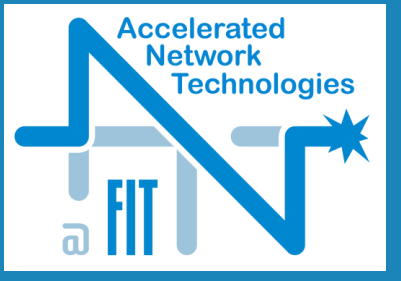
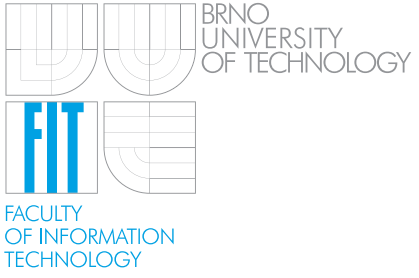
SIGCOMM 2011
Session 9
Network Architecture and Operations



Vlastimil Košař

Brno University of Technology, Faculty of Information Technology
Božetěchova 2, 612 00 Brno, CZ
www.fit.vutbr.cz/~ikosar



INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Obsah

Článek 1.

R3: Resilient Routing Reconfiguration
Ye Wang, Hao Wang, Ajay Mahimkar, Richard Alimi, Yin Zhang, Lili Qiu, Y. Richard Yang

Problémy současných sítí z pohledu odolnosti

- Používáno rychlé přesměrování (FRR) pro zajištění odolnosti při výpadku
  - Složitost - náročnost na šířku pásma a složitost výpočtu při násobných výpadcích
  - Zahlcení - dominový efekt při násobných výpadcích
  - Nemožnost předpovědět výkon řešení kvůli obrovskému množství možných permutací

Cíle R3

- Dokazatelně odolný proti zahlcení při množství různých scénářů selhání
- Efektivní využívání výpočetního výkonu a paměti
- Flexibilní z pohledu různých výkonnostních požadavků
- Odolný proti variabilitě síťového provozu a selháním topologie

Rozšíření

- Variabilní provoz
- Realistické scénáře selhání
- Prioritní odolné směrování
- Ladění parametrů - výkon x vytížení sítě x zpoždění
- MPLS směrování na základě toků

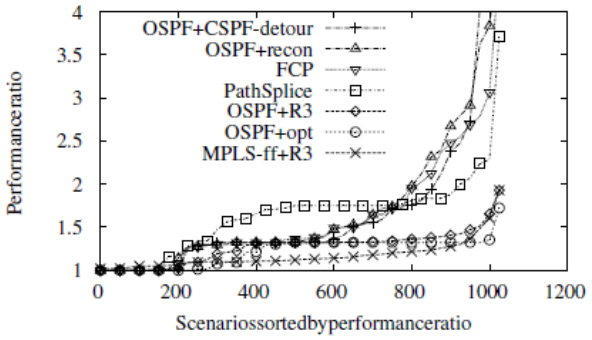
Fáze fungování R3

- Offline precomputation - předpočítání možných přesměrování podle scénářů výpadků
  - Minimalizace maximálního zatížení linek při možném přesměrování
  - Optimalizace pomocí lineární programování
- Online reconfiguration - úprava předpočítaných přřesměrování podle aktuálního selhání
  - Vyhnutí se vypadnuté lince
  - Efektivně vypočitatelná v reálném čase

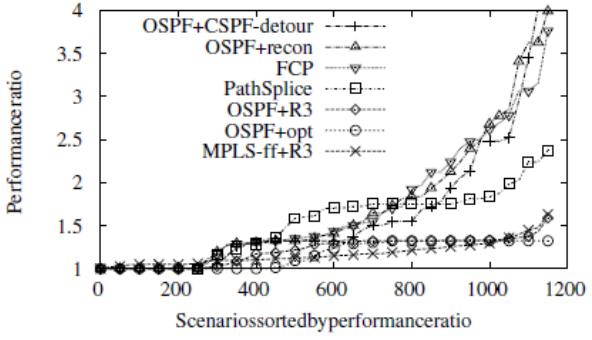
Vyhodnocení

- Simulace nad modely několika velkých sítí

Výkonnost při selhání

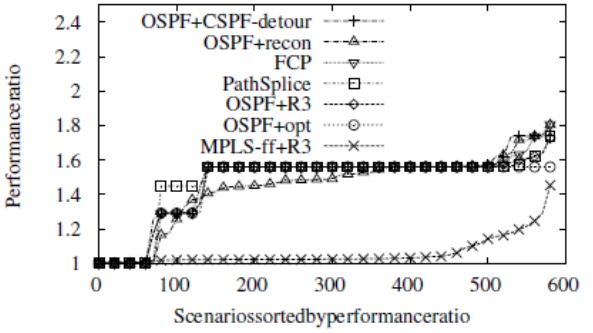


(a) two failures

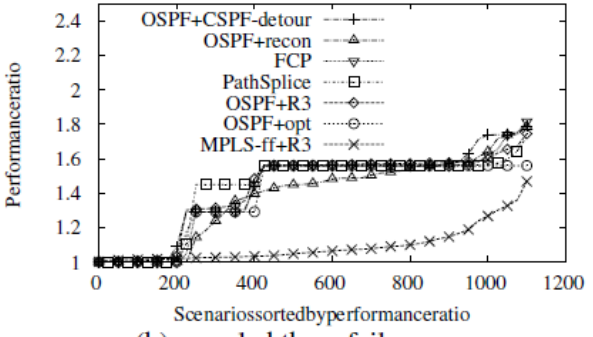


(b) sampled three failures

Figure 5: Sorted performance ratio under multiple failures during peak hour: US-ISP.



