Dopady a omezení CENELEC architektur na důkaz bezpečnosti

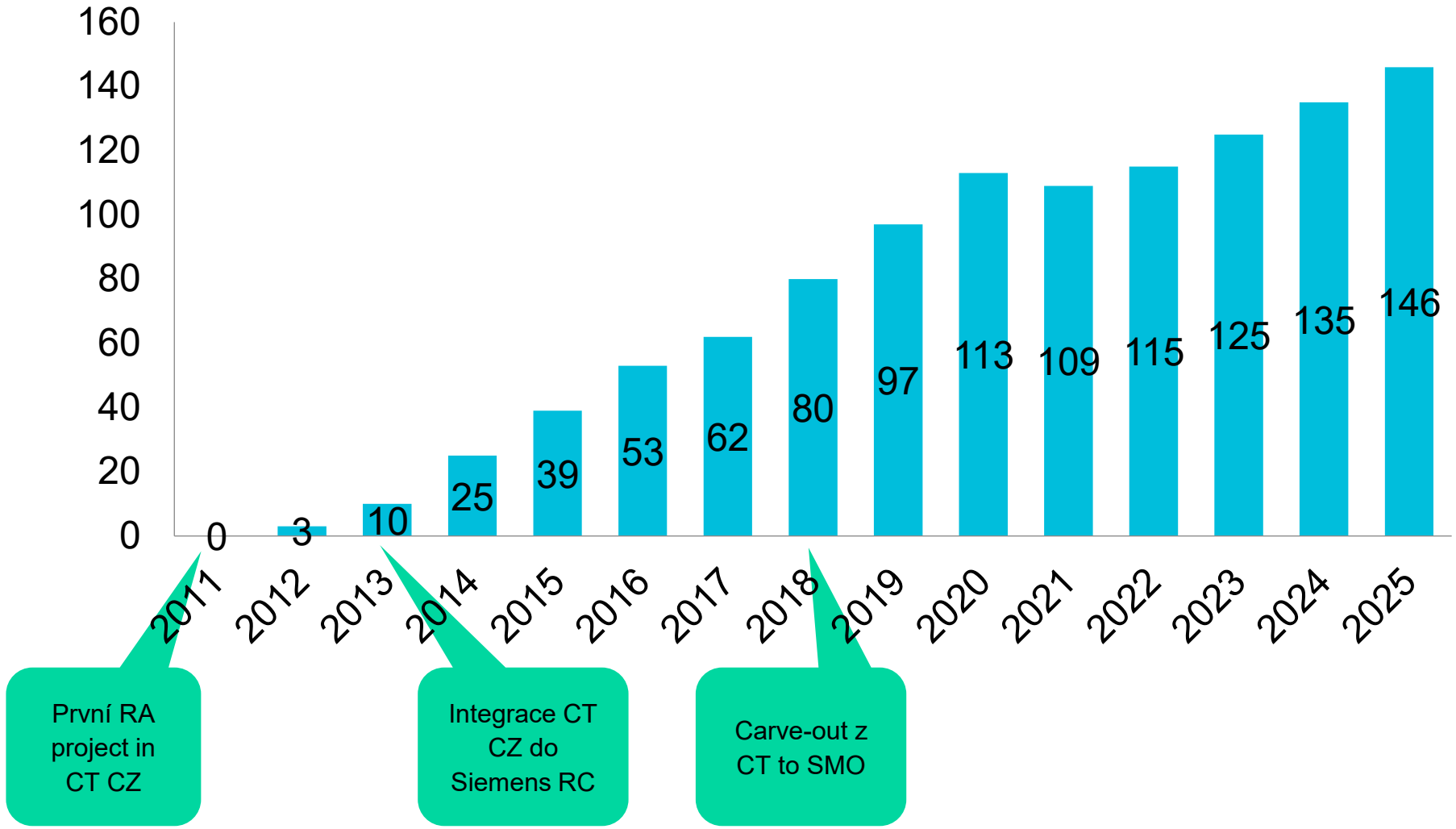
SIEMENS Mobility, Praha, 10. 2. 2026

SIEMENS

Obsah

SIEMENS

Historie oddělení RI LCE CZ

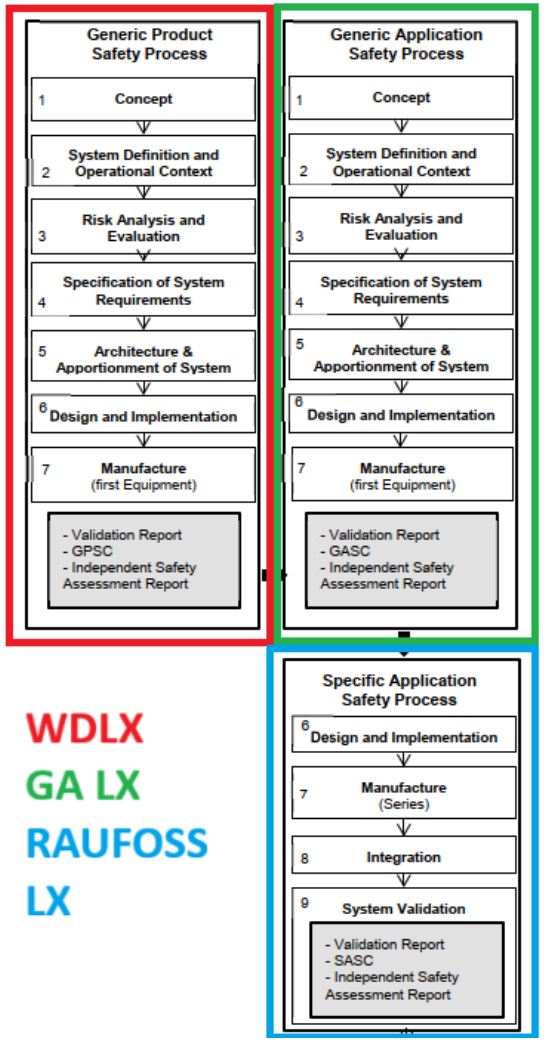


Projektové role:

- HW/SW/SYS vývojáři a architekti
- HW/SW/SYS validátoři
- RAMS management
- Security SW Design (CS)
- PM, QM
- Scrum masters

SIEMENS

RI LCE – Od produktového R&D až k zákazníkovi



- Pokrytí kompletního vývojového a integračního cyklu od generického produktového návrhu až po konkrétní aplikaci (EN 50126-1)
- PZZ WDLX, distribuované ovládací a komunikační moduly s EULYNX pro SINET (xCM – DCM, PCM, CCM,…)
- Security – CoreShield infrastruktura

Příklad:

GP – WDLX 0.7

GA – GA LX Subsystem Stage 1

SA – Raufoss LX

SIEMENS

EN 50129 příloha E. – Architektury podle SIL

Table E.4 — Architecture of system, subsystem or equipment

Techniques/Measures	SIL 1	SIL 2	SIL 3	SIL 4	
1 Separation of safety-related functions from non-safety-related functions to prevent unintended influences	See 7.2, "Section 3 of the Technical Safety Report"				
2 single electronic structure with self-tests and supervision	R	R	NR	NR	(a)
3 single electronic structure based on inherent fail-safety	R	R	HR	HR	(b)
4 single electronic structure based on reactive fail-safety	R	R	HR	HR	(c)
5 Dual electronic structure	R	R	NR	NR	(d)
6 Dual electronic structure based on composite fail-safety with fail-safe comparison	R	R	HR	HR	(e)
7 Diverse electronic structure with fail-safe comparison	R	R	HR	HR	(f)
For a given SIL all techniques of the grey shaded group are alternatives, i.e. at least one of these techniques should be chosen. For a given safety-related function, several techniques may be combined so as to address all kinds of faults affecting the function. Techniques 2 to 7 include also architectures where additional electronic structures are used for availability purposes (e.g. 2oo3).					

