Progresivní technologie v informatice II

IoT

inteligentní domácnost, způsoby komunikace, výhody, rizika

Fakulta informačních technologií
České vysoké učení technické v Praze

Financováno Evropskou unií
NextGenerationEU
Národní plán obnovy
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

- Kdy a jak efektivně **přenášet** logicky i časově správná data v IoT
- Determinismus
- Jak zabezpečit
- Protokoly
- Bezpečnost

Zdroje:

Kapitola 10 z Kopetz, H.: Real-Time Systems. Springer, ISBN 978-1-4419-8236-0

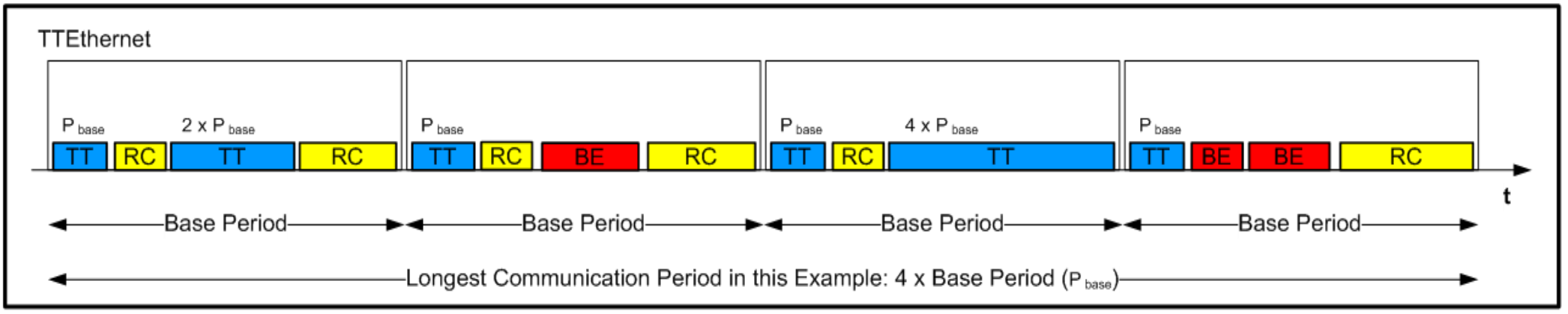
Přednášky ZCU: http://www.kky.zcu.cz/cs/courses/vrs

Požadavky:

- Nízká latence protokolu
- Minimální jitter (kolísání velikosti zpoždění paketů)
- Globální časová báze (viz minulá přednáška, Kopetz)
- Rychlá detekce chyb na straně přijímače
- Pohlcení časových chyb komunikačním systémem (rušící uzel nesmí narušit komunikaci správných uzlů)

Řešení: globální čas, pro FT dva nezávislé samotestující se kanály se synchronizací obou

- **Event triggered** (spouštěné událostí): Ethernet, CAN, UDP
- **Rate-constrained** (garantované časové limity): ARINC 629, ARINC 684 (AFDX)
- **Time-triggered** (deterministická komunikace, přesné určení času): TTP, TTEthernet, FlexRay



http://en.wikipedia.org/wiki/TTEthernet

Spolehlivostní

- ECC
- Opakování přenosu … = časová redundance (zvyšuje jitter):

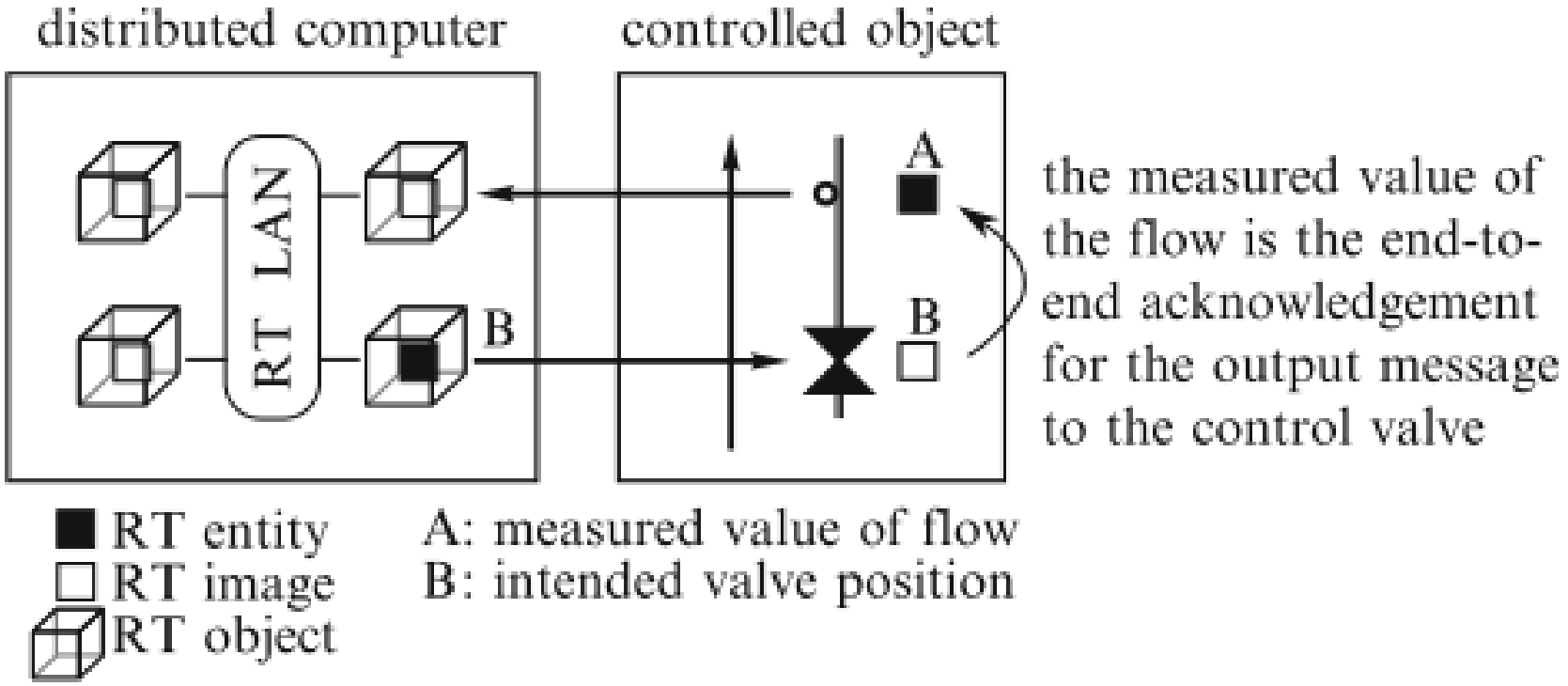
  PAR protokol (Possitive Acknowledgement-or-Retransmission): .... dlouhé , nelze pro RT

  RT řešení: pro periodické zprávy neopakovat vyslání, ale počkat na další zprávu
- Zajištění aby chybná zpráva nenarušila komunikaci (časové zapouzdření poruch): časový firewall = odpojení uzlu při nesplnění časových limitů

  (Př. chybná komponenta v CAN sběrnici, která posílá zprávy s nejvyšší prioritou blokuje komunikaci ostatních komponent)

- Detekce poruch: CRC … jen detekce ne oprava …
  - detekce chyby na výstupu (u přijímače) … musí detekovat ztrátu komunikace a přepnout se do bezpečnostního režimu (*safe state*)
  - Detekce na vstupu … porušení periodicity: vyslání chybové zprávy

  Komunikační protokol musí detekovat selhání komponenty a informovat zbylé … *membership service*
- End-to-end potvrzení: když na výsledku spolupracuje více uzlů … očekávaný efekt
- Determinismus : pořadí zpráv obzvláště pro replikované zprávy a více redundantních kanálů (pořadí zpráv může být různé = ztráta schopnosti maskovat poruchy)



Zásada: nikdy nevěřit akčnímu členu (aktuátoru), vždy změřit a zpracovat výsledek!

- Nutnost změn konfigurace bez velkých zásahů do SW nebo HW
- Komunikační topologie .. multicast ne point-to-point …. informace se šíří všem uzlům
- Dynamické přidání nového komunikačního partnera (např. využívání různých prvků v autě různými řidiči .. přizpůsobení uživateli)
- Technické potřeby a ekonomická omezení (řízení elektrárny nebo pračky)
- Fyzická izolace poruch … rušení, optika
- Efektivní (=levné) přenosové medium … váha a cena v autě rozhoduje

- Základ = BMTS (*basic message transport service)*
- Cíl: přenášet zprávy od vysílače k přijímači/ům z vysokou spolehlivostí, malým zpožděním a minimálním jitterem
- Tok zpráv v BMTS musí být jednosměrný (zamezení vlivu chyb přijímače)
- BMTS … něco jako datagramová služba, ale navíc s časem

- **Event triggered** : sporadické zprávy, nelze splnit časové garance zpoždění mezi vysíláním a přijímáním, při větším počtu zpráv než BMTS zpracuje – ztráta zprávy
- **Rate-constrained** : sporadické zprávy, ale s garancí maximálního toku. Garance worst-case latence, jitter závisí na zatížení sítě (= nejhorší – minimální latence přenosu)
- **Time-triggered** : dané přesné okamžiky vysílání a přijímání, jitter je daná přesností globálního času

Šířka pásma (*„bandwidth“*) a propagační zpoždění:

Přenosová rychlost vlny v kabelu je cca 2/3 rychlosti světla (300,000 km/s) … zpoždění signálu na 1km je 5μs

Bitová délka kanálu (*bit length, bl*) = počet bitů, které mohou projít kanálem v rámci stejného propagačního zpoždění

Př. Šířka pásma je 100 Mbit/s a délka kanálu 200m, *bl* =?

řešení: *bl* … 100 bitů

propagační zpo

bl = šířka pásma x(krát) zpoždění dané délkou kanálu/sběrnice

Dodržení minimálního intervalu propagačního zpoždění mezi dvěma následnými zprávami:

$$data\ efficiency < m/(m + bl)$$

bit lenght … bl
délka zprávy .. m bitů

Př. Sběrnice 1km, šířka pásma 100Mb/s, délka zpráv 100 bitů:
bl = 500 bitů, data_efficiency=100/(100 + 500) = 16.6%.