(a) two failures



(b) sampled three failures

Figure 6: Sorted performance ratio: SBC.

Článek 2.

Detecting the Performance Impact of Upgrades in Large Operational Networks

Ajay Mahimkar, Han Hee Song, Zihui Ge, Aman Shaikh, Jia Wang, Jennifer Yates, Yin Zhang, Joanne Emmons

Proč detekovat

- Změny mohou mít významný dopad na chování a vlastnosti sítě
- Ve velkých sítí může být dopad upgrade nečekaný
- Ve velkých sítí je ruční kontrola nepraktická a zdlouhavá
- Časté změny ve velkých sítích

Výzvy

- Jak identifikovat upgrade v síti
- Jak zjistit dopad upgrade
- Jaké jsou společné vlastnosti mezi elementy s podobnými detekovanými změnami chování
- Jak detekovat celosíťové agregované změny chování

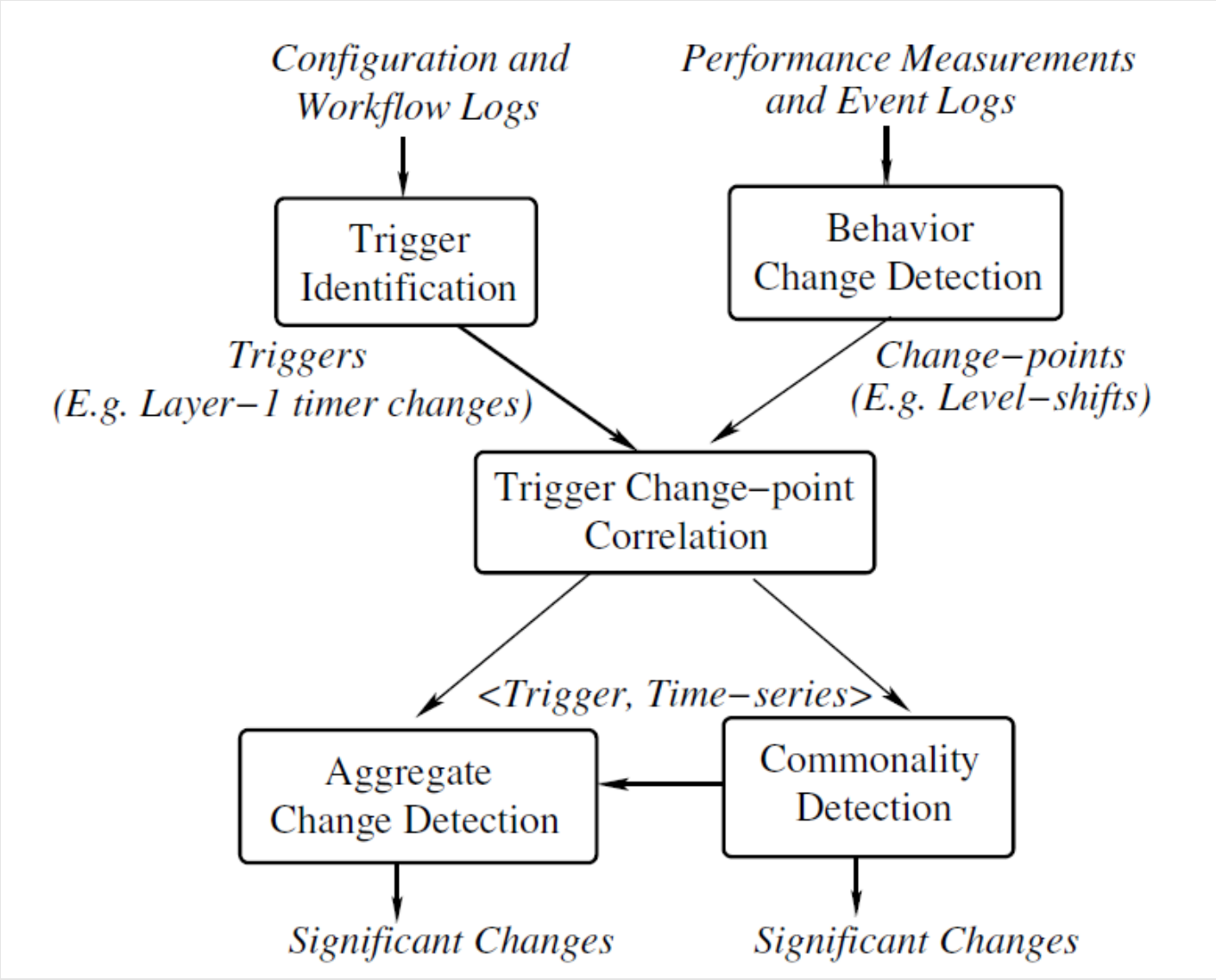
Síťové upgrade

- Operční systémy a firmware
