**PROVÁDĚCÍ KONCEPT SW ŘEŠENÍ (PK)**

projektu

Národní informační systém integrovaného záchranného systému (NIS IZS)

část

**G. Spolehlivost, disaster recovery a krizové scénáře**

Dokument obsahuje: Metodiku a výpočet bezpečnosti na úrovni HW   
a výpočet bezpečnosti na úrovni celého systému.

Verze: 5.1b

Schválil za Dodavatele: RNDr. Vladimír Příbramský

Aktualizace: 17/4/2014

Obsah

[01. Spolehlivost navrženého řešení 3](#_Toc385247376)

[1.1 Oblast telefonie 3](#_Toc385247377)

[1.2 Oblast SW 3](#_Toc385247378)

[Krizové scénáře 3](#_Toc385247379)

[1.2.1 Výpadek IPL na CDC 3](#_Toc385247380)

[1.2.2 Výpadek databáze na CDC 4](#_Toc385247381)

[1.2.3 Výpadek IPL na KDC 4](#_Toc385247382)

[1.2.4 Výpadek mapových služeb na KDC 5](#_Toc385247383)

[1.2.5 Výpadek konektivity na KDC (ostrovní provoz) 5](#_Toc385247384)

[1.3 Oblast HW 5](#_Toc385247385)

[Krizové scénáře 6](#_Toc385247386)

[1.3.1 Výpadek jednoho centrálního DC 6](#_Toc385247387)

[1.3.2 Výpadek dvou centrálních DC 6](#_Toc385247388)

[1.3.3 Výpadek tří centrálních DC 7](#_Toc385247389)

[1.3.4 Výpadek krajského DC 7](#_Toc385247390)

[1.3.5 Výpadek VDI serveru 7](#_Toc385247391)

[1.3.6 Výpadek elektrické energie 7](#_Toc385247392)

[1.3.7 Selhání HW 7](#_Toc385247393)

[1.3.8 Lidská chyba (manipulace s HW, nasazování nových verzí SW) 9](#_Toc385247394)

[1.4 Oblast síťové infrastruktury 9](#_Toc385247395)

[1.4.1 Výpadek jednoho síťového prvku v redundanci 9](#_Toc385247396)

[1.4.2 Výpadek obou prvků v redundanci 9](#_Toc385247397)

[1.4.3 Výpadek CDC 10](#_Toc385247398)

[1.4.4 Výpadek KDC 10](#_Toc385247399)

[1.4.5 Výpadek NSPTV 10](#_Toc385247400)

[1.4.6 Odpojení kraje od ITS 10](#_Toc385247401)

[1.4.7 Rozdělení kraje 10](#_Toc385247402)

[1.4.8 Rozpůlení ITS 10](#_Toc385247403)

[1.4.9 Ztrátovost na lince 11](#_Toc385247404)

[1.4.10 Pád ITS 11](#_Toc385247405)

# Spolehlivost navrženého řešení

Dodavatel návrhem řešení NIS IZS zajišťuje požadovanou vysokou dostupnost a 200% zálohu všech služeb provozovaných v režimu 24x7x365 a definovanou dostupnost dle smlouvy. Následující kapitoly popisují zajištění spolehlivosti jednotlivých subsystémů, krizové scénáře a postupy pro disaster recovery.

### Oblast telefonie

Příjem tísňových volání je zajištěn na úrovni KDC a jako kritická služba má 300% zálohu. Řešení IP telefonie je navržené jako dvouvrstvá architektura. Vlastní řízení telefonie a pořizování záznamu hovoru je na úrovni KDC, část funkcionalit kontaktního centra a management nahrávek a jejich archivace je na úrovni CDC.