Nejlepší využití kanálu (pro zprávy kratší než *bl*) je menší než 50% … není efektivní posílat krátké zprávy po dlouhých kanálech s velkou šířkou pásma

(Pro 100m kanál s 1Gb/s minimální zpráva > 500b)

bit-length kanálu jako funkce jeho délky a šířky pásma:

Channel length and propagation delay in seconds	Bandwidth of the channel in bits per second and bit length in seconds						
	10 kbit 100 µs	100 kbits 10 µ	1 Mbit 1 µ	10 Mbit 100 ns	100 Mbit 10 ns	1 Gbit 1 ns	10 Gbit 100 ps
1 cm – 50 ps	<1	<1	<1	<1	<1	<1	<1
10 cm – 500 ps	<1	<1	<1	<1	<1	<1	5
1 m – 5 ns	<1	<1	<1	<1	<1	5	50
10 m – 50 ns	<1	<1	<1	<1	5	50	500
100 m – 500 ns	<1	<1	<1	5	50	500	5 k
1 km – 5 µs	<1	<1	5	50	500	5 k	50 k
10 km – 50 µs	<1	5	50	500	5 k	50 k	500 k

= řízení rychlosti informačního toku mezi vysílačem a přijímačem (*congestion … zahlcení*)

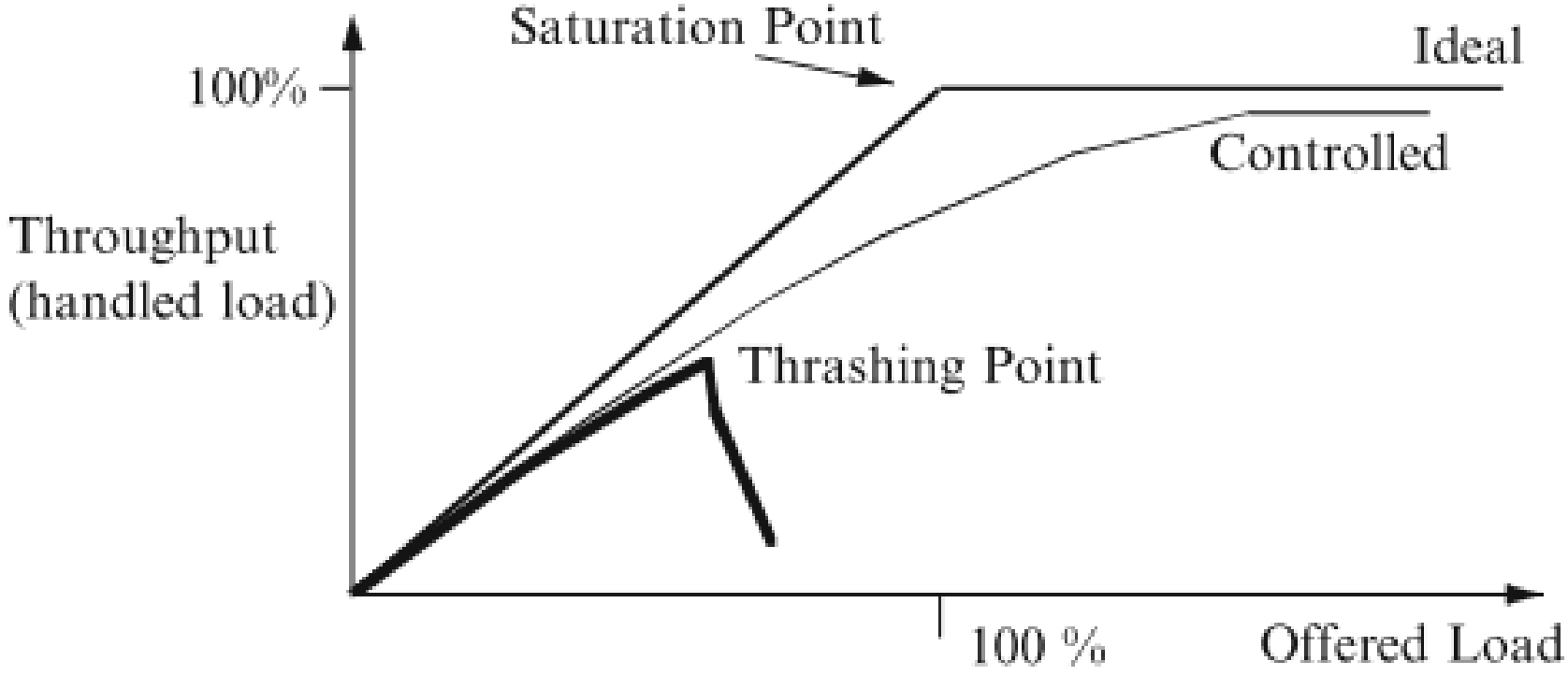
- **Back-pressure**: zpoždění vysílání, když je zahlcená síť
- **Explicitní řízení**: přijímač posílá ACK (PAR protokol)
- **Best-effort řízení**: buffery, přetečení bufferu=zahození zprávy (nepredikovatelnost, nelze použít v hard RT systémech)
- **Rate-constrained**: před začátkem komunikace nastavení maximálního toku


Computer to Pilot:
"Please fly more slowly, I cannot follow your commands"

- **Implicitní řízení:** a priori před začátkem komunikace nastavení okamžiků vysílání a přijímání
  - Globální časová báze
  - Žádné ACK zprávy v době běhu
  - Detekce poruch – přijímač
  - Latence detekce – krátká, závisí na přesnosti synchronizace hodin

V RT nesmí být!!!

Způsobují ho: retry mechanizmy, služby OSY (čas pro dynamické plánování)



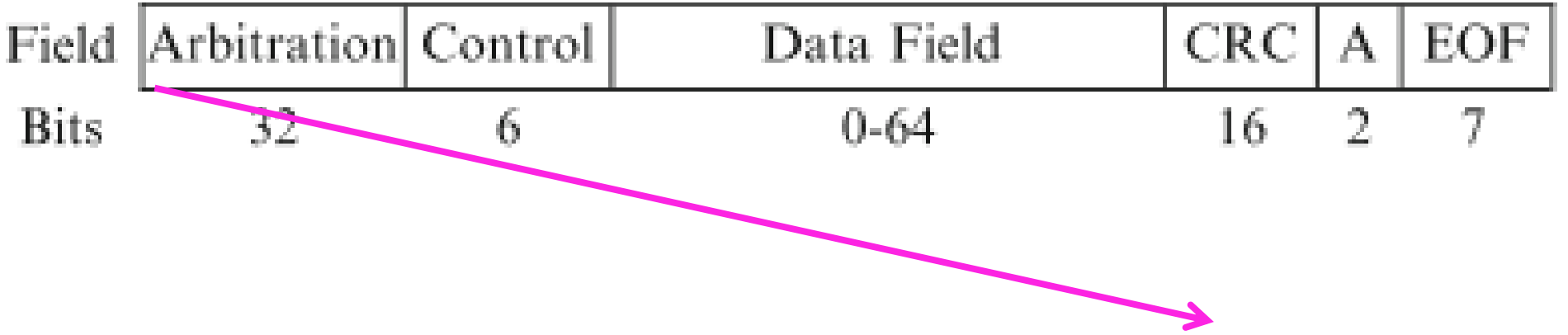
- Event-Triggered (komunikace spouštěná událostmi): Ethernet, CAN, UDP
- Rate-Constrained (komunikace s minimálním garantovaným tokem pro minimální šířku pásma): token protokol, ARINC 625, AFDX, Audio-Video (IEEE 802.1 AVB)
- Time Triggered (komunikace spouštěná časem): TTP, TTEthernet, Flex-Ray

Komunikace spouštěná událostmi:

- nelze poskytnout časové garance
- nízkoúrovňový protokol, který zvyšuje spolehlivost linky, není přímo viditelný z BMTS a zvyšuje jitter

- CSMA/CD *(carrier sense multiple access-collision detection)*
- IEEE standard 802.3
- strategie řízení best-effort
- pro RT – rozšíření standardu na deterministický přenos zpráv

- CSMA/CA *(carrier sense multiple access-collision avoidance)*
- formát CAN zprávy:



Field	Arbitration	Control	Data Field	CRC	A	EOF
Bits	32	6	0-64	16	2	7

- dominantní a recesivní zprávy (první bit 0/1) ... *zpráva začínající 0 má nejvyšší prioritu*
- propagační zpoždění kanálu menší než délka zprávy

- efektivní protokol,
- jednosměrný, nespolehlivý
- multi-casting pro LAN
- best-effort řízení

RT aplikace: poměr mezi latencí a spolehlivostí není HW, ale v aplikační vrstvě (na rozdíl od TCP) ... využití v multimediálním streamování

= komunikace s minimálním garantovaným tokem

pro minimální šířku pásma:

- garantovaná maximální přenosová latence a maximální jitter
- při překročení – best-effort strategie (možnost zahlcení)
- komunikační systém musí obsahovat informaci o garantované šířce pro každý vysílač (předem nebo dynamicky)
- detekce časových chyb a zahlcení
- není deterministické (nelze predikovat čas doručení zprávy)

- LAN (token ring IEEE 802.5, token bus .. deterministické řízení???)
- řízení speciální řídící zprávou ... token

THT = token hold time (max. doba držení tokenu uzlem)

TRT = token-rotation time (nejdelší čas oběhu tokenu sítí)

selhání ... ztráta tokenu (= např. porucha pracujícího uzlu ... dá se detekovat, že se nic nepřenáší)

- mini-slotting protokol („waiting room“)
- přístup ke sdílené sběrnici řízen:
  - SG (*synchronization gap*) – řídí vstup do čekacího místa (stejný pro všechny uzly)
  - TG (*terminal gap*) – řídí přístup z čekacího místa ke sběrnici (časovač, různý pro každý uzel, musí být násobkem propagačního zpoždění ... *mini-slot*)

    pro všechny uzly *i* musí: $SG > Max\{Tg_i\}$
  - protokol garantuje, ze si uzel nemonopolizuje sběrnici →i uzel s nejnižším TG (nejvyšší prioritou) může poslat druhou zprávu až po ukončení přenosu všech uzlů ve waiting roomu.
  - typické hodnoty pro 2Mbit/s kanál: TG: 4-128ms

