysis | ASQ* [online]. American Society for Quality, 2020 [cit. 2020-05-08]. Dostupné z: https://asq.org/quality-resources/fmea

[66] *What is a Fault Tree Analysis?* [online]. American Society for Quality, 2002 [cit. 2020-05-08]. Dostupné z: http://asq.org/quality-progress/2002/03/problem-solving/what-is-a-fault-tree-analysis.html

[67] PATIL, Rajkumar Bhimgonda a Laxman WAGHMODE. Life Cycle Cost (LCC) Optimization of Band Saw Cutting Machine through Reliability Analysis. *1st International Conference on Mechanical Engineering: Emerging Trends in Engineering*. 2014

[68] KOUDELKA, Ctirad a Václav VRÁNA. *RIZIKA A JEJICH ANALÝZA*. Ostrava: VŠB – TU Ostrava, 2006

[69] *Eltodo TOMMS* [online]. Praha: Eltodo, 2014 [cit. 2020-05-11]. Dostupné z: http://www.tomms.cz/

[70] *PIARC Technical Commitee C.4: LIFE CYCLE ASPECTS OF ELECTRICAL ROAD TUNNEL EQUIPMENT*. PIARC, 2012. ISBN 978-2-84060-272-5

[71] *IEC 61508: Functional Safety - IEC 61508 Explained* [online]. International Electrotechnical Commission | IEC, 2020 [cit. 2020-05-11]. Dostupné z: https://www.iec.ch/functionalsafety/explained/

[72] PŘIBYL, Pavel, J. HEISSIGER, J. ŠTEFAN a L. HLADKÝ. *Technologické vybavení tunelů pozemních komunikací:: Technické podmínky - změna 1*. 2010. ELTODO EG

[73] *ČSN EN 1627 (746001): Dveře, okna, lehké obvodové pláště, mříže a okenice - Odolnost proti vloupání - Požadavky a klasifikace*. Český normalizační institut, 2012

[74] *Security Tip (ST04-015): Understanding Denial-of-Service Attacks* [online]. CISA | Department of Homeland Security, 2009 [cit. 2020-05-16]. Dostupné z: https://www.us-cert.gov/ncas/tips/ST04-015

[75] *Ransomware - What Is It & How To Remove It | Malwarebytes* [online]. Malwarebytes, 2020 [cit. 2020-05-16]. Dostupné z: https://www.malwarebytes.com/ransomware/

[76] *What is a keylogger? How attackers can monitor everything you type | CSO Online* [online]. IDG Communications, 2018 [cit. 2020-05-16]. Dostupné z: https://www.csoonline.com/article/3326304/what-is-a-keylogger-how-attackers-can-monitor-everything-you-type.html

[77] *What is a Firewall?: Firewalls defined, explained, and explored | Forcepoint* [online]. Forcepoint, 2020 [cit. 2020-05-16]. Dostupné z: https://www.forcepoint.com/cyber-edu/firewall

[78] *What is a Malware?: Malware defined, explained, and explored | Forcepoint* [online]. Forcepoint, 2020 [cit. 2020-05-16]. Dostupné z: https://www.forcepoint.com/cyber-edu/malware

[79] *SQL injection* [online]. w3schools, 2020 [cit. 2020-05-16]. Dostupné z: https://www.w3schools.com/sql/sql_injection.asp

[80] *USB Kill.com - Official USB Killer Site - USBKill* [online]. USBKILL, 2020 [cit. 2020-05-16]. Dostupné z: https://usbkill.com/

[81] HALDAR, Achintya a Sankaran MAHADEVAN. First-Order and Second-Order Reliability Methods. *Probabilistic Structural Mechanics Handbook: Theory and Industrial Applications*. Boston: Springer, 1995, 27-52. DOI: 10.1007/978-1-4615-1771-9_3

[82] *Monte Carlo Simulation Definition* [online]. Investopedia | Dotdash, 2020 [cit. 2020-05-17]. Dostupné z: https://www.investopedia.com/terms/m/montecarlosimulation.asp

[83] JANAS, Petr, Martin KREJSA a Vlastimil KREJSA. *Přímý Optimalizovaný Pravděpodobnostní Výpočet*. Vysoká škola báňská – Technická univerzita Ostrava, 2015. ISBN 978-80-248-3798-7

[84] *Zákon č. 412/2005 Sb.: Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti* [online]. AION CS, 2005 [cit. 2020-05-17]. Dostupné z: https://www.zakonyprolidi.cz/cs/2005-412

[85] *Zákon č. 181/2014 Sb.: Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)* [online]. AION CS, 2014 [cit. 2020-05-17]. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-181

[86] DURAČICKÁ, Zuzana. NIS: Co přináší nová směrnice EU o síťové a informační bezpečnosti? *IT Systems*. https://www.nic.cz/files/nic/doc/ITSystems_NIS_102016.pdf, 2016, 2-3

[87] *European Union Agency for Cybersecurity* [online]. ENISA, 2020 [cit. 2020-05-17]. Dostupné z: https://www.enisa.europa.eu/

[88] *PLC Programming Courses for Beginners*|*RealPars* [online]. RealPars B.V., 2020 [cit. 2020-05-17]. Dostupné z: https://realpars.com/

[89] TICHÝ, Tomáš, J. ŠTEFAN, R. PIXA a I. MILKÓŠIK. *SYSTÉM PRO ŘÍZENÍ, DIAGNOSTIKU A SIMULACI TECHNOLOGIE V TUNELECH*. Eltodo, 2019

10. SEZNAM OBRÁZKŮ

11. SEZNAM TABULEK