Systémy řízení telefonie umístěné v jednotlivých KDC musí být pro zajištění požadované míry spolehlivosti vždy zdvojené, pracující v režimu Active-Active. Pro zajištění další míry zabezpečení je hovor určený pro zpracování v rámci určitého kraje v případě nedostupnosti konektivity do hlasových bran v primární lokalitě doručen na vstupní linky „párového kraje“. V případě výpadku hlasové technologie umístěné v rámci jednoho kraje bude v rámci konfigurace systémů umístěných v „párovém kraji“ zajištěna přeregistrace telefonních přístrojů z takto postiženého kraje. Daného fungování bude využito v případě zachování vnitřní konektivity propojených krajských systémů. V případě výpadku obou krajských systémů, tvořících funkční pár, bude hovor směrován z veřejné sítě dle dalších nastavených kritérií (přeliv v případě HZS, přesměrování tísňových hovorů do telefonie OŘ u PČR a ZZS).

### Oblast SW

Navržená architektura AAA je řešena jako 3 aktivní DC, která mají plně konzistentní data v databázi s tím, že v konzistentním stavu jsou data v databázi udržována replikačním mechanismem na úrovni ESB. Při výpadku jednoho DC jsou k dispozici dvě plnohodnotná DC. Při výpadku dvou DC je k dispozici třetí plnohodnotné DC s plně konzistentními daty a to bez přerušení provozu.

### Krizové scénáře

### Výpadek IPL na CDC

V případě, že dojde k výpadku k výpadku uzlu IPL v CDC, přebírá jeho funkcionalitu další uzel v rámci Fabric clusteru. Funkcionalita CDC není v tomto případě nijak omezena. Po jeho obnovení dohledovým centrem je uzel zapojen do Fabric clusteru a dochází k obnovení standardního režimu provozu.

V případě, že dojde k výpadku obou uzlů IPL ve Fabric clusteru v daném CDC, přestává být CDC jako takové v rámci NIS IZS aktivní a dochází k jeho odstavení. Funkcionalitu inkriminovaného CDC přebírá další CDC. MiniIPL na KDC registruje nedostupnost IPL na CDC a registruje klienty NSPTV na jiné dostupné CDC.

V případě výpadku IPL na dvou uzlech je řešení situace analogické. Tzn., dojde k odstavení obou center. Po obnovení funkcionality CDC respektive dvou CDC, jsou zařazeny CDC jako aktivní a miniIPL na KDC na ně opět směrují provoz.

### Výpadek databáze na CDC

Výpadek databáze na CDC je možný v dvojím charakteru. Databáze v rámci jedno CDC je zdvojena na dvou uzlech, které je možné v případě výpadku jednoho nahradit. Databáze je tedy plně odolná proti výpadku jednoho ze dvou nodů CDC.

V případě, že by došlo k výpadku obou uzlů databáze (ať již sehnáním obou databází nebo jinou funkcionalitou CDC), dojde k odstavení provozu na dané CDC a přesměrování na další CDC. Tento zásah je možné realizovat díky použité multi-master replikaci. Replikační řešení umožní běh řešení i přes případný výpadek dvou CDC.

#### Scénář výpadku jednoho databázového uzlu v rámci CDC

Po výpadku aktivní databáze je automaticky přesměrována komunikace s DB pomocí failover mechanizmu na druhou databázi. Poškozená databáze nebo virtuální stroj, na kterém databáze běžela je následně obnoven a zařazen do failover režimu.

#### Scénář výpadku dvou databázových uzlů v rámci CDC

Po výpadku obou databázových uzlů je pomocí automatizovaného monitoringu (po uplynutí timeoutu) nastavena IPL datového centra jako neaktivní. Přihlášeným operátorům je odeslána informace o nedostupnosti CDC a požadavek na novou registraci na CDC. Stejně tak je odeslána i informace o nedostupnosti CDC všem krajským miniIPL, které vybírají CDC pro připojení operátorů NSPTV. Po obnovení obou DB uzlů na postiženém CDC je replikačním nástrojem enterpriseDB, dle transakčního logu dosynchronizována databáze do konsistentní podoby. Dohledové centrum na základě monitoringu zprovozní CDC jako aktivní.