- formát zpráv na fyzické vrstvě standard IEEE 802.3
- protokol alokuje staticky definovanou šířku pásma každému vysílači ve virtuální linkové vrstvě. Virtuální link propojuje vysílače s určeným počtem přijímačů

AFDX garantuje:

- zachování pořadí doručovaných zpráv po virtuální lince
- minimální šířku pásma, maximální přenosovou latenci a max. jitter
- žádné ztráty dat z důvodů přeplnění bufferu

Airbus A380: (Boeing Dreamliner

Latency (ms)	0–0.5	0.5–1	1–2	2–3	3–4	4–8	8–13
Percent of traffic	2%	7%	12%	16%	18%	38%	7%

multimedia ... jednosměrný, point-to-point systém, ... specializovaný zjednodušený protokol

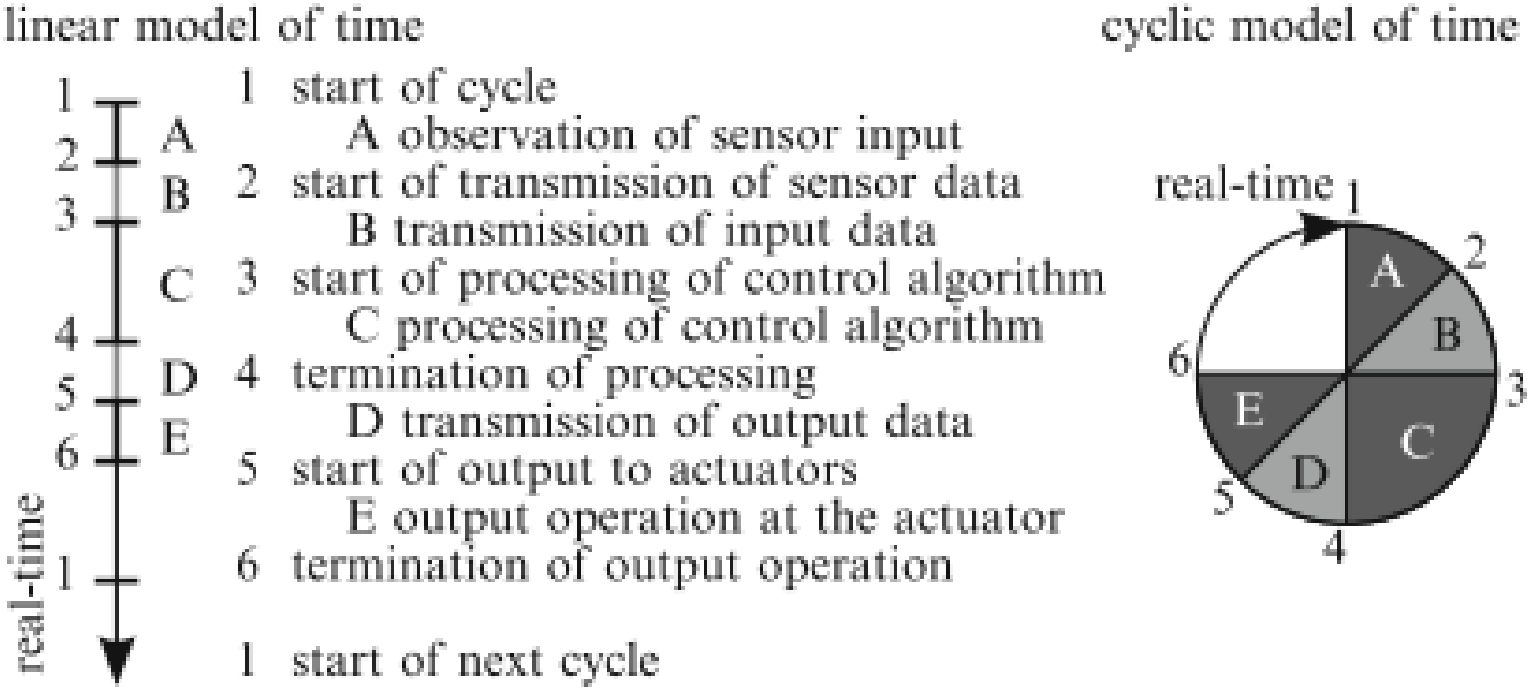
QoS pro multimedia:

1. přesná synchronizace ... µs
2. omezené worst-case zpoždění přenosu ... ms
3. dostupnost dynamicky alokovaných zdrojů po celou dobu přenosové sekce

IEEE 802.1 AVB (audio/video bridging) ... spec. Ethernet

komunikace spouštěná časem →

cyklické časové řízení, bezkonfliktní plánování časových zpráv, cyklický model času (určená perioda a fáze), žádné zpoždění, žádné buffery, determinismus, globální časová báze



TCCS = time-controlled circuit switching

- CA-TCCS – collision avoidance TCCS ... posun sporadických událostí pro zamezení konfliktu TT a ET událostí
- P-TCCS – preemptive TCCS ... přerušení - přeplánování TT události a zaslání TT zprávy s minimálním zpožděním a jitterem
- CT-TCCS – collision tolerant TCCS ... při dvou třídách zpráv: TT a neřiditelných ... odeslání replik TT zpráv s tím, že aspoň jedna replika dojde nepoškozena

- CA-TCCS: TT komunikace, detekce časových chyb,
- FT synchronizace: korekce lokálních hodin
- membership service: membership vektor

- TT-Ethernet ... vyvinutý na TU Vídeň prof. Kopetz & spol.
- TTEthernet ... průmyslový standard

http://www.ttagroup.org/passing-the-torch.html

- komunikční protokol: kombinace TT protokolu s FT synchronizací hodin (podobné TTP) bez „membership“ služeb

  a ET protokolu podobného ARINC 629 bez čekacích míst

- systémový integrátor rozděluje čas do dvou intervalů (pro TT a ET komunikaci) a podle toho nastavuje další parametry

automobily Audi a BMW

Typický postup:

- Přístup do vybraného podsystému
- Hledání zranitelných míst
- Proniknutí a řízení podsystému

- Pasivní (jen sbírání tajných informací)
- Aktivní (modifikace chování napadeného systému)

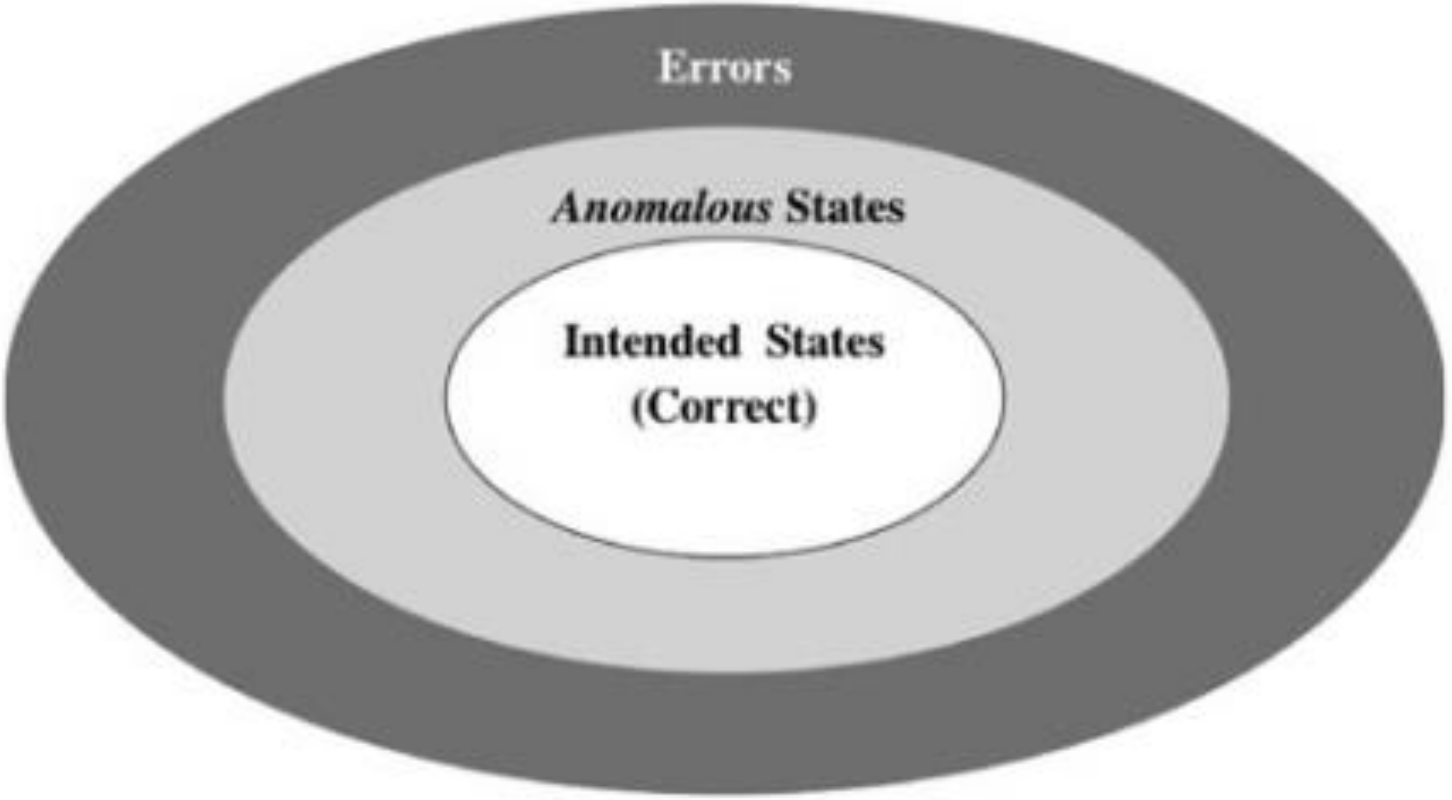
Obrana: detekce útoků (detekce anomálií), firewally, zmírnění následků útoku

Bezpečnostní politika na všech úrovních (včetně organizačních pravidel a zohlednění HCI)