- Konfigurace

Zdroje klíčových identifikátorů výkonu

- SNMP
- Syslog

Architektura



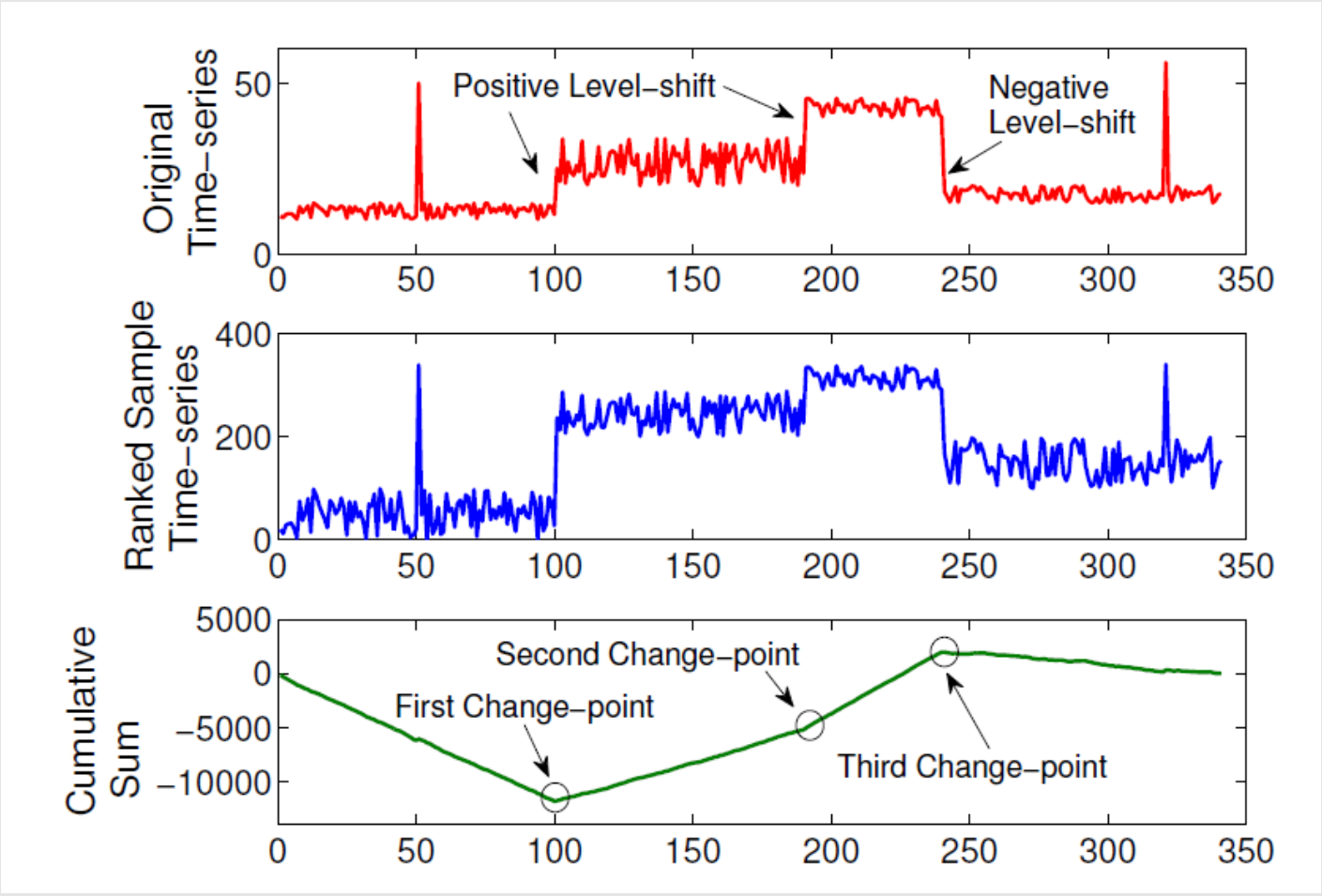
Přístup a přínosy

- Metriky ohodnocení parametrů změn (trigger)
  - Vzácnost - upgrady jsou obyčejně vzácné
  - Coverage/Skewness - upgardy zasahují větší množství elementů
- Detekce trvalé změny
  - Non-parametric rank-based behavior change detector (CUSUM)
  - Pro každý parametr vyhodnocuje více bodů změny a ohodnocuje je důležitostí změny
- Detekce klíčových identifikátorů
  - Detekuje identifikátory spojené s normálním provozem sítě nemající vliv na výkonnost a odfitruje je
  - Pak aplikuje statistical rule mining - identifikace atributů běžného chování sítě
- Agreguje události podle oblastí s běžným chováním a pak aplikuje detekci změn