#### Scénář výpadku databází dvou CDC

V případě výpadku funkcionality databáze na dvou CDC je veškerý provoz směrován na třetí CDC, které kapacitně dostačuje nárokům na zapojení všech operátorů. Obnovu stavu databází řeší dohledové centrum, které postupně zapojí obnovené CDC a dojde k synchronizaci dat v databázích.

### Výpadek IPL na KDC

V případě, že dojde k výpadku k výpadku uzlu miniIPL v KCD, přebírá jeho funkcionalitu další uzel v rámci Fabric clusteru. Funkcionalita KCD není v tomto případě nijak omezena. Po jeho obnovení dohledovým centrem je uzel zapojen do Fabric clusteru a dochází k obnovení standardního režimu provozu.

V případě, že dojde k výpadku obou uzlů miniIPL ve Fabric clusteru v daném KDC, přestává být miniIPL jako takové v rámci NIS IZS aktivní a dochází k jeho odstavení. Funkcionalitu inkriminovaného KDC přebírá CDC. Přebrání funckionality miniIPL KDC je realizováno v rámci automatizovaného dohledu služeb KDC. Komunikaci s telefonní službou zajištuje IPL v CDC. V tomto případě je také nedostupný registr mapových služeb na KCD. Klienti OŘ si musejí zajistit komunikaci s předem definovaným KDC. Po obnovení funkcionality je obnovena původní komunikace miniIPL s telefonií a registr služeb na miniIPL.

### Výpadek mapových služeb na KDC

V případě, že dojde k výpadku GISové služby na daném KDC, je nutné, aby systémy konzumující tuto službu, přešli na záložní KDC. Mechanizmus přechodu je řešen za pomoci miniIPL na KDC. MiniIPL vrací konzumujícím klientským aplikacím adresu REST služeb na GIS, v případě lokálního výpadku jsou miniIPL vraceny adresy ze zastupujícího KDC. Výpadek služeb ArcGIS I (služby specifické na úrovni kraje) návrh neřeší.

Po obnovení funkcionality mapových služeb je přes miniIPL na KDC vracena opět lokální adresa mapových služeb daného KDC.

### Výpadek konektivity na KDC (ostrovní provoz)

V případě výpadku absolutní konektivity na KDC přechází systém do režimu ostrovního provozu. Aplikace NSPTV jako taková je neaktivní v daném kraji a příjem tísňového volání je u složek ZZS a PČR přesměrován na úrovni telefonie do OŘ. U HZS je a příjem tísňového volání zajištěn přelivem hovorů do jiného předem definovaného kraje. Mapové služby pro OŘ jsou tímto výpadkem nedotčeny.

Po obnovení konektivity je příjem telefonních hovorů opět směrován na dané KDC.

V případě výpadku konektivy na ITS v KDC je možné tok datových vět z NSPTV do OŘ HZS postiženého kraje směrovat přes záložní konektivitu MPLS mezi OŘ HZS a CDC.

### Oblast HW

Architektura řešení vychází z koncepce tří aktivních nezávislých DC s rozložením zátěže. Jednotlivé instance databází, souborového systému jsou rovnoměrně distribuovány přes všechna DC a využití/zátěž datového provozu je monitorována a spravována síťovým load-balancerem v HA zapojení.

V architektuře tří aktivních nezávislých CDC s rozložením zátěže na všechna tři CDC s online synchronizací databáze, souborového systému, bude nastaven nadřazený monitoring v Hypervizoru, který bude rozkládat zátěž na všechna tři DC.

Vzhledem k tomu, že je zátěž rozložena na všechna tři DC s hlavním důrazem na pražské CDC 1 a Plzeňské CDC 3 + KDC PL a Olomouc CDC 2 + KDC OL (v poměru 40+40+20), je umožněno využít část kapacity výpočetního výkonu DC v Olomouci na školení, testování a jiné servisní úlohy. V případě výpadku některého DC jsou operátoři směrováni na jiné aktivní CDC. Na všech DC vždy běží celá nezávislá infrastruktura, která poskytuje operátorům stejné služby. Uživatel ve své podstatě nepozná na jaké CDC je připojen a provoz je automaticky řízen load balancery, které směrují požadavky uživatelů podle nadefinovaných pravidel. Stav datových center je monitorován z lokality nezávislé na těchto CDC/KDC.