- Zákeřný útok na kód – virus, červ, Trojský kůň (statický i dynamický)
- Spoofing – útočník se maskuje jako legitimní uživatel (např. phishing)
- Nalezení hesla – slovníkové metody (obvykle používaná hesla) x hrubá síla
- Nalezení šifry – hledání klíče (obrana AES)
- Odmítnutí služby – např. umělé zahlcení sítě
- „Botnet“ útok – napadení sítě uzlů a znemožnění práce uživatelům („bot“ je zkratka robota)

= snížení pravděpodobnosti útoku na minimum

- Časová omezení (určení max. doby (de)kódování)
- Omezení zdrojů
- Každá bezpečná architektura musí obsahovat:
  - Kódováni symetrickým klíčem
  - Kódováni veřejným klíčem
  - Hash funkce
  - Generátor náhodných čísel

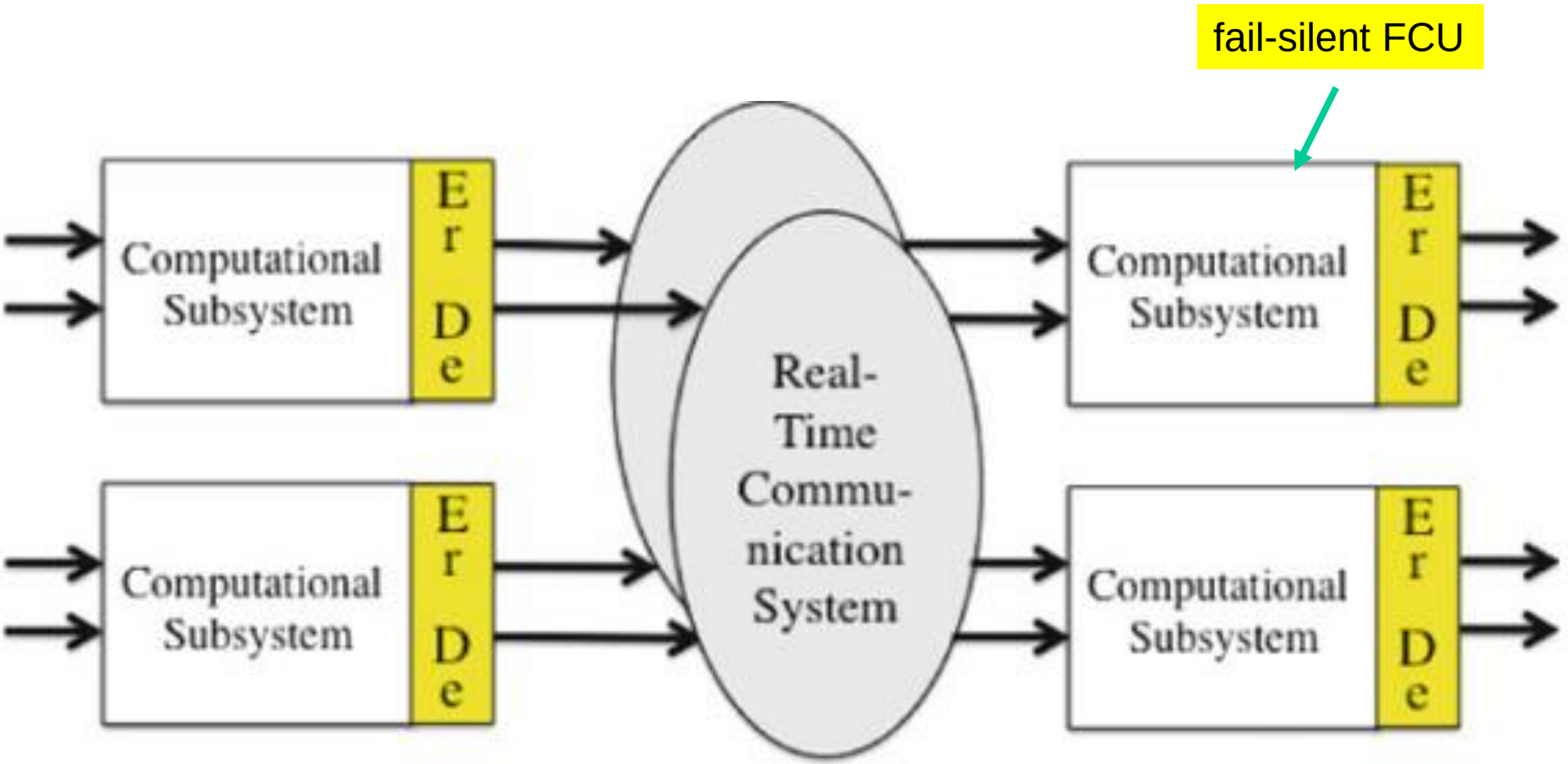


- Detekční susbsystém musí být oddělen od procesního, nezávisle na OS (2 skupiny návrhářů: OS a detekce anomálií) … on-line

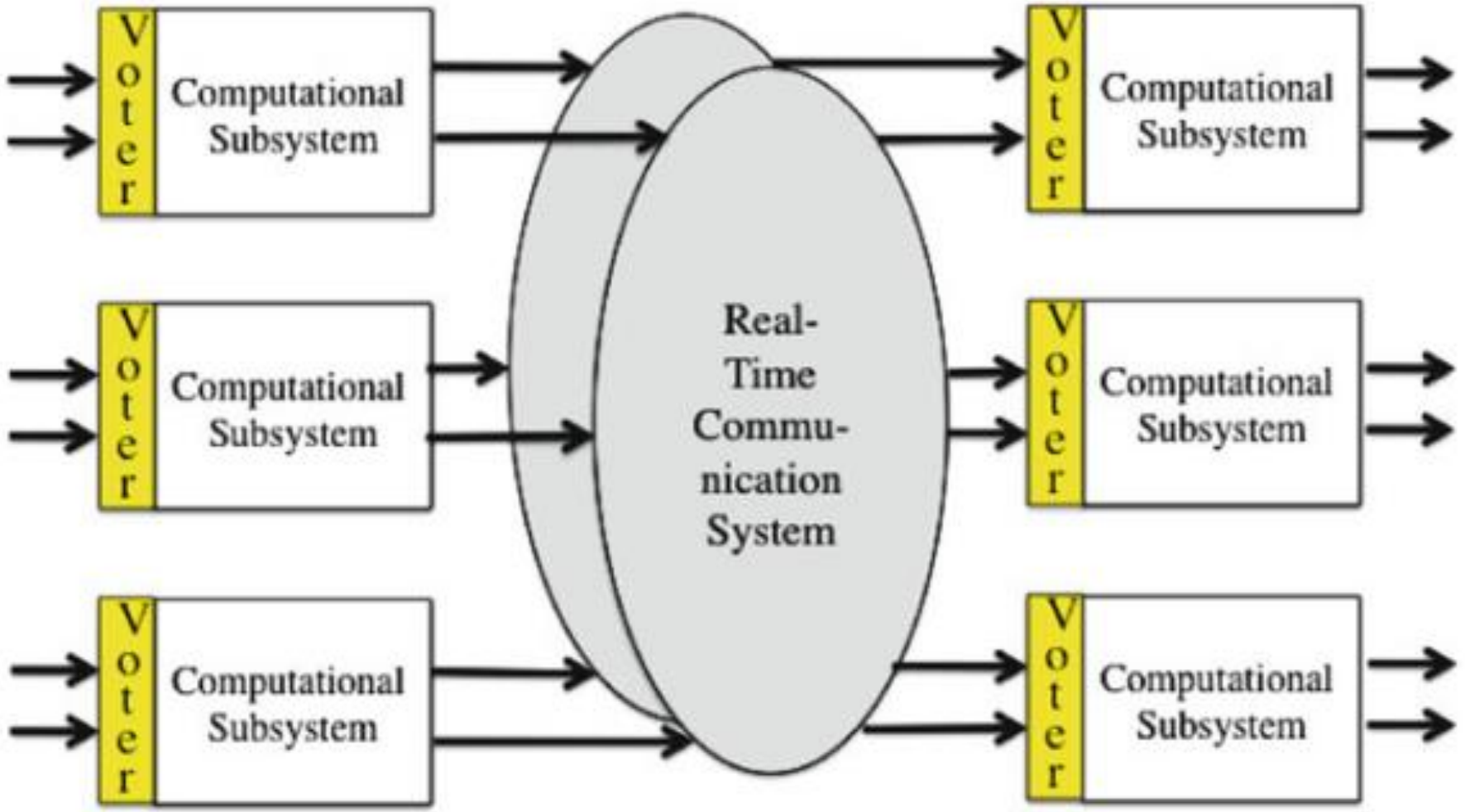
- Redundance
- Srovnání s etalonem („zlatá reference“)
- Kontrola WCET

