Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Nové metody výpočtu odolnosti

Luděk Lukáš
Ústav bezpečnostního inženýrství

Úvod

- zajistit bezpečnost znamená ochránit aktiva před škodícím účinkem hrozeb,
- hlavním ukazatelem schopnosti ochránit je odolnost,
- odolnost se zajišťuje jak preventivními, tak represivními opatřeními,
- v rámci krizového řízení se také pracuje s odolností, její vnímání je podobné jako v zajištění bezpečnosti, ale vztahuje se na celý objekt,
- možným přístupem k řešení je koncept konvergované bezpečnosti, realizující sloučení slučitelných druhů bezpečnosti v jeden celek.

Odolnost

Odolnost
je definovaná jako schopnost systému předvídat, odolávat, absorbovat, reagovat, přizpůsobit a zotavit se z narušení bezpečnosti.
Odolnost prvku kritické infrastruktury tedy vyjadřuje jeho připravenost a adaptabilitu na možné hrozby (rizika), které významně omezují nebo negují jeho funkčnost.

Odolnost
Schopnost/ vlastnost něčeho čelit hrozbám. Odolnost lze pojmout také jako schopnost systému nebo společnosti odolávat, zmírňovat, přijímat a obnovovat následky účinků nebezpečí včasným a účinným způsobem, včetně zachování a obnovy jeho nezbytné základní struktury a funkcí. (Výkladový slovník MV, 2016)

Odolnost

Odolnost
schopnost prvku KI zajistit svoji cílovou funkci v podmínkách působení vnějších a vnitřních činitelů.

Odolnost (resilience)
schopnost organizace, systému či sítě odolat hrozbám a čelit vlivu výpadků. (Výkladový slovník KB, 2016)

Odolnost představuje schopnost zamezit vzniku újmy (a v případě vzniku překonat její dopady).

Z pohledu bezpečnosti je vhodné odlišit:
• odolnost objektu
• odolnost systému ochrany

Odolnost

Odolnost objektu (prvku kritické infrastruktury)
kritériem je stav plnění cílové funkce

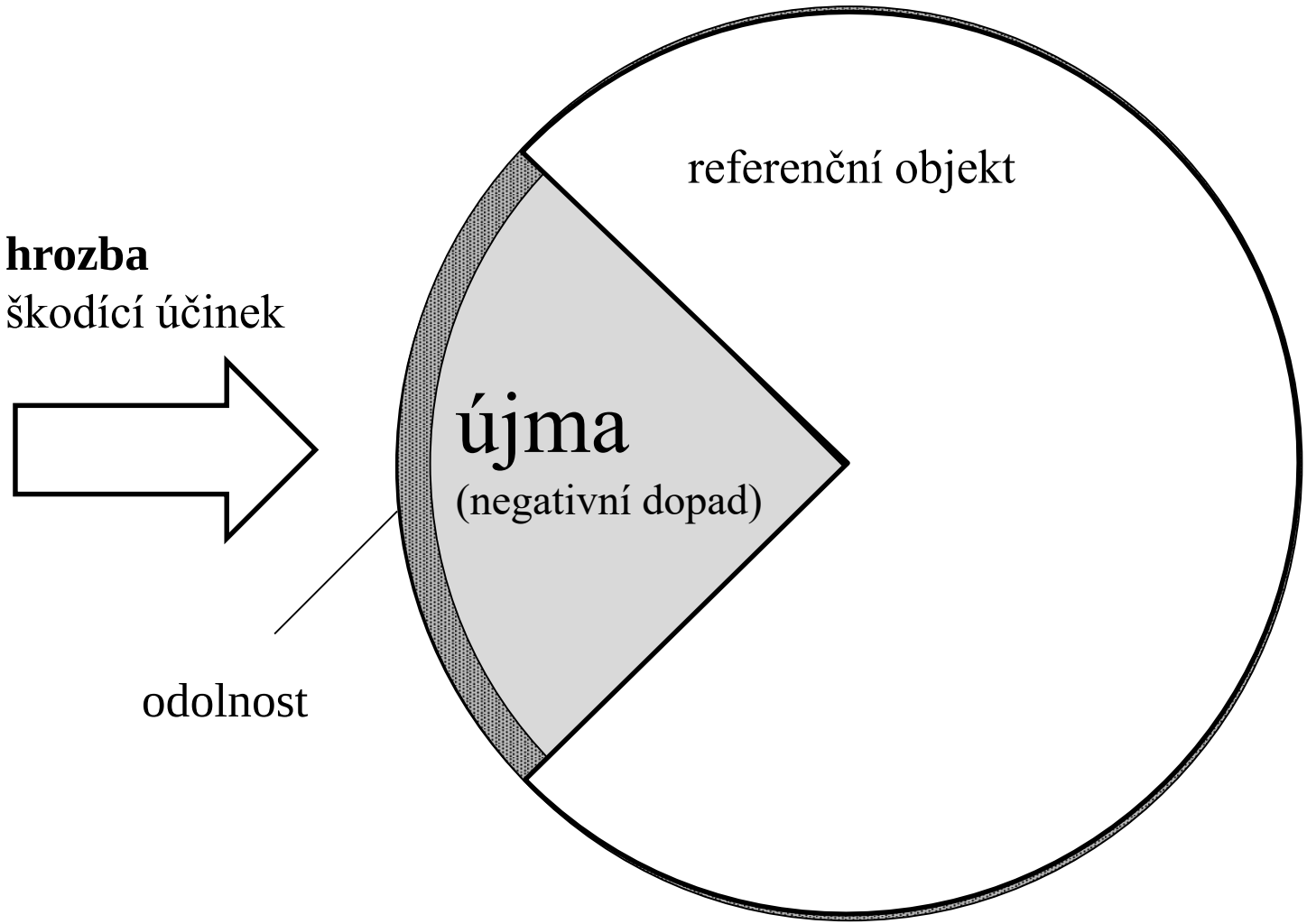
- vyjadřuje jeho schopnost zajistit funkci v podmínkách působení vnějších a vnitřních činitelů,
- vyjadřuje jeho připravenost a adaptabilitu na možné hrozby, které významně omezují nebo negují funkčnost objektu,
- odolnosti lze dosáhnout jednak souborem systémových opatření všech aktérů podílejících se na jeho správě a rovněž vnitřními schopnostmi nebo vlastnostmi prvku přirozeně odolávat vnějším a vnitřním vlivům prostředí,
- součástí zajištění odolnosti objektu je jeho systém ochrany.