Disaster recovery proces má popsat proces obnovy normálního provozu NIS-IZS při neočekávaném výpadku/havárii, při němž dojde k přerušení nebo omezení činnosti některé ze systémových součástí nebo výpadku více takových součástí. Příčiny výpadku mohou být následující:

* Výpadek na komunikační síti;
* Selhání HW;
* Lidská chyba (manipulace s HW, implementace nových verzí SW);
* Selhání DC (el. energie, povodně, bouřky, požáry, apod.);

V takovýchto případech je potřeba zajistit detekci výpadku, kontinuitu provozu, krizovou komunikaci, ochranu infrastruktury, integritu informačních systémů a obnovení provozu v době, která je definována v provozní smlouvě.

Pro detekci výpadku je nutné zařadit do infrastruktury NIS-IZS monitorovací prvek ve formě dohledového pracoviště, které bude umístěno mimo DC. Toto dohledové pracoviště bude nepřetržitě sledovat a vyhodnocovat dostupnost všech sledovaných systémů v jednotlivých DC a v případě nenadálé události a/nebo výpadku, započne proces k zajištění kontinuity provozu, zahájí krizovou komunikaci a podnikne všechny nezbytné kroky k obnovení plného provozu.

Proces zajištění kontinuity provozu spočívá v následujících krocích:

1. Detekce chyby
2. Přesměrování provozu na běžící DC
3. Stanovení příčiny a určení doby, kdy dojde k obnovení plného provozu
4. Obnova DC s výpadkem:
   1. Obecná
      * + Nahlášení výpadku s identifikací problému a doby jeho pravděpodobného odstranění.
        + Definovaný scénář, který je samostatně uvedený níže (např. selhání HW, viz ad. 5.2.)
        + Kontrola konzistentního stavu databázových operací.
        + Synchronizace (nebo kontrola) souborových systémů obsahujících telefonní záznamy.
        + Připojení DC zpět do provozu;
        + Kontrola dosynchronizace dat ze  vzniklého časového okna do plně synchronního stavu.
   2. Selhání HW
      * Výměna nefunkčního HW
   3. Při lidské chybě (např. upgrade SW)
      * Obnovení VM do stavu před zásahem

### Krizové scénáře

### Výpadek jednoho centrálního DC

Po výpadku jednoho CDC budou v ostatních aktivních CDC dostupné veškeré služby NIS IZS, zátěž na aktivní 2 CDC je load balancery rozkládána v poměru 50:50. Po obnově vypadlého DC dojde k jeho uvedení do stavu shodného s aktivními DC (automaticky - dosynchronizace DB, přenesení změn na souborovém systému, manuálně – synchronizace systémových a aplikačních updatů, resp. konfigurací v případě), následně bude ručně obnoveno rozkládání zátěže opět na všechna tři CDC.

### Výpadek dvou centrálních DC

Krizový scénář počítá s výpadkem dvou DC (najednou nebo postupně), kdy je veškerý provoz směrován na poslední zbývající CDC. Běžící CDC bude mít nastavenou automatickou politiku v Hypervizoru, který pomocí nastavených pravidel pro rozdělování systémových zdrojů zajistí přednost běhu produkčního prostředí na úkor testovacího a školícího, aby zajistilo dostatečný výkon na odbavení operátorských požadavků. Scénář obnovy počítá s postupnou obnovou nejdříve jednoho CDC a po jeho uvedení do provozu bude započata obnova zbývajícího CDC (postup bude shodný jako v případě scénáře výpadku jednoho DC).

### Výpadek tří centrálních DC

Krizový scénář počítá s výpadkem tří CDC (najednou nebo postupně) a to způsobem, kdy dojde k přesměrování veškerého telefonního provozu na záložní řešení v systémech OŘ, a to do doby než bude alespoň jedno CDC zprovozněno.