Detekce chyb

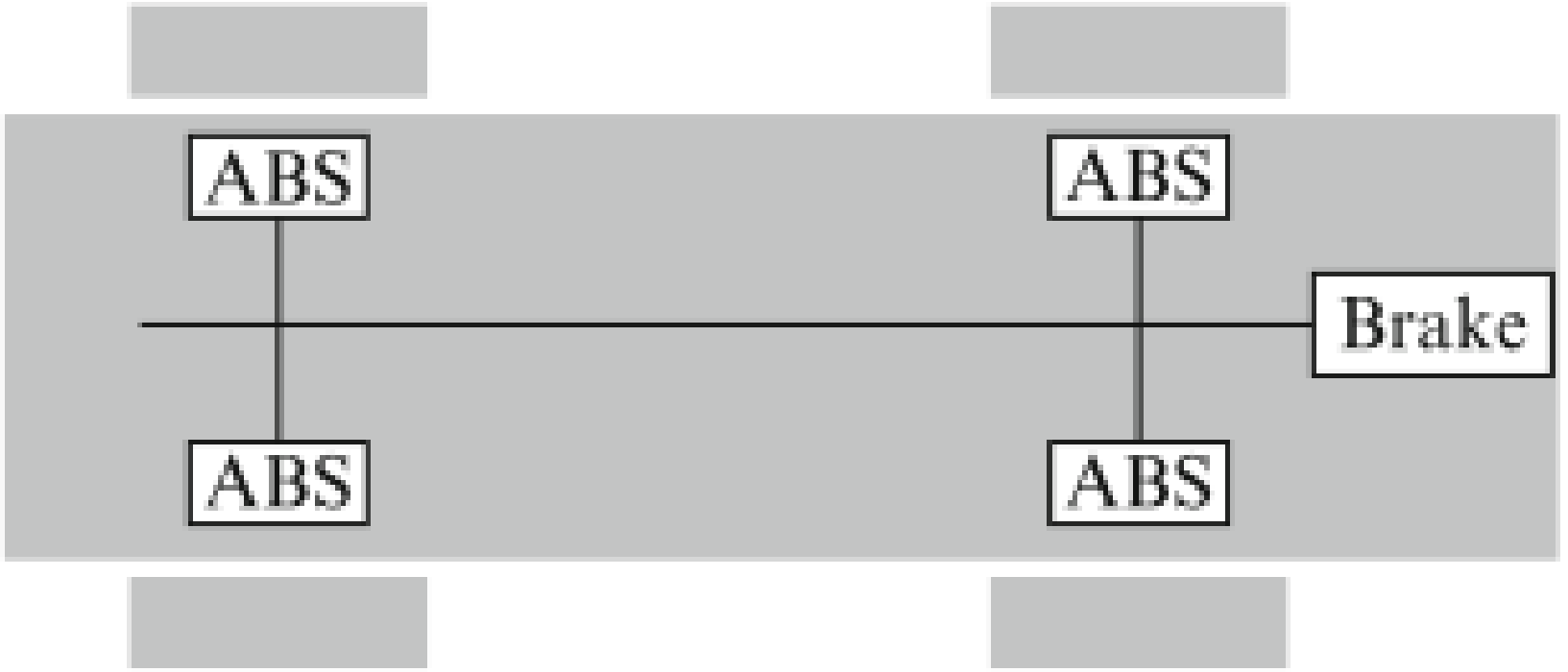
- Opět redundance
- Srovnání s etalonem („zlatá reference“) - CRC
- Duplikace i kanálů (protokoly, LIF – linking interface)



FCU (Fault-Containment Unit) = jednotky, ve kterých můžou nastat poruchy v podstatě nezávisle
FTU = fault-tolerant unit
ErDe = detektor poruch


Voter
Computational Subsystem
Voter
Computational Subsystem
Voter
Computational Subsystem
Real-Time Commu-nication System
Voter
Computational Subsystem
Voter
Computational Subsystem
Voter
Computational Subsystem

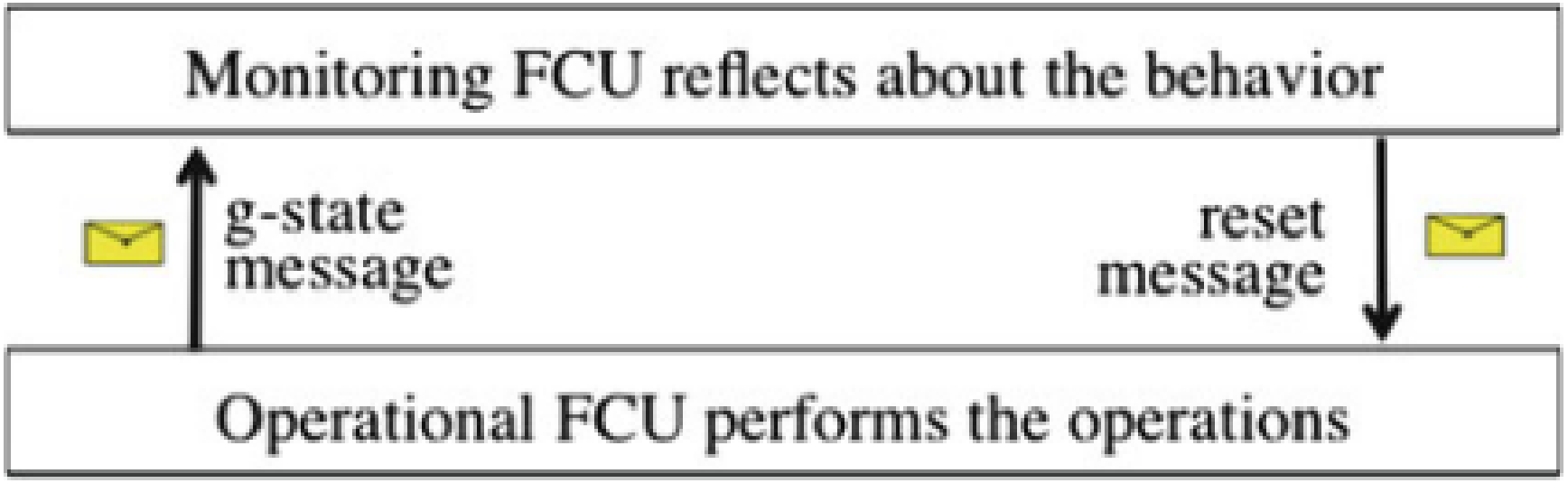
- Brzdy, ABS systém



- ET (přidání času – watchdog) vs TT architektura

Když je závažnost následků poruch nepřímo úměrná pravděpodobnosti jejich objevení (časté poruchy mají mít malý vliv na QoS)

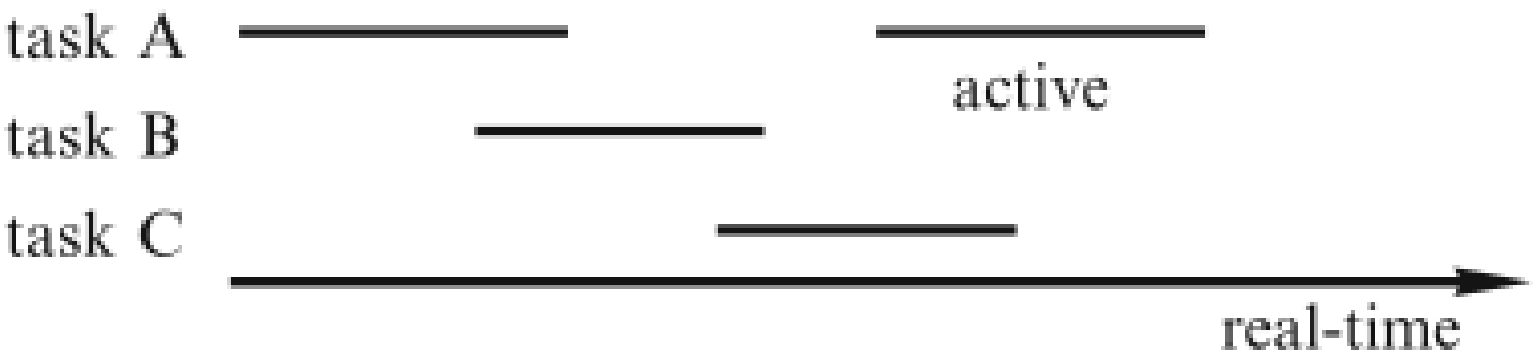
Alespoň dva subsystémy, dvoukanálové řešení:

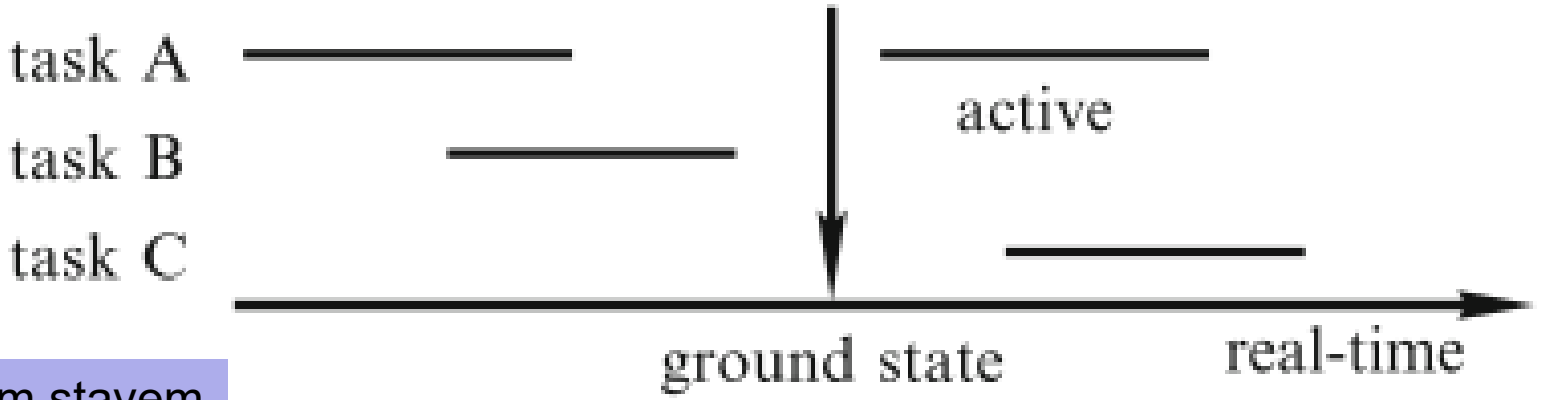


- Kdy začlenit opravenou jednotku
- Pomáhá g-stav (základní, ground)
- U cyklických systémů na začátku cyklu

- Restart obnovené komponenty:
  - Monitorovací komponenta pošle RESET zprávu TII
  - po RESETu self-test obnovené komponenty
  - Scan všech senzorů – zjištění akt. módu řízeného systému
  - Po získáni informace o g-stavu (může se reintegrovat) synchronizace s ostatními subsystémy