Odolnost

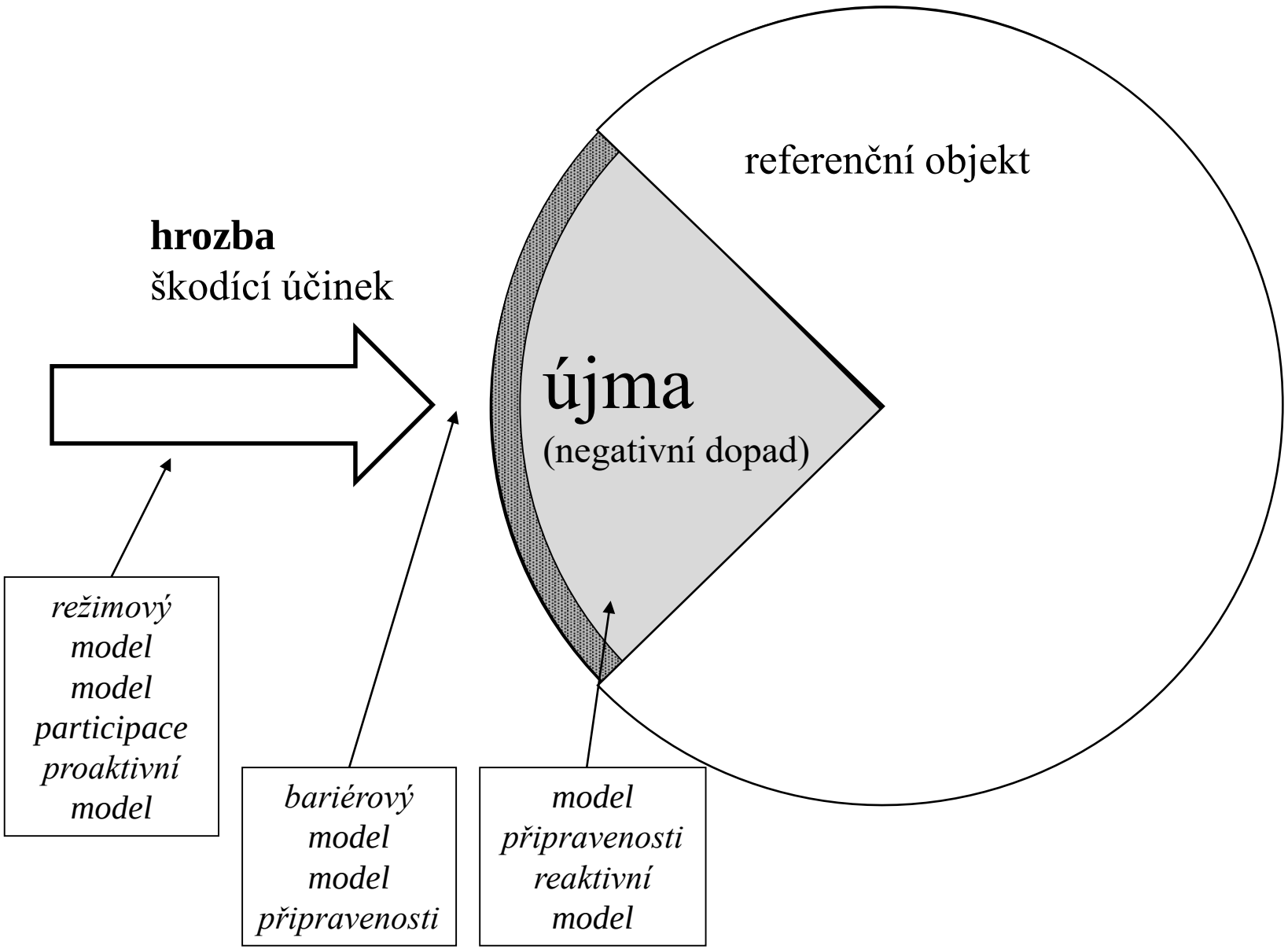
Odolnost systému ochrany
kriteriem je stav ochrany aktiv

- vyjadřuje schopnost referenčního objektu chránit aktiva a zvládat narušení bezpečnosti,
- vyjadřuje, jak je referenční objekt schopen vzdorovat působení škodícího účinku a jak ochraňuje svoje aktiva,
- co vše a s jakou intenzitou musí škodící účinek překonat, aby mohl referenčnímu objektu způsobit újmu na aktivech; případně s jakou pravděpodobností za daných podmínek dojde k újmě na aktivech (narušení bezpečnosti).

Odolnost


referenční objekt
hrozba
škodící účinek
újma
(negativní dopad)
odolnost

Odolnost


referenční objekt
hrozba
škodící účinek
újma
(negativní dopad)
režimový model
model participace
proaktivní model
bariérový model
model připravenosti
model připravenosti
reaktivní model

Odolnost

Ukazatele odolnosti

Robustnost - schopnost vydržet a přestát účinky negativního působení bez významné degradace funkce (funkčnosti).

Připravenost - představuje jeho schopnost odolávat očekávaným narušením bezpečnosti / krizovým situacím, plánovat a mít reálně připravena opatření, síly a prostředky k jejímu překonání a zajištění obnovy funkce,

Reakceschopnost (doba odezvy) - představuje schopnost aktivace sil a prostředků k obnově funkce objektu (prvku kritické infrastruktury).

Obnovitelnost (doba obnovy) - představuje jeho schopnost obnovit funkci po narušení bezpečnosti / mimořádné události na původní (požadovanou) úroveň.