### Výpadek krajského DC

Tento scénář předpokládá nedostupnost KDC z pohledu serverové infrastruktury. Zálohu pro KC zajišťuje primárně další KDC. Scénář je nutné vnímat zejména z pohledu systémů pro operační řízení (uživatelé KDC).

### Výpadek VDI serveru

1. V tomto případě se jedná o výpadek jednoho VDI serveru v Clusteru v rámci složky (ZZS nebo PČR). Druhý server umístěný v dané lokalitě zajistí virtuální koncové stanice bez výpadku spojení. Příjem tísňových hovorů nebude nijak zasažen.
2. V tomto případě se jedná o výpadek obou VDI serverů v Clusteru v rámci složky (ZZS nebo PČR). Příjem tísňových hovorů bude v tomto případě realizován podle záložního scénáře při nedostupnosti všech pracovišť dané složky v kraji (přeliv, přesměrování). V případě výpadku VDI serverů při probíhajícím hovoru se hovor neukončí. Bude možné takový hovor dovytěžit bez běžící aplikace ApNIS. V aplikaci ApNIS, u neuzavřených událostí bude umožněno i jiným operátorům dopisování informací, které byly vytěženy po pádu  Clusteru VDI serverů.

### Výpadek elektrické energie

Krizový scénář počítá s možným výpadkem napájení el. energií tak, že se předpokládá, že přívod el. energie pro potřeby napájení zařízení v serverovně DC bude rozdělen do dvou nezávislých větví, minimálně na úrovni zdvojených rozvaděčů. Do každého racku budou přivedeny dva nezávislé přívody a připojeny k PDU (Power Distribution Unit) racku, které jsou taktéž zdvojeny.

Dojde-li k výpadku jedné napájecí větve, jsou všechna zařízení v racku napájena přes zbývající PDU a odpovídající DC zdroje (které jsou v každém konkrétním zařízení taktéž zdvojeny).

Pro případ celkového výpadku dodávky el. energie od dodavatele budou v každé napájecí větvi zapojeny zdvojené UPS odpovídajícího výkonu, které umožní bezpečné uložení a zachování konzistentních stavů dat aplikací běžících v rámci NIS IZS a také případné vypnutí všech zařízení, která jsou součástí řešení NIS IZS. UPS bude schopna dodávat el. energii odpovídajícího výkonu po dobu nejméně 20 minut. K překlenutí doby přerušení dodávky el. energie bude zároveň do el. sítě automaticky zapojen nezávislý zdroj el. energie v podobě dieselagregátu, který bude schopen dodávat minimálně takový výkon, aby byl schopen udržet provoz všech zařízení NIS IZS po libovolně dlouhou dobu, a to pouze doplňováním potřebných provozních zdrojů.

Pro případ výpadku chladicího systému DC je počítáno s jeho kompletním zdvojením v rámci celého DC v kapacitě potřebné pro udržení provozního prostředí pro všechna zařízení NIS IZS.

### Selhání HW

Krizový scénář předchází možnému selhání jakéhokoliv HW tak, že veškerý HW je minimálně zdvojen, a to jak na úrovni základních komponent, tak i na úrovni celých DC. V případě selhání HW se počítá se zahájením servisních prací dle sjednaného SLA v provozní smlouvě.

1. Blade chassis
   1. Je odolné vůči 50 procentnímu výpadku počtu ventilátorů
   2. Je odolné vůči 50 procentnímu výpadku napájecích zdrojů
   3. Je odolné vůči 50 procentnímu výpadku síťových modulů

Technik vymění v rámci SLA vadný díl za běhu systému. Tyto subsystémy jsou vyměnitelné za běhu zařízení (technologie hot-plug)

* 1. Havárie blade serveru

Server se za běhu systému vyjme a nahradí plně funkčním serverem za běhu systému. Na něj se následně nainstaluje Hypervizor, který se zapojí do Centrální správy virtualizace, kde blade server přebere roli havarovaného serveru.