Vyhodnocení

- Data od Tier-1 ISP

CUSUM detekce více bodů změny



False positive rate pro rarness a skewess metriky

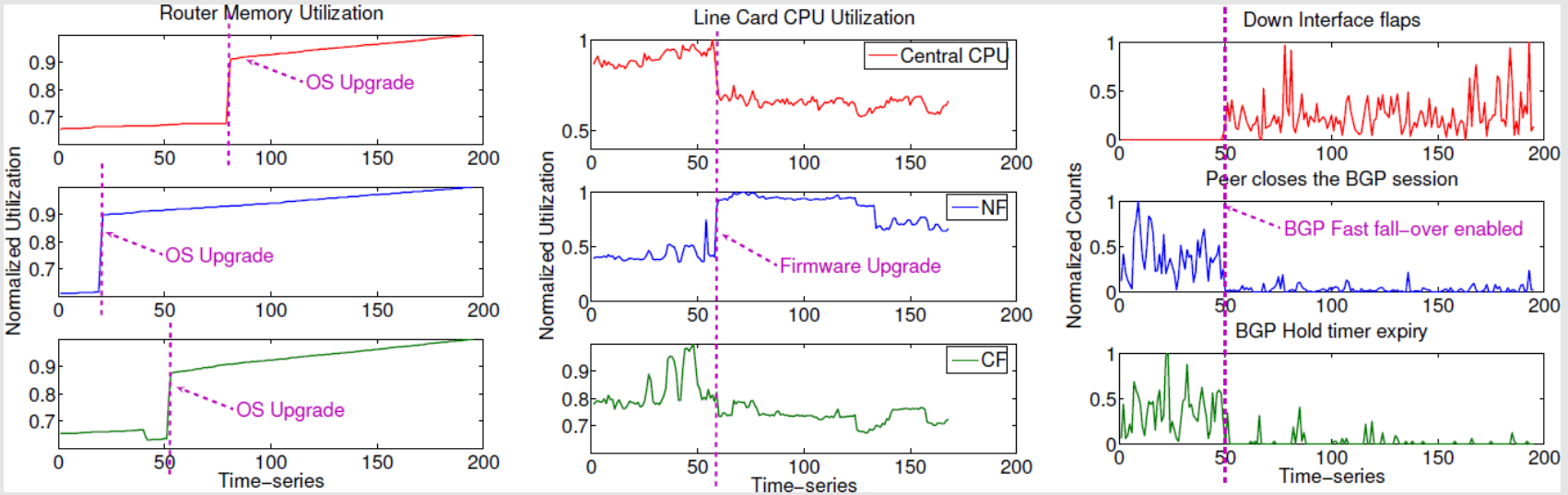
	Threshold	Output	False positives (FP)	FP rate
Config. sessions	2	2199	101	0.05
	4	6272	1095	0.17
	6	9562	2297	0.24
	8	12791	3873	0.30
	10	13581	4168	0.31
Triggers	2	120	4	0.03
	4	185	9	0.05
	6	212	17	0.08
	8	228	23	0.10
	10	236	27	0.11

Table 2: Number of configuration sessions and triggers output by MERCURY using the rareness metric and varying the rareness threshold from 2 to 10. The false positives are computed by comparing to customer provisioning sessions.

	Output	False positives (FP)	FP rate
Config. sessions	647	116	0.18
Triggers	92	24	0.26

Table 3: Number of configuration sessions and triggers output by MERCURY using the skewness metric. The false positives are computed by comparing to customer provisioning sessions.

Case studie 3 změn v síti - OS, firmware a konfigurace



Článek 3.

California Fault Lines: Understanding the Causes and Impact of Network Failures
Daniel Turner, Kirill Levchenko, Alex C. Snoeren, and Stefan Savage

Proč se zabývat selháními síťových komponent

- Nejméně prozkoumaný faktor ovlivňující end-to-end dostupnost

Výzvy

- Jak často nastávají selhání síťových komponent
- Jak dlouho trvají
- Jaké jsou jejich příčiny
- Jaký je jejich dopad
- Jak používat současné zdroje dat nízké kvality pro analýzu