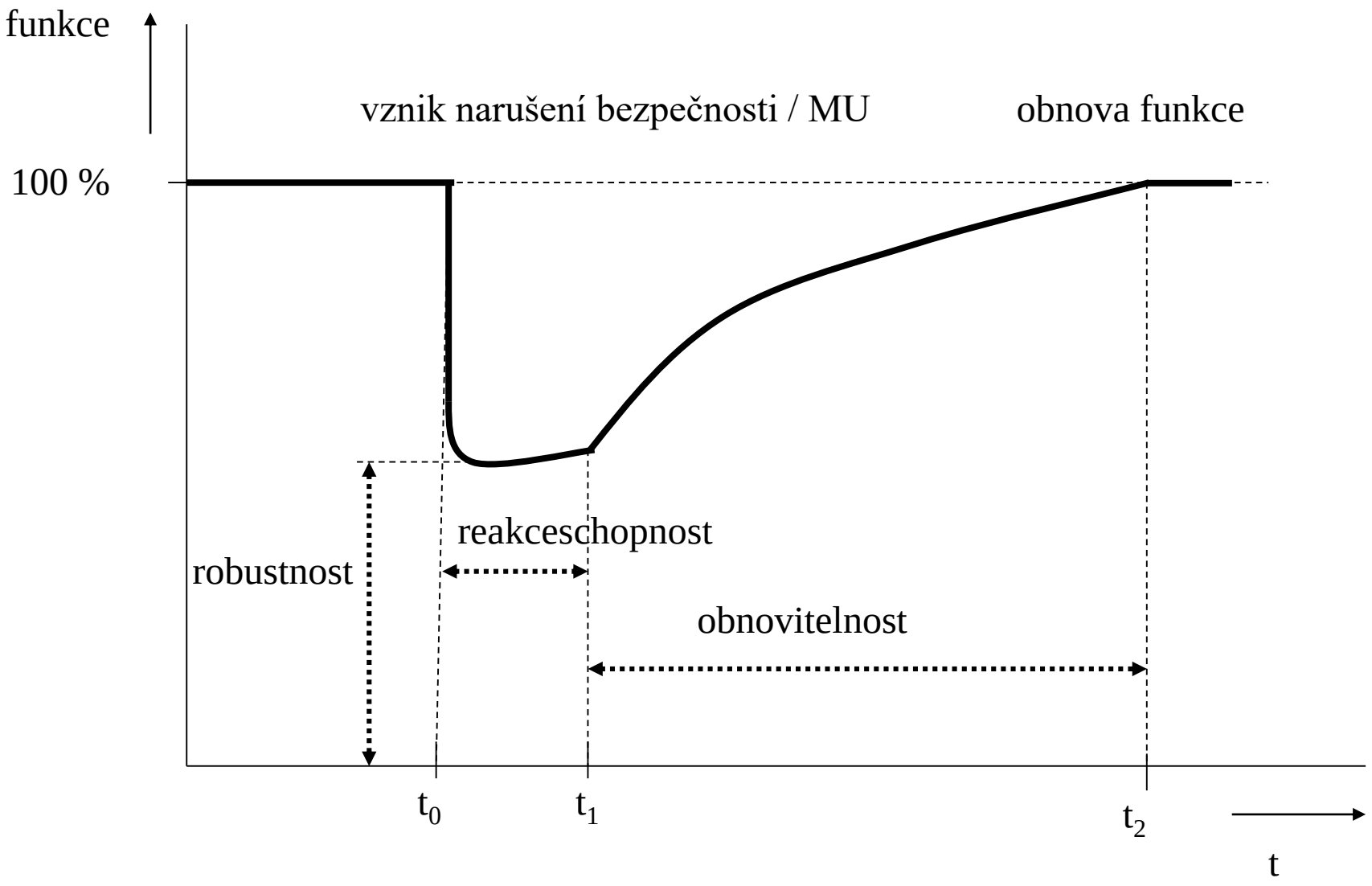
Odolnost

Robustnost objektu (prvku kritické infrastruktury)
- přestavuje pevnost, stálost, odolnost vůči deformaci,
- je to schopnost vydržet a přestát účinky negativního působení bez významné degradace funkce (funkčnosti),
- robustnost je členěna na strukturální robustnost a robustnost zabezpečení.

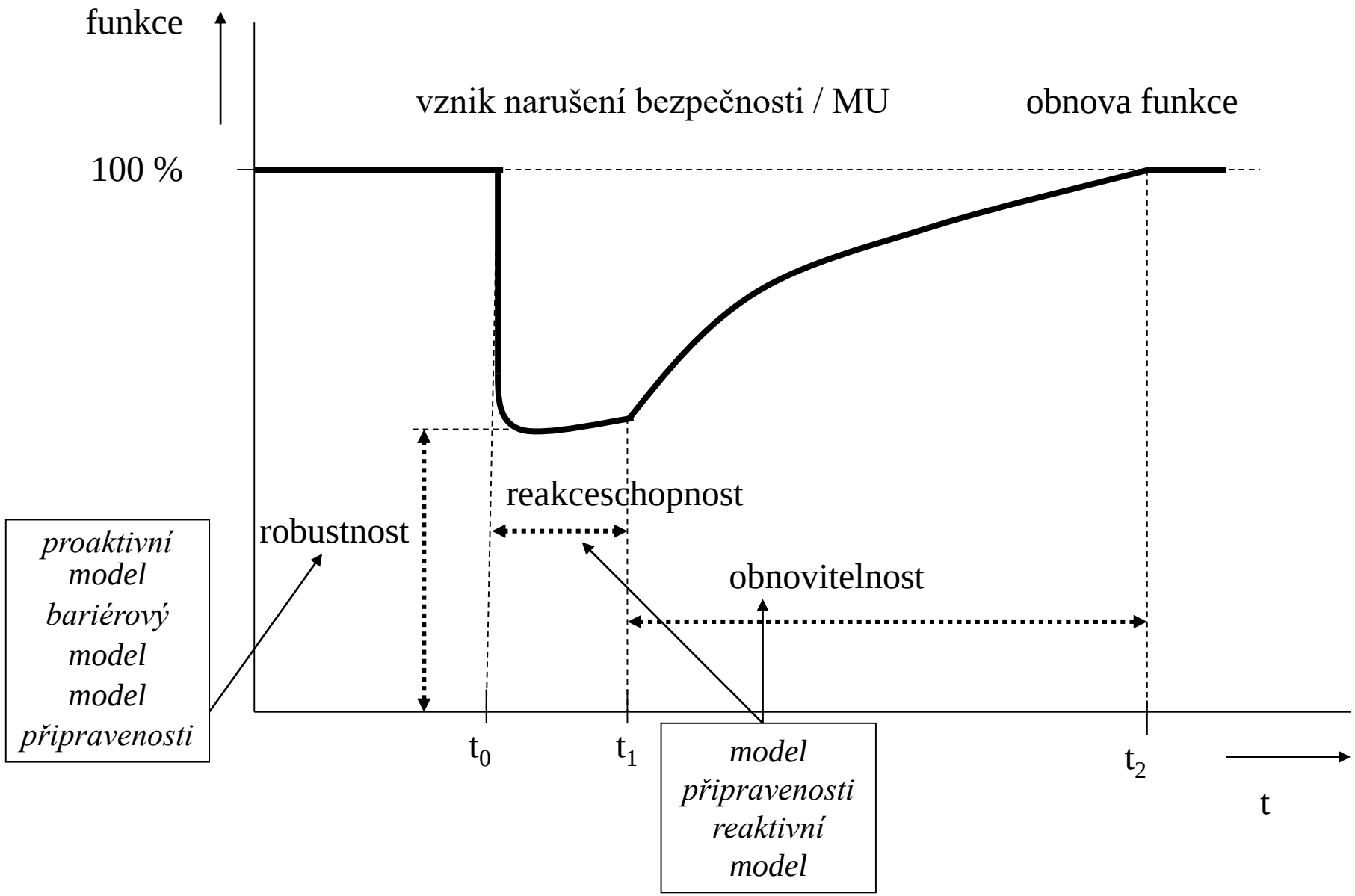
Strukturální robustnost objektu (prvku kritické infrastruktury)
- schopnost plynoucí z konstrukce prvku, jeho systémového uspořádání, technologií, systému řízení, personálu (způsob naplnění cílové funkce).

Robustnost zabezpečení objektu (prvku kritické infrastruktury)
- schopnost vydržet účinky negativního působení pomocí bezpečnostních opatření (opatření zabezpečení), fyzické bezpečnosti, informační bezpečnosti, personální bezpečnosti atd.