Při vyšším než 50 procentním výpadku subsystému (chlazení, zdroje, sítě) se provoz automaticky pomocí load balanceru přesměruje na jiné funkční CDC a blade servery se manuálně odstaví. Následně se bude se řešit servis vadných dílů.

1. Výpadek rack serveru
   1. Výpadek napájecího zdroje
   2. Výpadek napájecího zdroje
   3. Výpadek ventilátoru

Technik vymění v rámci SLA vadný díl za běhu systému. Tyto sub systémy jsou vyměnitelné za běhu (technologie hot-plug)

* 1. Závažnější závada (síť, řadič disku, CPU, RAM, základní deska atd.)

V tomto scénáři se server odstaví a technik provede potřebnou opravu. Do provozu se RACK server vrátí nainstalováním a nastavením Hypervizoru. Následně se procesně uvede do provozního stavu.

1. Diskové pole CDC/KD
   1. Havárie disku (redundance dle RAID)

Technik vymění disk v rámci SLA za běhu systému. Tyto sub systémy jsou vyměnitelné za běhu (technologie hot-swap).

* 1. Havárie zdroje (redundance 2N)

Technik zdroj disk v rámci SLA za běhu systému. Tyto sub systémy jsou vyměnitelné za běhu (technologie hot-swap).

* 1. havárie řadiče

Přebírá jeho provoz druhý, v případě havárie obou (nebo příslušné police) se odstavuje diskové pole, provoz se pomocí load balanceru směruje na jiné datacentrum a technik provede výměnu dílu, otestuje a obnoví provoz diskového pole a připojí do Hypervizoru. Následně se procesně uvede do provozního stavu.

1. Archivační jednotka (HW)
   1. Je odolná vůči 50 procentnímu výpadku počtu ventilátorů
   2. Je odolná vůči 50 procentnímu výpadku napájecích zdrojů
   3. Je odolná vůči 50 procentnímu výpadku síťových modulů
   4. Je odolná vůči 50 procentnímu výpadku nodů (tzv. serverových nodů/modulů)

Technik vymění v rámci SLA vadný díl za běhu systému. Tyto sub systémy jsou vyměnitelné za běhu díky architektuře RAIN

V případě výpadku celé archivační jednotky přebírá automaticky celý provoz pomocí load balanceru archivační jednotka v druhém CDC. Po zprovoznění archivační jednotky je následně ručně přesměrován provoz zpět a automaticky se zahájí dosynchronizace dat.

V případě výpadku všech tří archivačních jednotek se archivovaná data ukládají na provozní diskové pole v každém CDC. Po zprovoznění jedné archivační jednotky jsou archivovaná data z provozních diskových polí automaticky přesunuta do archivační jednotky pomocí archivačního SW. Všechny 3 archivační jednotky se zprovozňují jedna po druhé a ihned do zprovoznění automaticky pomocí load balanceru a archivačního SW přecházejí do normálního provozního stavu. Každá zprovozněná archivační jednotka se automaticky sesynchronizuje s ostatními běžícími archivačními jednotkami.

### Lidská chyba (manipulace s HW, nasazování nových verzí SW)

V případě lidské chyby (zpravidla chyba administrátora), se následky řeší podle typu způsobených škod, viz výše uvedené krizové scénáře. V případě nasazování nových SW releasů je vždy popsán mechanismus pro návrat do posledního provozního stavu. V případě zásadních změn aplikace (např. změna databázových objektů) je k nasazování vypracován podrobný scénář s tím, že bude zpravidla postupováno v následujících krocích:

1. Odstavení CDC/KDC
2. Nasazení změny
3. Otestování změny
4. Datová dosynchronizace
5. Přesměrování provozu na DC 1
6. Smoke testy
7. Odstavení DC 2 a 3
8. Nasazení změny
9. Otestování změny
10. Datová dosynchronizace
11. Obnovení plného provozu

### Oblast síťové infrastruktury

### Výpadek jednoho síťového prvku v redundanci

V případě výpadku jednoho jakéhokoliv prvku v redundanci dojde k okamžitému převzetí plné funkcionality na druhý prvek. Tato konvergence bude v řádech jednotek ms a neovlivní běžný provoz sítě. Pro příklad vypadne jeden z CE směrovačů, kontrolní mechanizmy například HSRP zareaguje okamžitě změnou směrovací tabulky na druhém CE a dojde k obnovení datového okruhu. Podobně se zachová přepínačová, firewallová a load-balancerová vrstva sítě. V tomto scénáři nedojde k rozpojení datových ani telefonních spojení.