Bez základního stavu

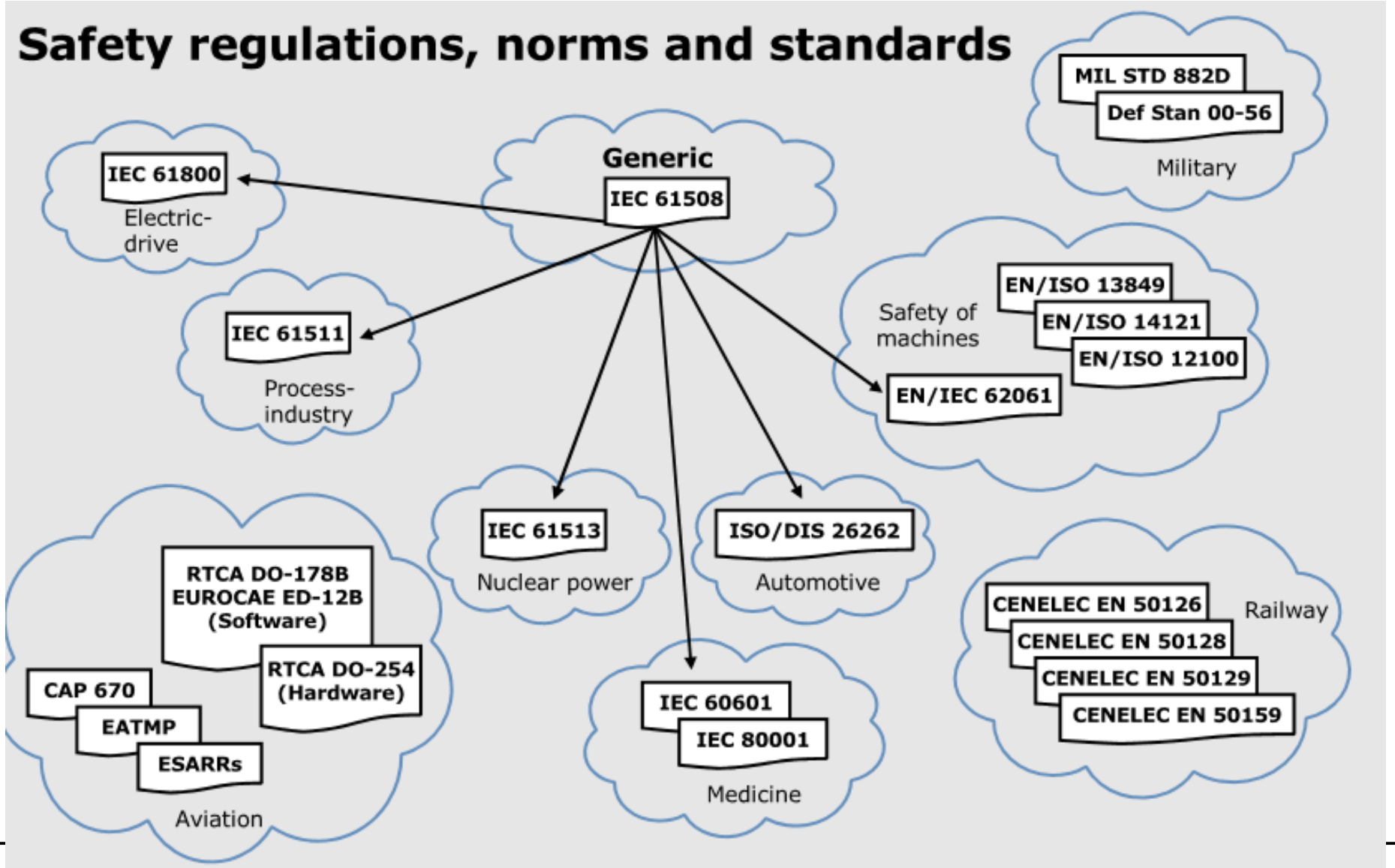


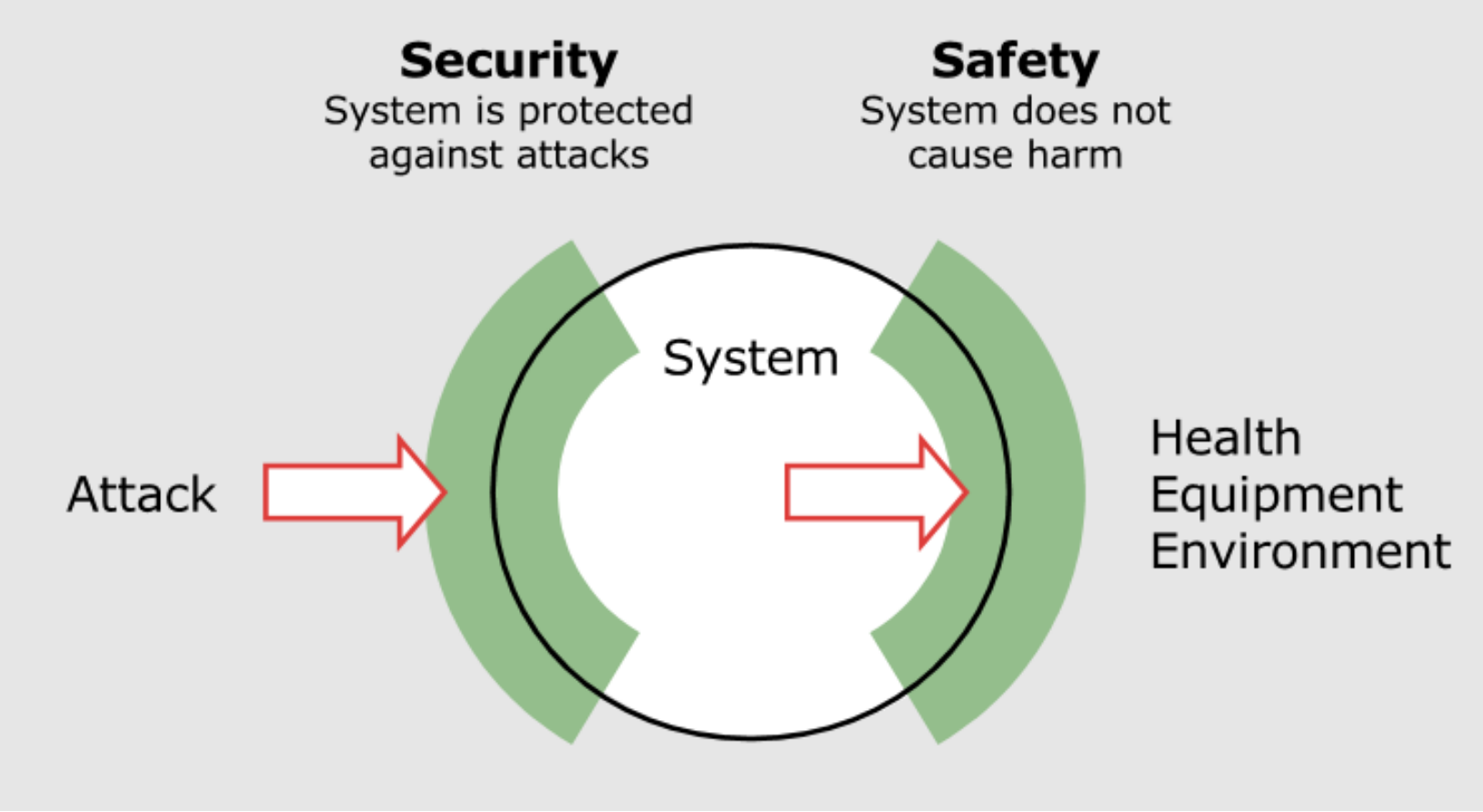


Se základním stavem

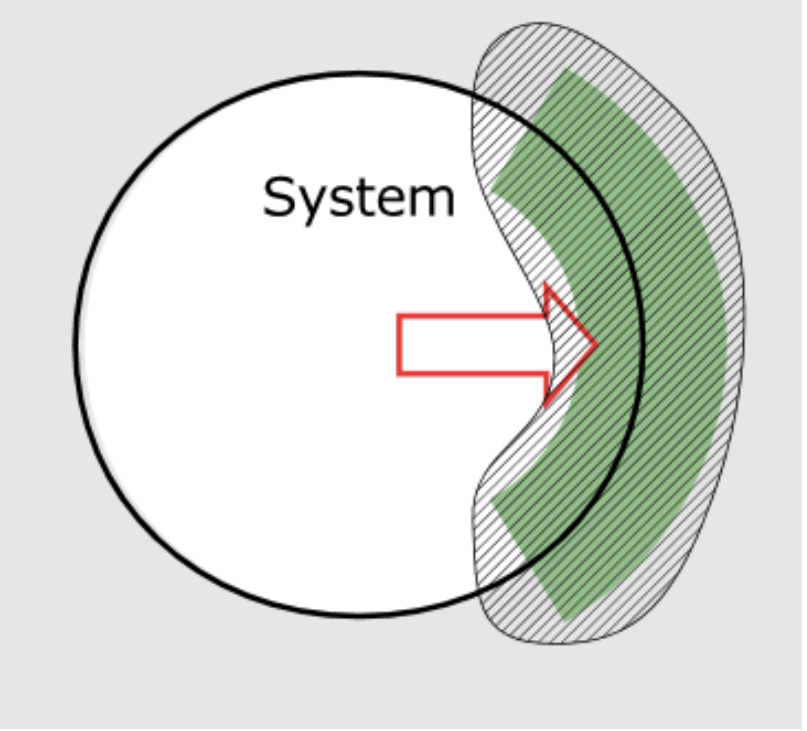
Restart křižovatky

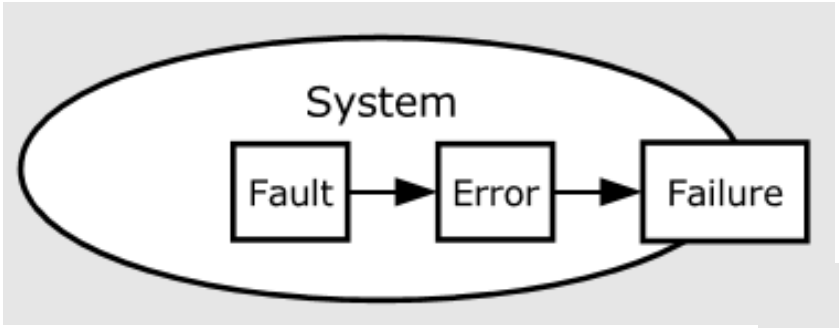
1. Jednodušší verze (relativně snadná synchronizace mezi realitou a řídícím systémem): restartovací vektor pro semafory nastaví všude oranžovou, pak červenou a nakonec hlavní tah na zelenou … *ground state*
2. Složitější alternativa: rekonstrukce stavu podle log souboru, kde je uložena posloupnost výstupních signálů před poruchou