Odolnost


funkce
vznik narušení bezpečnosti / MU
obnova funkce
100 %
robustnost
reakceschopnost
obnovitelnost
t_0
t_1
t_2
t

Odolnost


funkce
vznik narušení bezpečnosti / MU
obnova funkce
100 %
robustnost
reakceschopnost
obnovitelnost
proaktivní model
bariérový model
model připravenosti
model připravenosti reaktivní model
t0
t1
t2
t

Statické hodnocení odolnosti

Odolnost prvku KI

- schopnost zajistit své fungování v podmínkách působení vnějších a vnitřních činitelů,
- schopnost překonat účinek negativního působení a zajistit kontinuálně činnost prvku kritické infrastruktury.

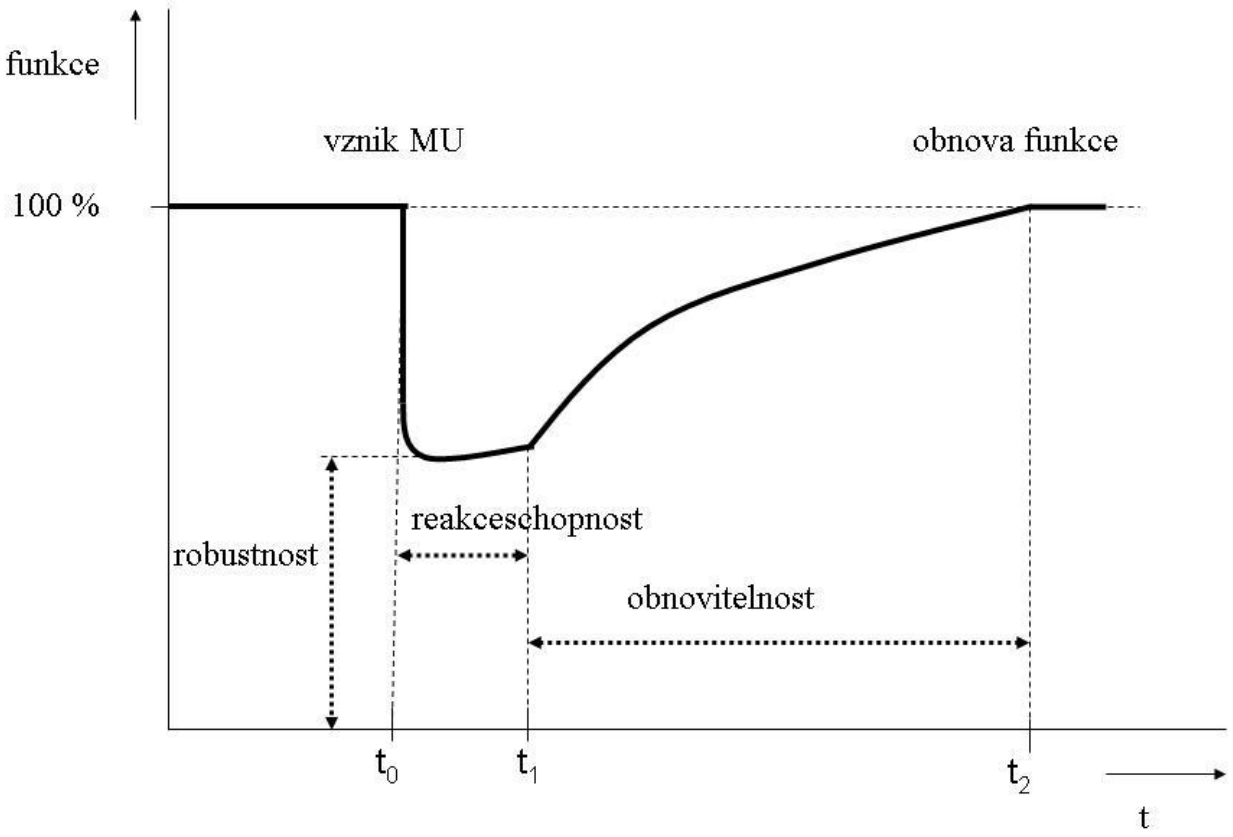
Odolnosti prvku KI se dosahuje:

- schopností vydržet účinky negativního působení,
- flexibilitou činnosti,
- absorpcí účinku negativního působení,
- adaptací na novou situaci,
- zapojením redundantních prvků,
- obnovou funkce atd.

Statické hodnocení odolnosti

Mezi základní ukazatele odolnosti prvku KI patří:

- robustnost,
- připravenost,
- reakceschopnost,
- obnovitelnost.



Statické hodnocení odolnosti

Hodnocení odolnosti prvku KI zaměřit na hodnocení:

- robustnosti,
- připravenosti.

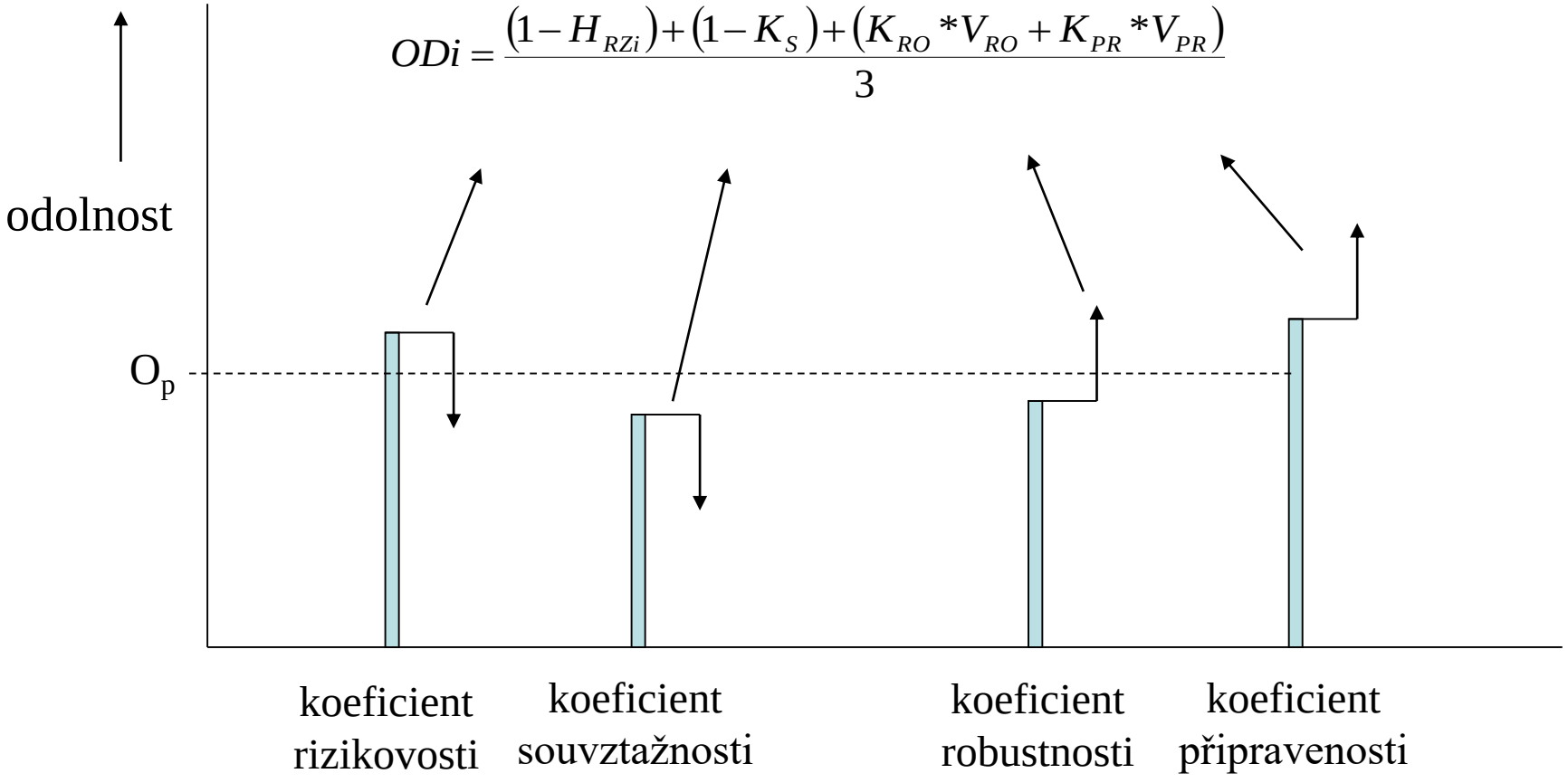
Základní interpretace hodnocení odolnosti:

Prvek KI je schopen zajistit cílovou funkci a odolat identifikovaným rizikům (A) výborně, (B) velmi dobře, (C) dobře, (D) dostatečně nebo (E) není schopen odolat.

Statické hodnocení odolnosti

Podstata hodnocení odolnosti prostřednictvím koeficientů

$$ODi = \frac{(1 - H_{RZi}) + (1 - K_S) + (K_{RO} * V_{RO} + K_{PR} * V_{PR})}{3}$$



Statické hodnocení odolnosti

Prvek KI je schopen zajistit cílovou funkci a odolat identifikovaným rizikům (A) výborně, (B) velmi dobře, (C) dobře, (D) dostatečně nebo (E) není schopen odolat.

hodnocení	Hodnota	slovní hodnocení	Minimální hodnota robustnosti	Minimální hodnota robustnosti zabezpečení	Minimální hodnota připravenosti
výborně (A)	0,8– 1	na všechna identifikovaná rizika je připraven, žádné z rizik není zanedbáno ve fungování nedochází k poruchám, kvalita a rozsah opatření přesahují možné dopady a důsledky újmy	0,5 jako výsledek vztahu $K_{RO} * V_{RO}$	Je vána váhami jednotlivých parametrů $V_{FB}; V_{IB}; V_{AB}; V_{PB}$	0,5 jako výsledek vztahu $K_{PR} * V_{PR}$
velmi dobře (B)	0,6 – 0,8	na všechna důležitá identifikovaná rizika je připraven, za určitých podmínek a ojediněle není obnova zajištěna v normě,	0,4 jako výsledek vztahu $K_{RO} * V_{RO}$	Je vána váhami jednotlivých parametrů $V_{FB}; V_{IB}; V_{AB}; V_{PB}$	0,4 jako výsledek vztahu $K_{PR} * V_{PR}$
dobře (C)	0,4 – 0,6	na většinu důležitých identifikovaných rizik je připraven, obnova funkce je zajištěna ve většině případů zajištěna v normě	0,3 jako výsledek vztahu $K_{RO} * V_{RO}$	Je vána váhami jednotlivých parametrů $V_{FB}; V_{IB}; V_{AB}; V_{PB}$	0,3 jako výsledek vztahu $K_{PR} * V_{PR}$
dostatečně (D)	0,2 – 0,4	na většinu identifikovaných rizik je připraven, je schopen obnovy funkce ale ve většině případů doba obnovy přesáhne standard	0,3 jako výsledek vztahu $K_{RO} * V_{RO}$	Je vána váhami jednotlivých parametrů $V_{FB}; V_{IB}; V_{AB}; V_{PB}$	0,3 jako výsledek vztahu $K_{PR} * V_{PR}$
není schopen odolat (E)	0 – 0,2	na většinu (více jak 1/2) identifikovaných rizik není připraven, nemá systém pro zajištění obnovy funkce	0,2 jako výsledek vztahu $K_{RO} * V_{RO}$	Je vána váhami jednotlivých parametrů $V_{FB}; V_{IB}; V_{AB}; V_{PB}$	0,2 jako výsledek vztahu $K_{PR} * V_{PR}$

Konvergovaná bezpečnost – dynamické hodnocení odolnosti

Základní východiska a principy:

- konvergovaná bezpečnost se zajišťuje pro určitý (společný) referenční objekt,
- do konvergované bezpečnosti lze zahrnout pouze slučitelné druhy bezpečnosti,
- je žádoucí, aby zahrnuté druhy bezpečnosti chránily shodná nebo alespoň částečně shodná aktiva,
- dopady působení hrozeb nesmí být protichůdné a projevují se na aktivech referenčního objektu negativně,
- všechny hrozby můžou mít pro referenční objekt existenciální dopady.

Konvergovaná bezpečnost umožňuje sloučit provozní bezpečnost, fyzickou bezpečnost a kybernetickou bezpečnost v jeden celek.

Konvergovaná bezpečnost

Dynamické hodnocení odolnosti

Základní principy, na nichž je postaveno hodnocení odolnosti z pohledu konvergované bezpečnosti:

- odolnost z pohledu konvergované bezpečnosti závisí na ochranných vlastnostech systému ochrany referenčního objektu a současně na intenzitě působení škodícího účinku (zdroj hrozby),
- změny odolnosti i působení škodícího účinku mají statický nebo dynamický charakter,
- změny odolnosti závisí na vnějších a vnitřních faktorech, tzv. penalizačních faktorech,

Dynamické hodnocení odolnosti

Základní principy, na nichž je postaveno hodnocení odolnosti z pohledu konvergované bezpečnosti (pokračování):

- odolnost lze hodnotit semikvantitativně společným ekvivalentem, který se nazývá **penalizace**,
- penalizace představuje číslo přidělené penalizačnímu faktoru, v jehož velikosti se odráží **míra závažnosti** vlivu působení škodícího účinku na referenční objekt a jeho aktiva,
- penalizace se určuje pro jednotlivé druhy bezpečnosti,
- penalizace bývá stanovena pro jednotlivá aktiva nebo centrálně na celý referenční objekt,
- vliv jednotlivých penalizací na jednom aktivu (vyvolaný stejnou událostí) se nesmí překrývat,
- velikost odolnosti by měla být vyjádřena v určitém rozmezí hodnot (např. 100 – 0), případně omezená alespoň z jedné strany maximální hodnotou (100).