Zdroje dat

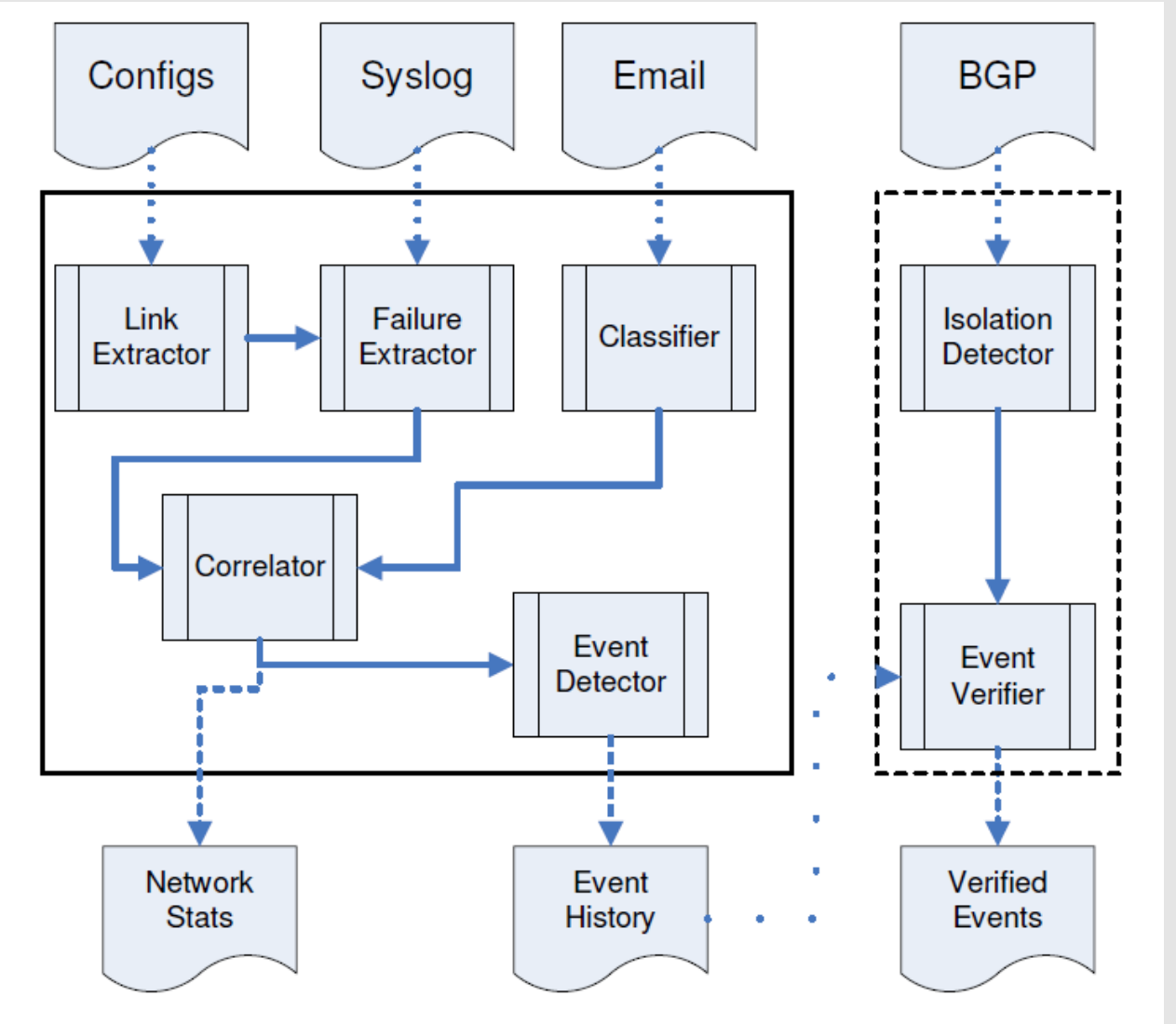
Zkoumaná síť

- CENIC network - Kalifornská vědecko výzkumná síť
- Získáno 5 let záznamů

Zdroje dat o síti

- Konfigurační data routerů
- Zprávy Syslogu
- BGP archiv
- Administrátorský mailing list

Workflow


Configs
Syslog
Email
BGP
Link Extractor
Failure Extractor
Classifier
Isolation Detector
Correlator
Event Detector
Event Verifier
Network Stats
Event History
Verified Events