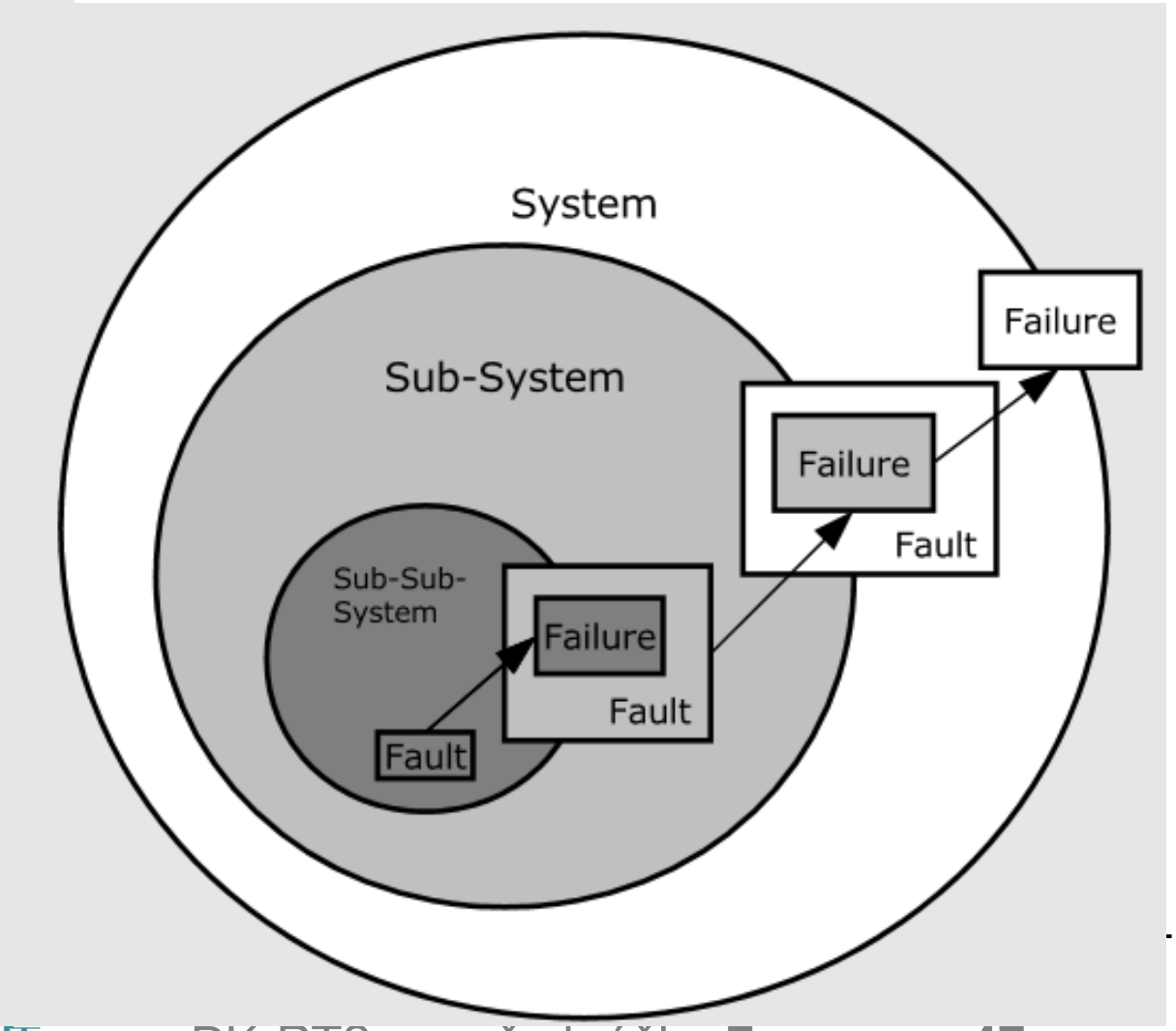

Safety regulations, norms and standards
Generic
IEC 61508
IEC 61800
Electric-drive
IEC 61511
Process-industry
MIL STD 882D
Def Stan 00-56
Military
Safety of machines
EN/ISO 13849
EN/ISO 14121
EN/ISO 12100
EN/IEC 62061
IEC 61513
Nuclear power
ISO/DIS 26262
Automotive
RTCA DO-178B
EUROCAE ED-12B
(Software)
RTCA DO-254
(Hardware)
CAP 670
EATMP
ESARRs
Aviation
IEC 60601
IEC 80001
Medicine
CENELEC EN 50126
CENELEC EN 50128
CENELEC EN 50129
CENELEC EN 50159
Railway


Security
System is protected against attacks
Safety
System does not cause harm
System
Attack
Health
Equipment
Environment

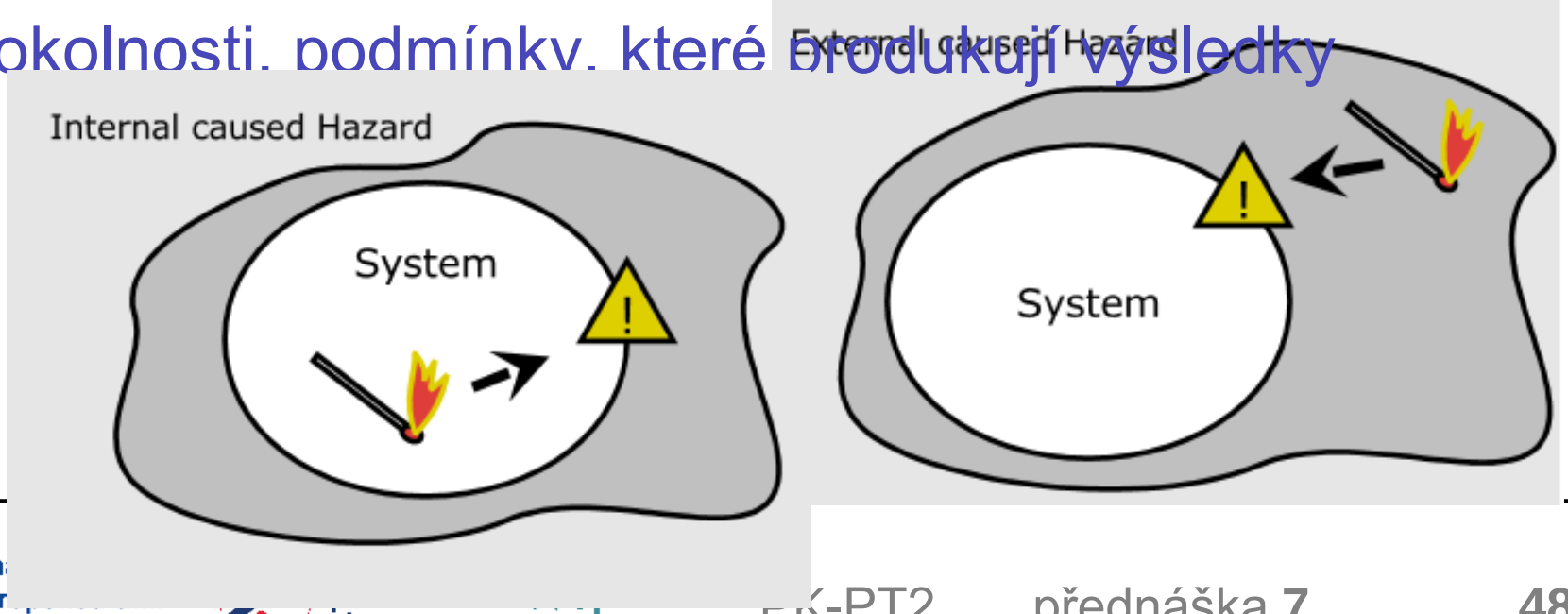
- Reliability: systém pracuje podle očekávání
- Spolehlivost (bezporuchovost) bezpečných funkcí (fungují podle očekávání): safety integrity level