Dynamické hodnocení odolnosti

Statické faktory (determinující faktory)

- jsou takové vlivy, které jsou spojeny se systém ochrany, působí do okamžiku, kdy jsou odstraněny,
- jedná se ale o dlouhodobé působení, samy se neopraví/neobjeví,
- příkladem existence/neexistence bezpečnostní politiky, poplachového zabezpečovacího systému, systému kontroly vstupu, pravidel tvorby a obměny hesel atd.

Dynamické faktory (dynamizující faktory)

- se samy v čase mění (vznikají/zanikají), doba jejich působení není přesně odhadnutelná,
- příkladem detekce pohybu pomocí kamerového systému, narušení bezpečnosti hlášené detektorem narušení, detekce aktivity mallwaru na síti, porucha zabezpečovacího systému, výpadek elektrické energie apod.

Dynamické hodnocení odolnosti

Katalog penalizačních faktorů

penalizační faktor	výchozí penalizace		
	FB	KB	PB
není stanoven režim pohybu materiálu v objektu - **STAT**	8	4	1
na plášti budovy není naplněna funkce detekce - **STAT**	2	1	1
narušení vnitřního prostoru objektu (DV) - **DYN**	4	4	2
poplach - EPS – **DYN**	8	8	4
nedostupnost lidských zdrojů – nemoc - **DYN**	2	2	4

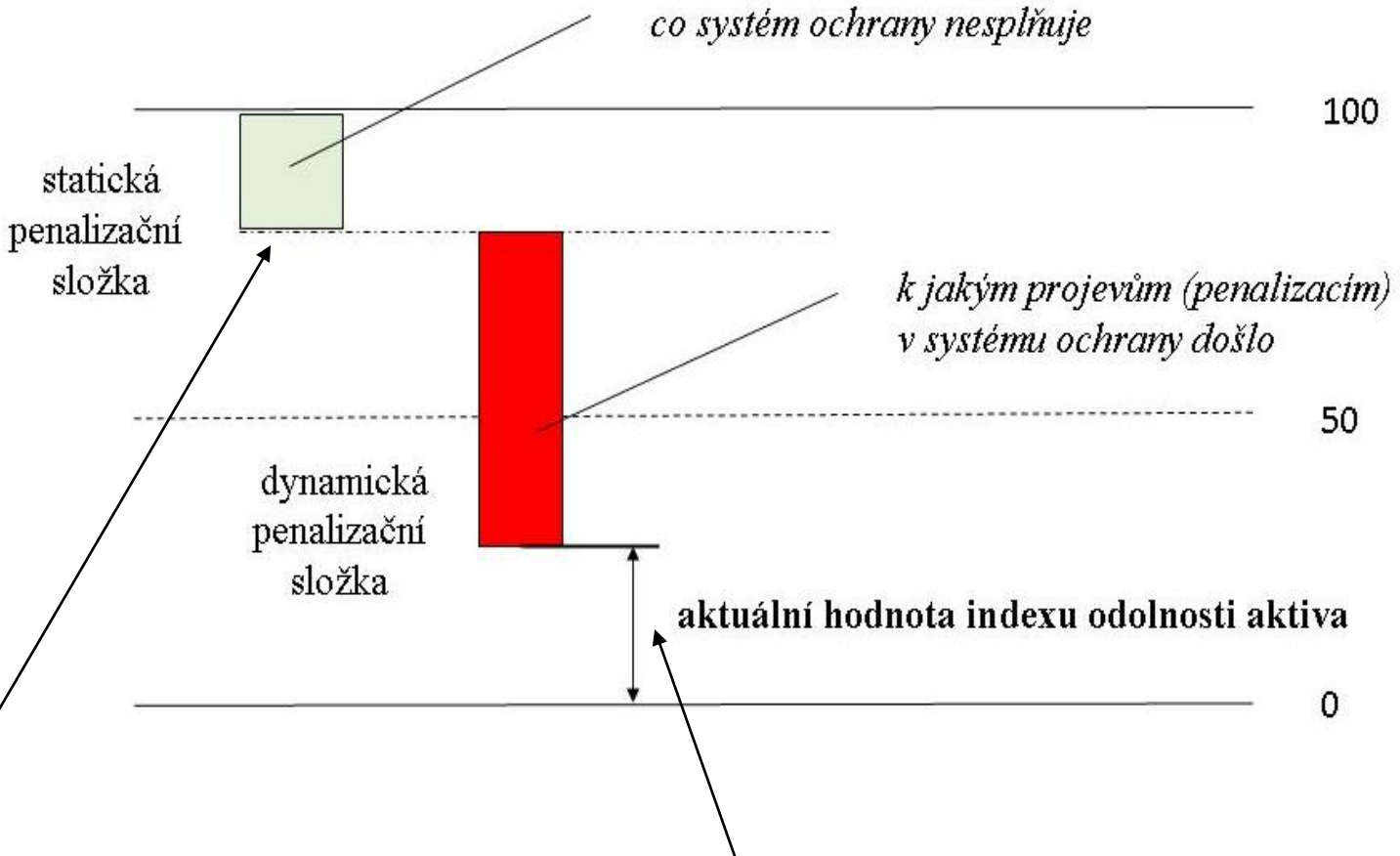
Dynamické hodnocení odolnosti

Index odolnosti referenčního objektu I_{ro}

- vyjadřuje, do jaké míry jsou v daném časovém okamžiku ochraňována aktiva referenčního objektu vůči hrozbám v daném druhu bezpečnosti,
- je bezrozměrným číslem, jehož hodnota se pohybuje v intervalu od 100 do 0,
- hodnota 100 vyjadřuje maximální odolnost, hodnota 0 pak nulovou odolnost
- počítá se pro jednotlivá aktiva referenčního objektu,
- začíná se výpočtem indexu statické odolnosti aktiva I_{ods} (vyjadřuje výchozí stav odolnosti systému ochrany),
- od něj se odečítají dynamické penalizace (v nich se odráží působení škodícího účinku a vlivy prostředí na odolnost),
- index odolnosti referenčního objektu I_{ro} vypočítá agregací indexů odolnosti aktiv s využitím váhování.