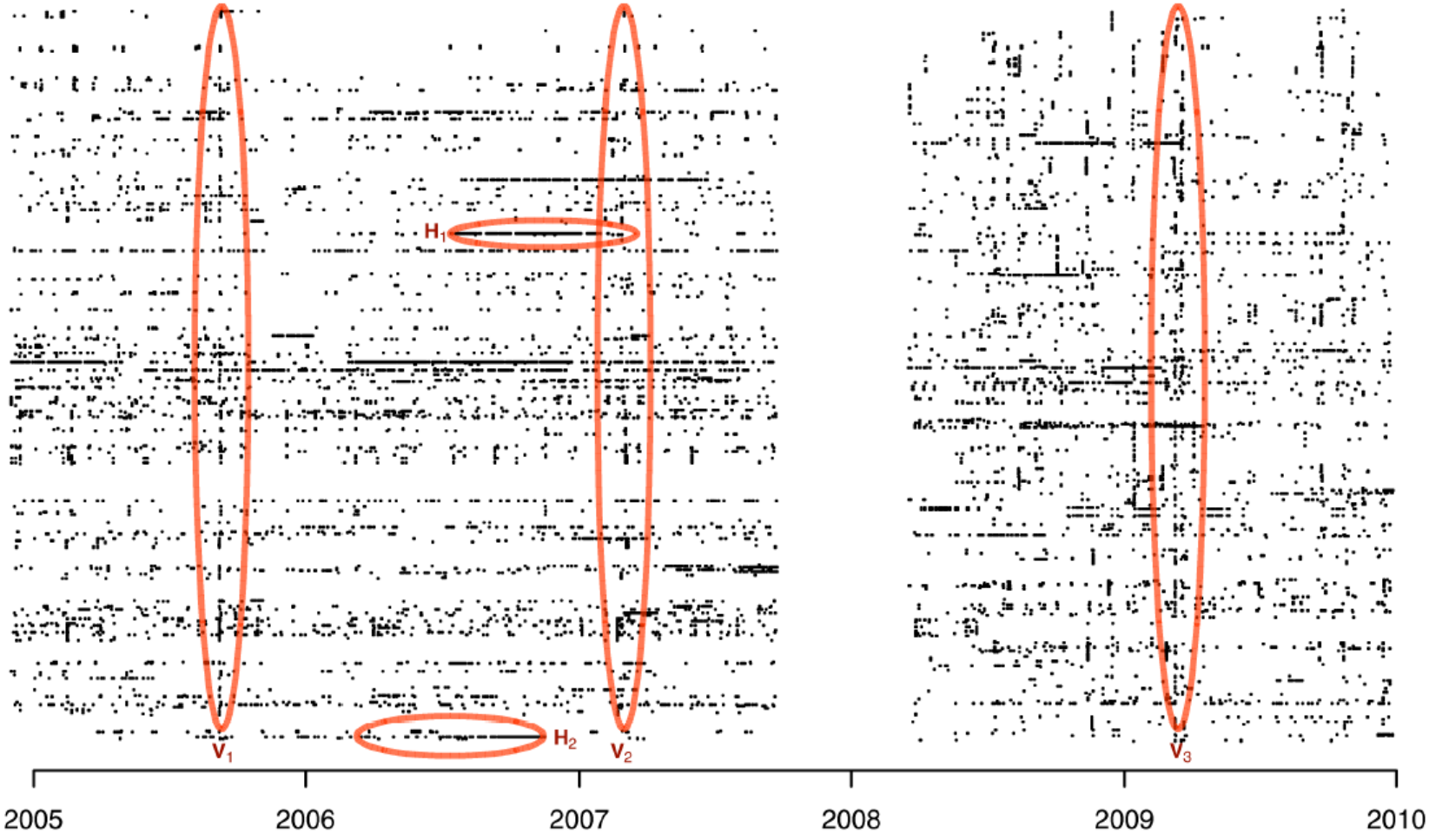
Metodologie

- Získání topologie
- Identifikace selhání
- Kategorizace selhání
- Validace

Kategorie selhání

Classification	Example causes or explanations
Power	"City-wide power failure", "UPS failure"
Hardware	"Replacing line card" , "Replacing optical amplifier"
External	Failure of non-CENIC equipment (e.g., leased fiber)
Software	"Upgrading IOS"
Configuration	"Modifying IGP metrics" , "adding IPv6 capability"
Other	"DoS attack" , "flooded machine room"
Unknown	Failures with unknown or unreported causes

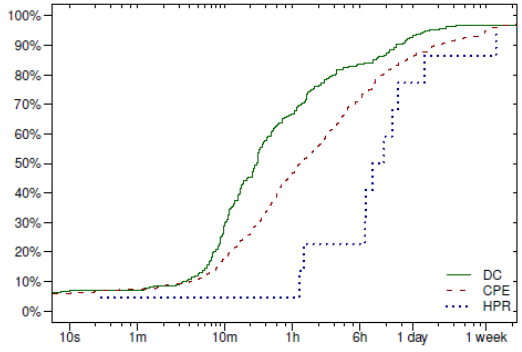
Rekonstruovaná historie selhání



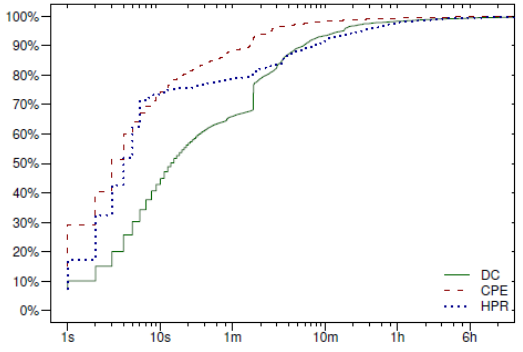
Počet selhání, downtime a čas opravy

	Annual failures			Annual downtime			Time to repair		
	Avg	Med	95%	Avg	Med	95%	Avg	Med	95%
DC	16.2	5.1	57.7	2.7 d	24 m	34 h	17.4 m	13.0 s	15.2 m
CPE	302.0	20.2	276.7	1.6 d	72 m	163 h	3.6 m	3.0 s	2.6 m
HPR	58.5	39.5	155.1	1.2 d	497 m	125 h	16.1 m	4.0 s	23.7 m
Internet2	12.9	14.3	29.1	0.2 d	112 m	19 h	20.7 m	54.0 s	75.5 m

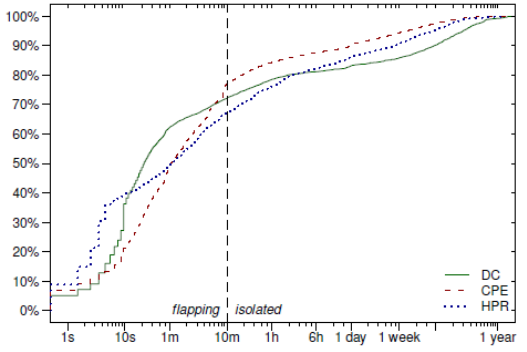
Downtime, čas opravy a doba mezi selháními podle sítě



(a) Annualized link downtime.

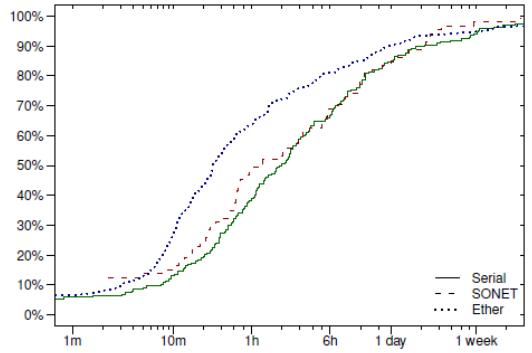


(b) Time to repair.