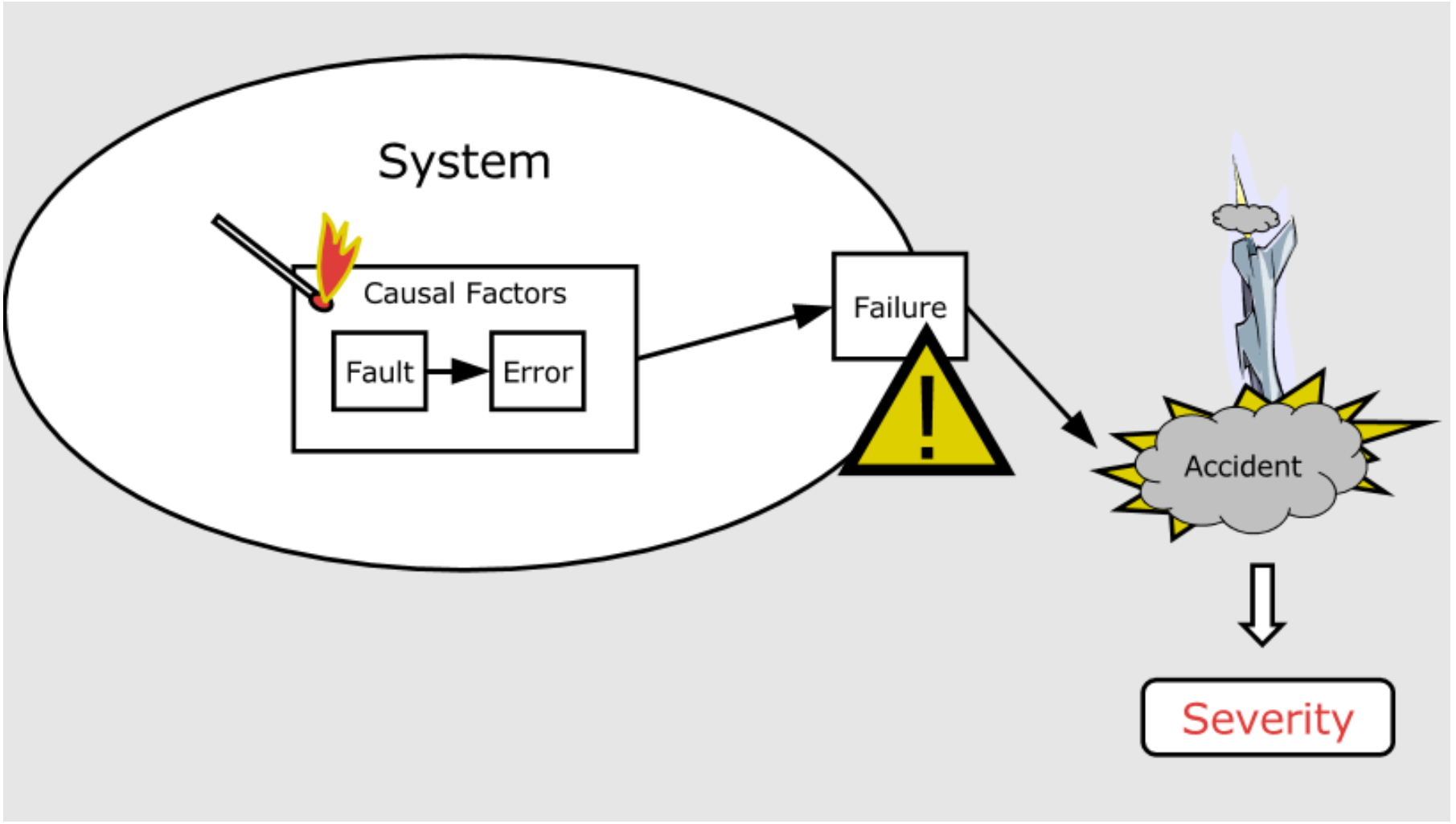


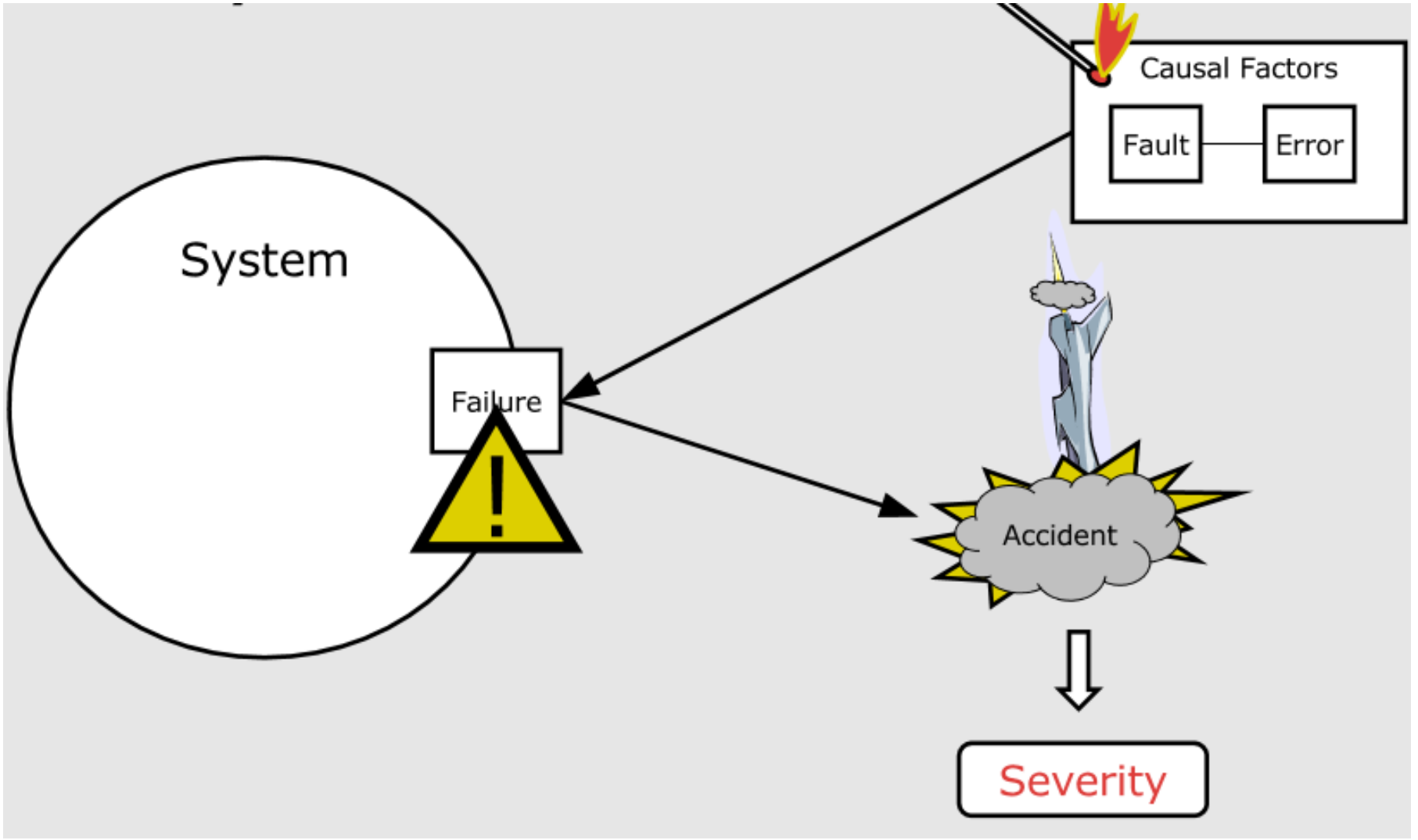

System
Fault
Error
Failure

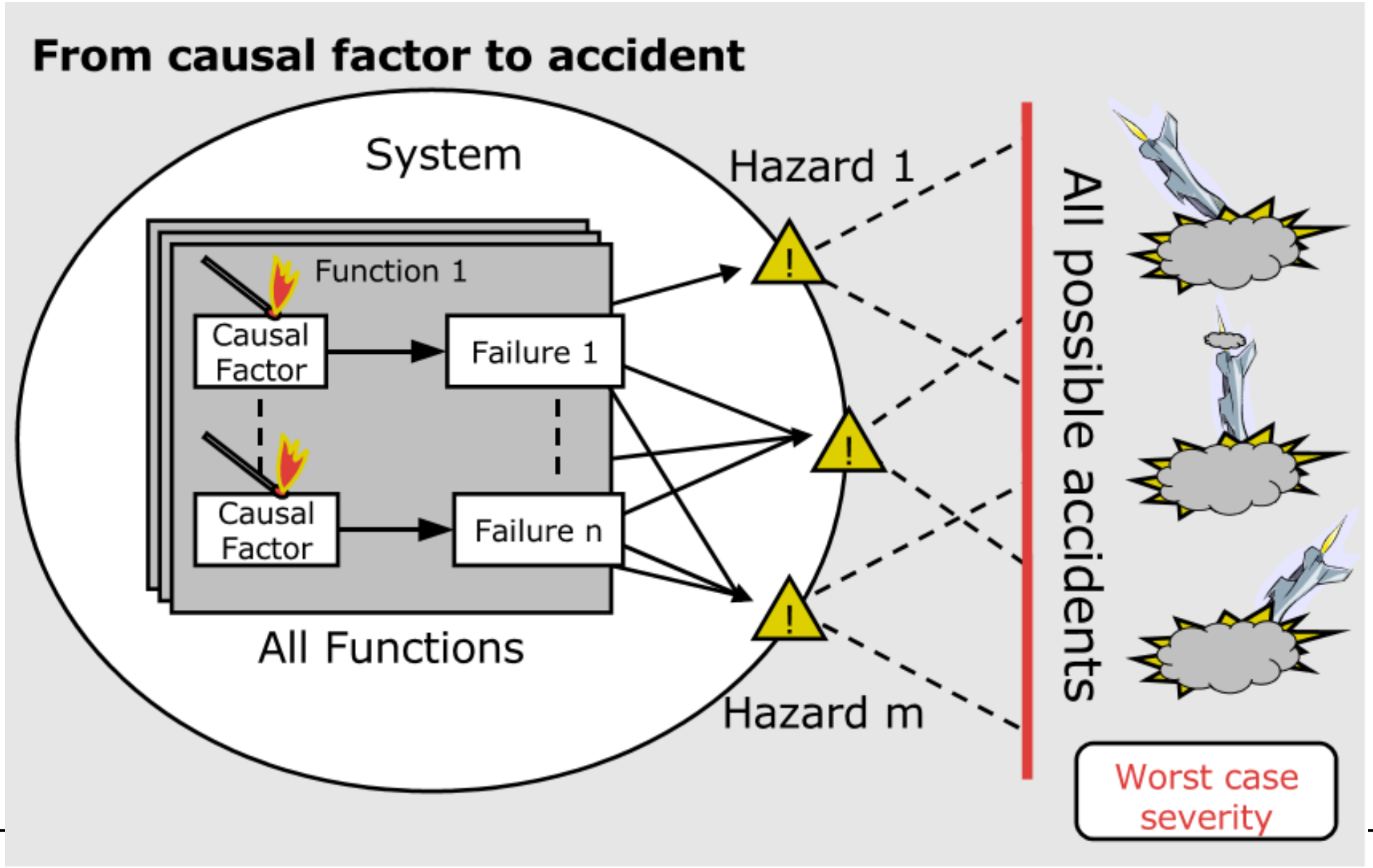

System
Sub-System
Sub-Sub-System
Fault
Failure
Fault
Failure
Fault
Failure

- Situace, stav nebo podmínka, která může vést k nehodě
  - hazardy jsou popsány na hranicích systému
  - je důležité identifikovat tyto hranice
- Každé nebezpečné selhání je hazard
- Faktory, které mohou přispět k hazardu:
  - okolnosti, podmínky, které produkují výsledky




System
Causal Factors
Fault
Error
Failure
Accident
Severity


Causal Factors
Fault
Error
System
Failure
Accident
Severity


From causal factor to accident
System
Function 1
Causal Factor
Failure 1
Causal Factor
Failure n
All Functions
Hazard 1
Hazard m
All possible accidents
Worst case severity

- robustní systém
- porucha automaticky vede do bezpečného stavu
- detekce poruchy, přechod a údržba
- detekce poruchy a upozornění uživatele
- redundance ve smyslu detekce násobných poruch, a tím předcházení latentním poruchám
- hardware, software a systémová integrace
- verifikace, validace, dokumentace
- důkaz toho, že systém je bezpečný