Dynamické hodnocení odolnosti

Podstata výpočtu indexu odolnosti aktiva I_{oda} pro daný druh bezpečnosti

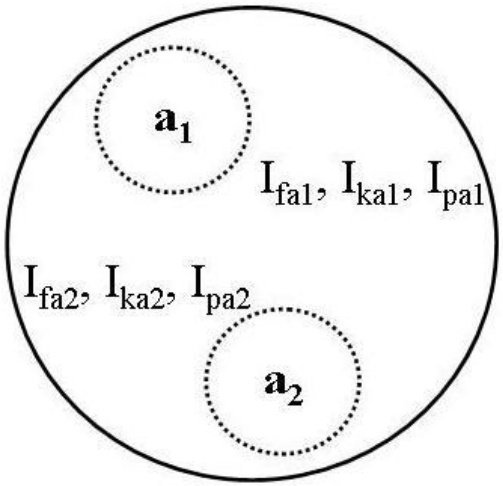


$$I_{ods} = 100 - \frac{\sum_{i=1}^{n} P_{si} * V_i}{P_{smax}} * 100$$

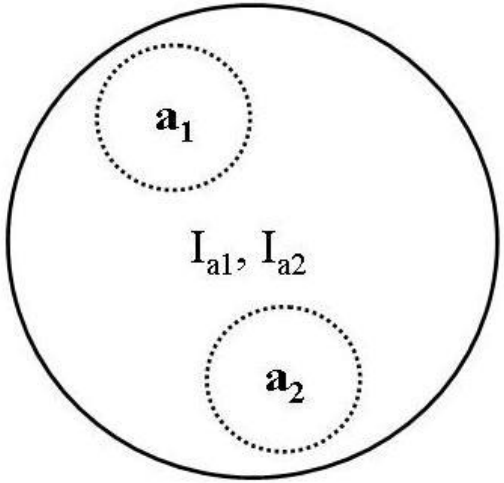
$$I_{f,k,p\,ai} = I_{ods} - \frac{\Sigma_{j=1}^{m} P_{dj} * V_j}{P_{dmax}} * I_{ods}$$

Dynamické hodnocení odolnosti

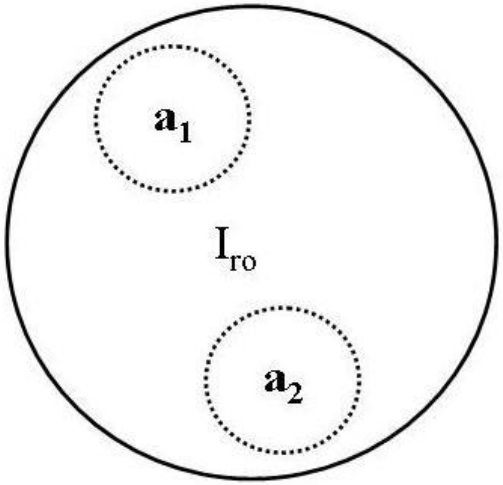
1. indexy odolnosti aktiv I_{fai}, I_{kai}, I_{pai} pro druh bezpečnosti



2. indexy odolnosti I_{a1}, I_{a2}, pro jednotlivá aktiva



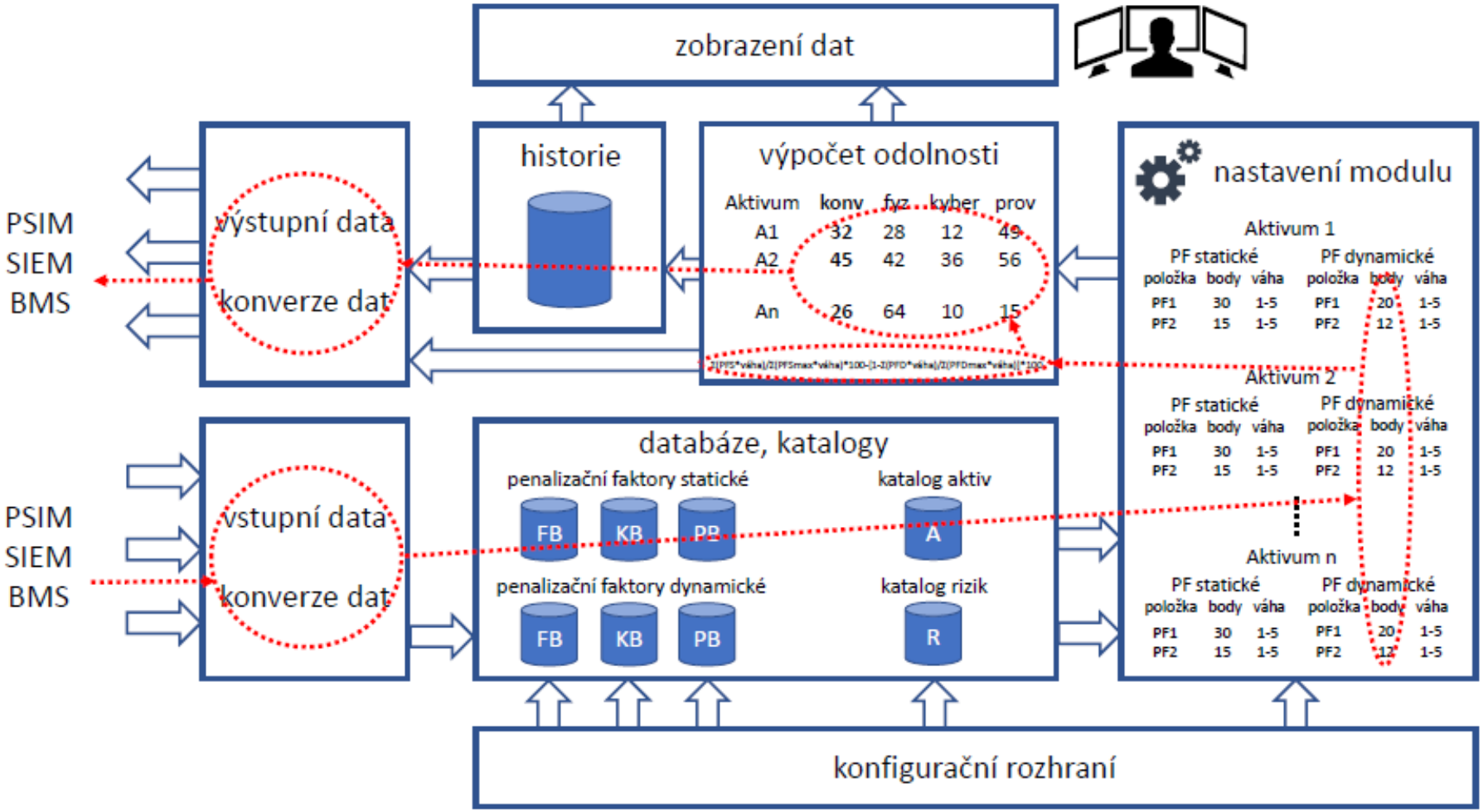
3. index odolnosti I_{ro} pro celý referenční objekt



$$I_{f,k,p\,ai} = I_{ods} - \frac{\Sigma_{j=1}^{m} P_{dj} * V_j}{P_{dmax}} * I_{ods} \quad \Rightarrow \quad I_{ai} = \frac{I_{fai} + I_{kai} + I_{pai}}{u} \quad \Rightarrow \quad I_{ro} = \frac{\Sigma_{i=1}^{u} I_{ai}}{u}$$