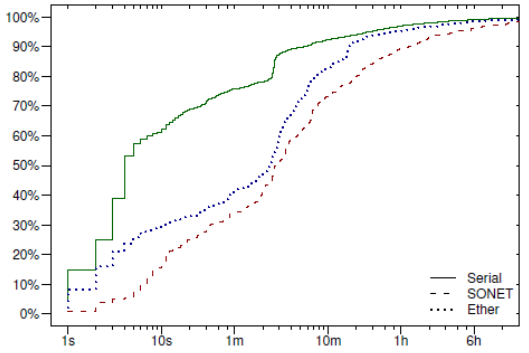


(c) Time between failures.

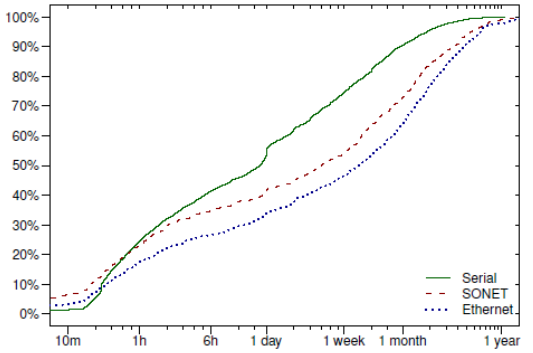
Downtime, čas opravy a doba mezi selháními podle HW typu spoje



(a) Annualized link downtime.

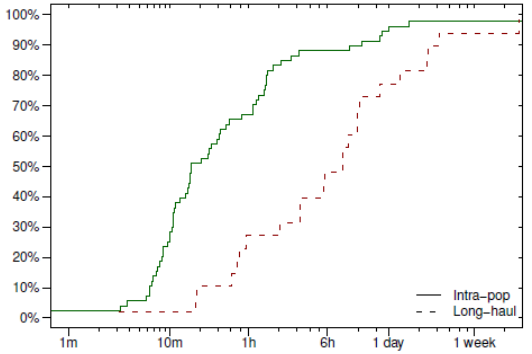


(b) Time to repair.

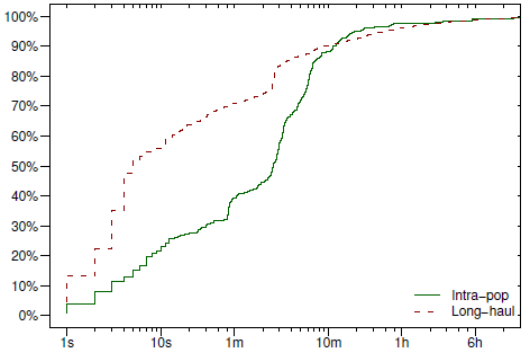


(c) Time between failures.

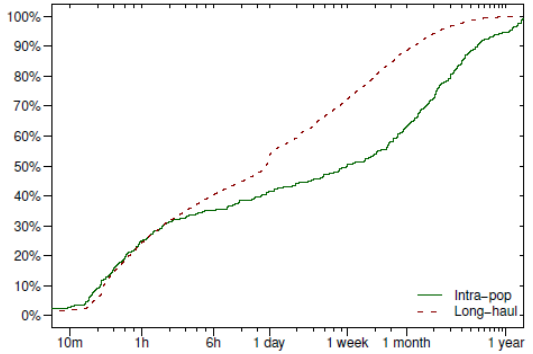
Downtime, čas opravy a doba mezi selháními podle třídy linky



(a) Annualized link downtime.

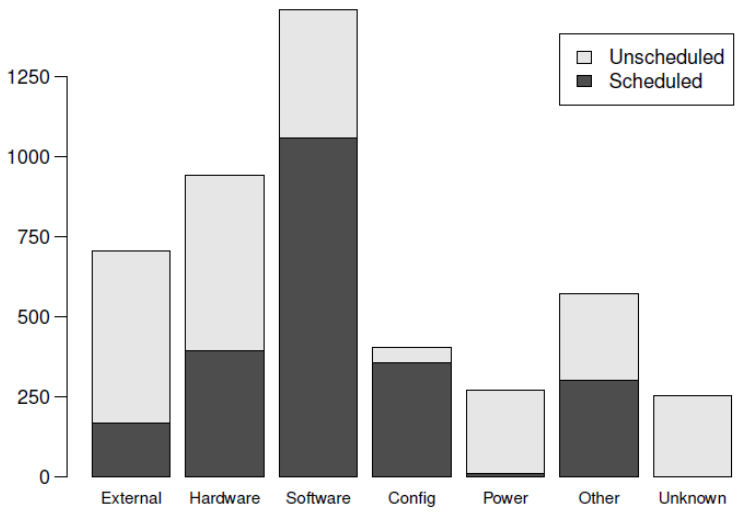


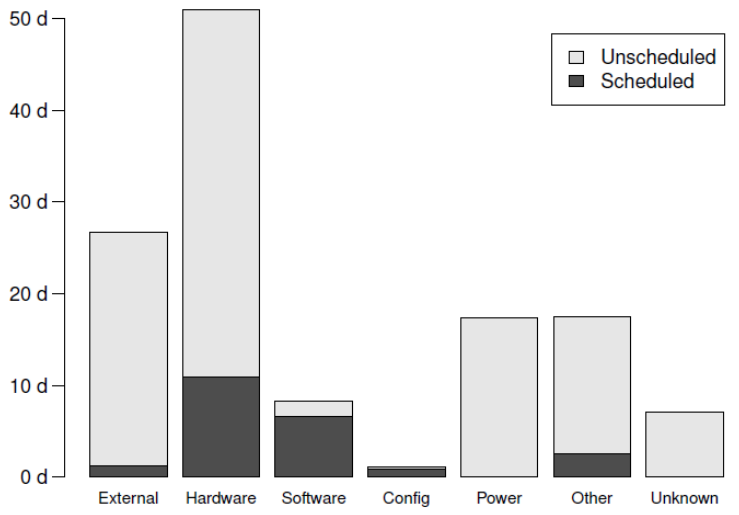
(b) Time to repair.