### Výpadek obou prvků v redundanci

V případě výpadku dvou prvků v redundanci dojde k následujícím událostem.

1. Výpadek CE směrovačů

Všechny připojené moduly systému jsou odpojeny od ITS. OS je plně nefunkční, CDC a KDC je odpojeno

1. Výpadek centrálních přepínačů CDC/KDC/OS

OS bude plně bez jakéhokoliv připojení

CDC/KDC budou okamžitě automaticky odpojeny od systému a bude se k nim přistupovat jako k celkovému výpadku datového centra.

1. Výpadek firewall a load-balancerů v CDC.

CDC bude okamžitě automaticky odpojeno od systému a bude se k němu přistupovat jako k celkovému výpadku CDC. Zbylé CDC převezmou veškerou funkcionalitu za vypadlé CDC a to až do jediného zbylého CDC.

### Výpadek CDC

V případě výpadku obou CE routerů v CDC dojde k automatickému přesměrování provozu na jiné CDC. Toto přesměrování bude iniciováno monitoringem.

### Výpadek KDC

V případě výpadku obou CE routerů v KDC (resp. v CDC s funkcí KDC) dojde k automatickému přesměrování provozu ze všech systémů OŘ a NSPTV ZZS a PČR na jiné funkční KDC. Pracoviště NSPTV v lokalitě HZS bude v takovém případě zcela bez konektivity a bude považováno za nedostupné; příslušné tísňové hovory budou směrovány na základě pravidel pro přelivy do lokality HZS v jiném kraji.

### Výpadek NSPTV

V případě výpadku obou CE routerů v lokalitě NSPTV (složky PČR, ZZS) bude taková lokalita z pohledu NIS IZS považována za nedostupnou a tísňová volání příslušná dané složce a kraji budou směrována do příslušného systému OŘ dané složky. Systémy OŘ vyjma lokality HZS budou odděleny zvláštními CE routery, tudíž je takový výpadek neovlivní.

### Odpojení kraje od ITS

V případě odpojení celého kraje od ITS, přejde síťová infrastruktura kraje na ostrovní režim, kdy dojde k zachování plné datové komunikace v rámci kraje. Pro zajištění ostrovního režimu budou všechny směrovače v kraji v zapojeni full mesh a směrování je tímto zachováno.

### Rozdělení kraje

V případě rozdělení kraje, kdy nebude přímá komunikace mezi jednotlivými složkami, dojde k přesměrování datových toků mezi složkami a KDC pomocí okruhu sítě ITS přes republikový okruh. Toto přesměrování toků je do 150ms, dojde však ke zvýšení latence, která by v rámci jednoho ITS okruhu nepřesáhla 30ms.

### Rozpůlení ITS

V případě rozpůlení ITS bude komunikace v rozdělených částech plně zachovaná, jednotlivá OS budou mít plný přístup ke KDC/CDC které zůstanou v dané části ITS. Komunikace mezi rozdělenými CDC/KDC nebude možná.

### Ztrátovost na lince

V případě ztrátovosti linky dojde k automatickému odpojení problémové linky a konvergence zachová plnou funkcionalitu všech propojení. V případě ztrátovosti na síťových zařízení dojde k vyřazení chybujícího zařízení z provozu, konvergence ITS se opět postará o obnovení datových spojení. Konvergence ITS je definována na 150ms.

### Pád ITS

V případě celkového pádu ITS nebudou funkční žádná propojení. Telefonie se bude směrovat do OŘ.