Dynamické hodnocení odolnosti

Funkční bloky modulu OSM – on-line změny



Příklad dynamického hodnocení odolnosti

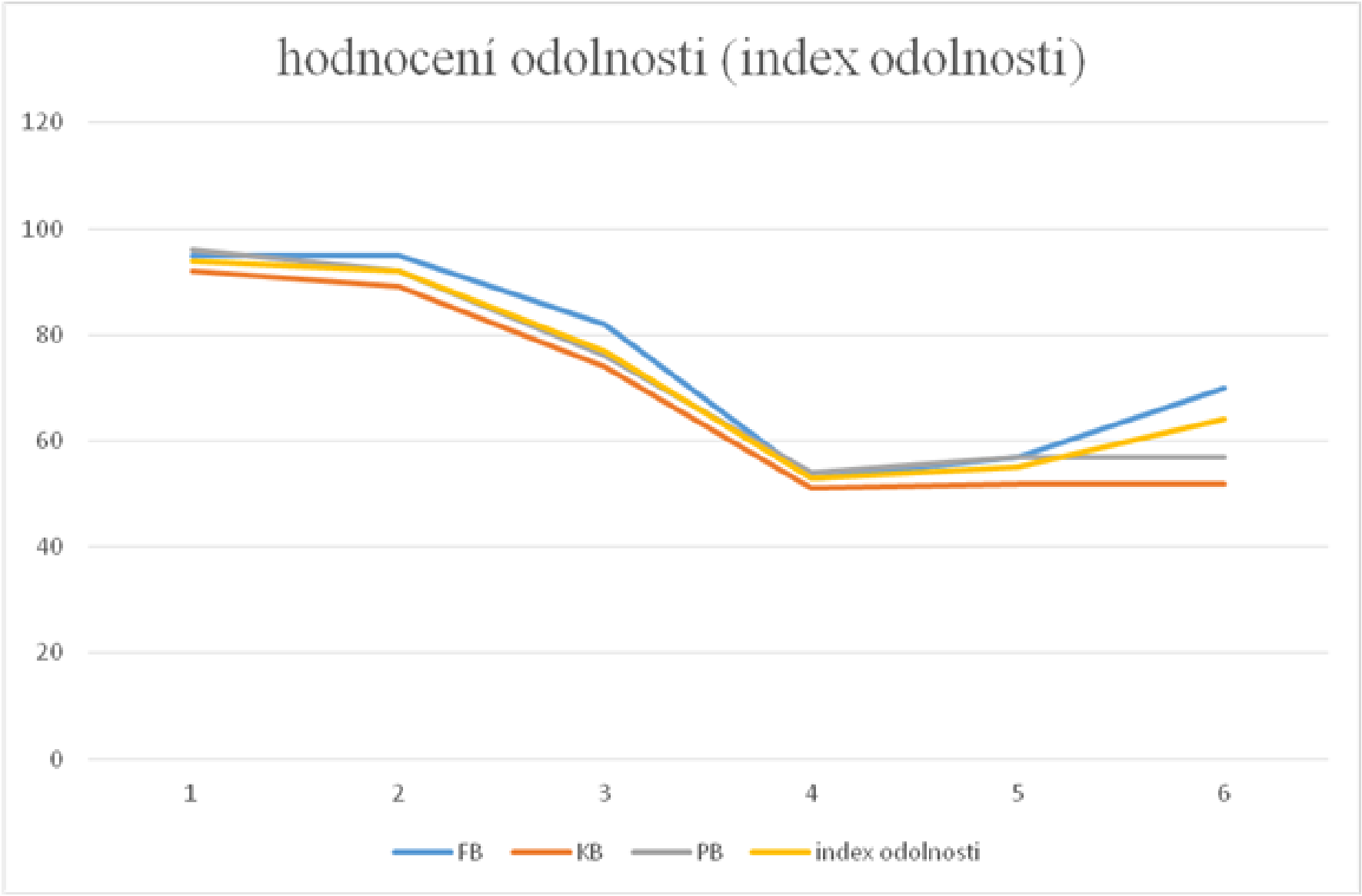
Charakteristika narušení bezpečnosti:
Dne 10. dubna 2018 v 21:00 hod. došlo ke vzniku požáru v technologických místnostech hlavního stavědla železniční stanice Břeclav. Oheň byl vlivem technologické poruchy. Nejprve došlo k požáru v místnosti s rozvaděči slaboproudých rozvodů, posléze se požár rozšířil i do dalších technologických místností. Zaměstnanci SŽDC se svými silami pokusili požár uhasit, avšak prudký rozvoj požáru si vynutil povolání jednotek požární ochrany. Požár byl uhašen po dvou hodinách. Vlivem požáru byla přerušena činnost železniční zabezpečovací signalizace, řídicích, informačních a komunikačních systémů. To způsobilo úplné vyřazení železniční stanice Břeclav z provozu, včetně signalizace na železničních přejezdech v nejbližším okolí. Nouzové obnovení provozu se předpokládá do dvou týdnů, úplné odstranění do půl roku. Vlivem požáru vznikla škoda na technologiích ve výši 100 mil. Kč, přerušením omezením provozu ve výši 50 mil. Kč

Příklad dynamického hodnocení odolnosti

Výsledné hodnocení odolnosti po fázích (technologie)

fáze	index odolnosti aktiva I_{fa} (odolnost FB)	index odolnosti aktiva I_{ka} (odolnost KB)	index odolnosti aktiva I_{pa} (odolnost PB)	index odolnosti I_{ro}
výchozí statická složka	96	93	96	95
výchozí	94.25	91.36	94.79	93.46
1. technologická porucha	94.65	87.90	91.07	90.01
2. vznik požáru	81.75	74.35	75.44	77.18
3. rozvoj požáru	54.14	52.95	54.47	53.85
4. plně rozvinutý požár	57.74	53.75	58.48	56.65
5. dohořívání požáru	70.46	56.66	58.03	61.71

Příklad dynamického hodnocení odolnosti



Závěr

- statické hodnocení odolnosti umožňuje hodnotit připravenost na narušení bezpečnosti,
- online hodnocení umožňuje průběžně vyhodnocovat stav odolnosti systému ochrany,
- hodnocení odolnosti je založeno na sumarizaci aktivních statických a dynamických penalizačních faktorech,
- v současnosti je nejobtížnější stanovit hodnotu penalizace pro jednotlivé penalizační faktory.

Poděkování

Tento příspěvek vznikl za podpory grantového projektu VI20172019054 "Analytický programový modul pro hodnocení odolnosti v reálném čase z hlediska konvergované bezpečnosti ", podpořeného Ministerstvem vnitra České republiky v letech 2017-2019.