(c) Time between failures.

Celkový počet selhání a celková doba selhání



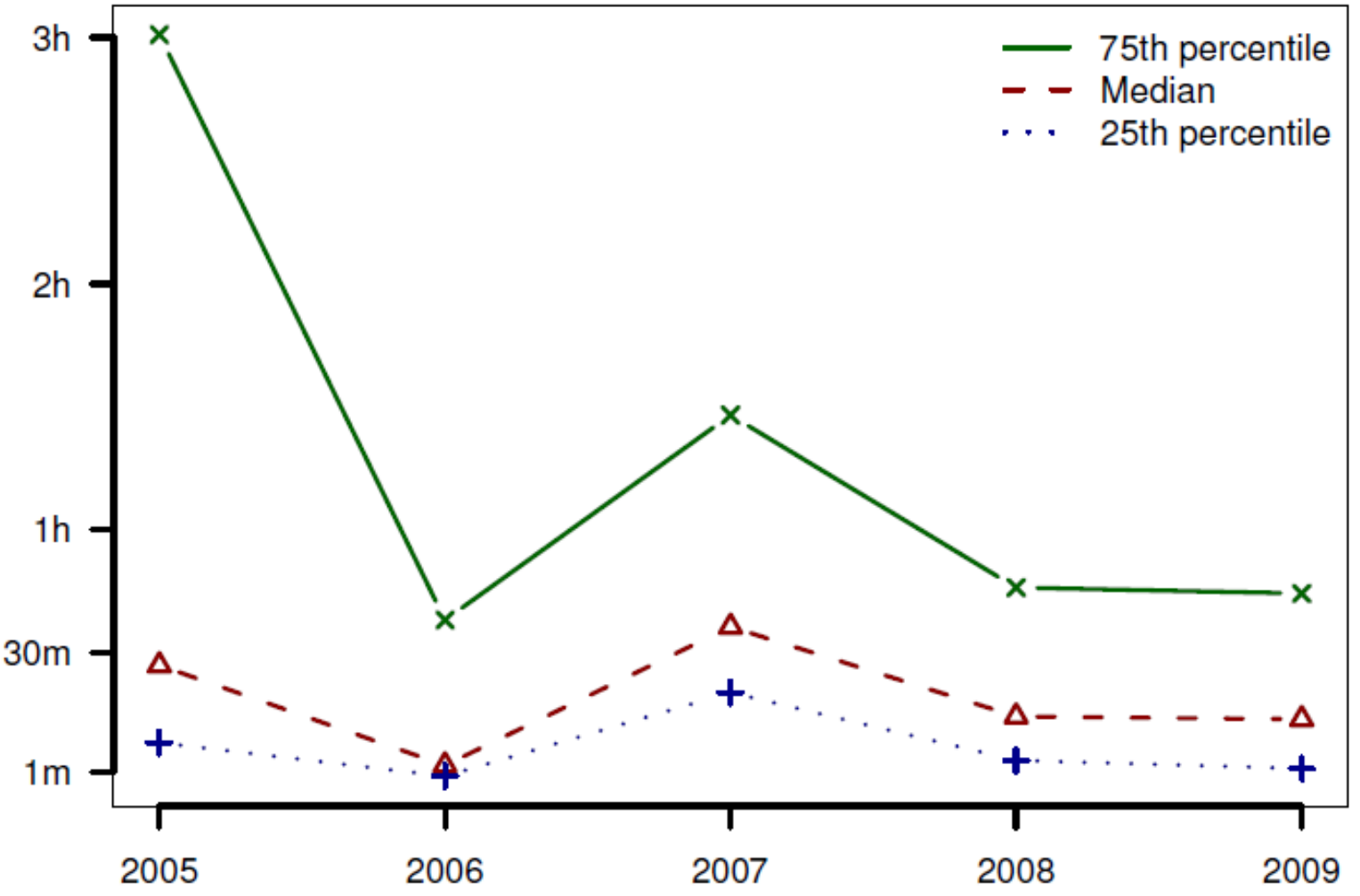


Příčiny selhání a jejich vážnost

Cause	Events	Time to repair	
		Avg	Med
Hardware	20%	95 m	5 m
Power	6%	93 m	18 m
External	15%	61 m	4.6 m
Software	32%	10 m	4 m
Configuration	9%	5 m	1 m
Other	12%	46 m	6 m
Unknown	5%	52 m	6 m

Cause	Notices	Scheduled	Impacting
Hardware	25%	65%	71%
Power	20%	4%	99%
External	15%	29%	95%
Software	12%	84%	99%
Other	12%	69%	82%
Configuration	8%	91%	45%
Unknown	7%	0%	99%

Down time linek podle jednotlivých roků



A nyní diskuze!