SIEMENS

Základní přístupy pro zajištění technické bezpečnost

Systémy s vnitřní (inherentní) bezpečností

- Lze realizovat pouze na úrovni komponent (taxativní výčet - příloha C. EN 50129)
- Nelze prokázat pro UPIC (příloha F. EN 50129)

Redundantní systémy

- Vícenásobný vstup, výstup a zpracování informací
- Modulární návrh (2oo2, 2oo3)
- SDT závisí na bezporuchovosti jednotlivých kanálů (součást návrhu)
- Ztráta procesního času výměnou, zápisem a komparací dat

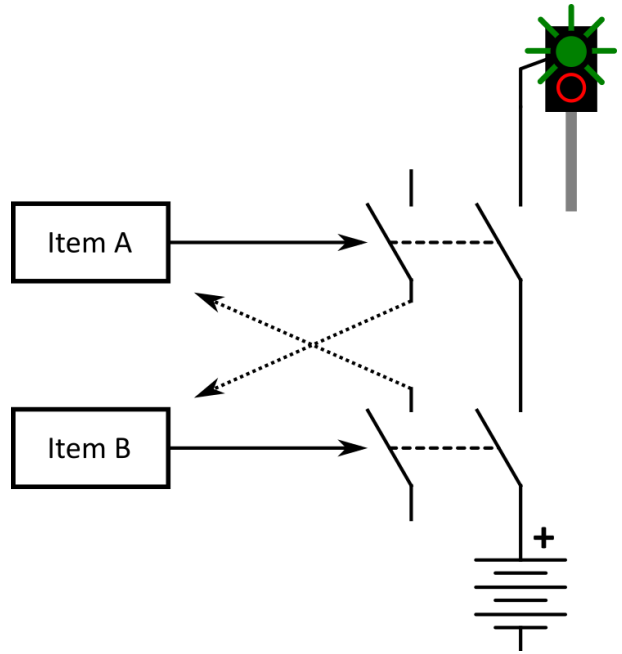
Reakční systémy

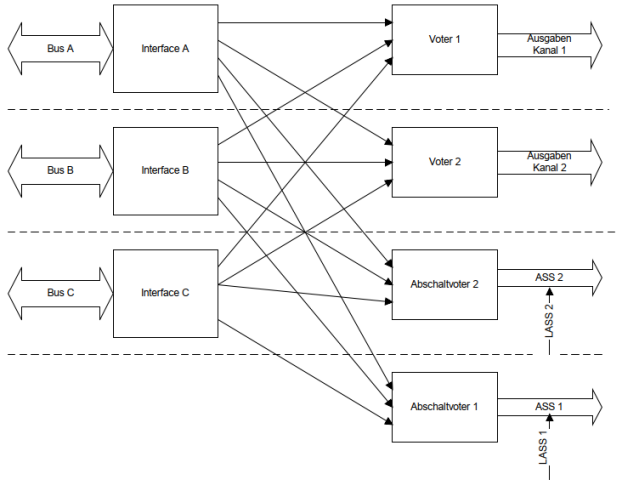
- Hlavní procesní kanál doplněný o nezávislý dohled
- SDT musí být dostatečně nízký pro každé rozhraní (krátkodobá tolerance hazardního stavu)
- Větší dostupný výpočetní výkon při stejném použitém HW

Redundantní (a diverzní) systémy

- Funkce je vykonávána alespoň dvěma nezávislými prvky
- Většina z nich musí souhlasit s provedením neomezující akce (např. stav povolující jízdu na návěstidle nebo přehození výhybky)
- Bezpečná reakce je vyvolána dříve než se nebezpečný stav objeví na externím rozhraní
- Diverzní systém poskytuje vyšší ochranu proti poruchám ze společné příčiny

- Příklad: Dvojité spínání návěstidla, 2oo3 logika spojená s dvoukanálovým výstupem



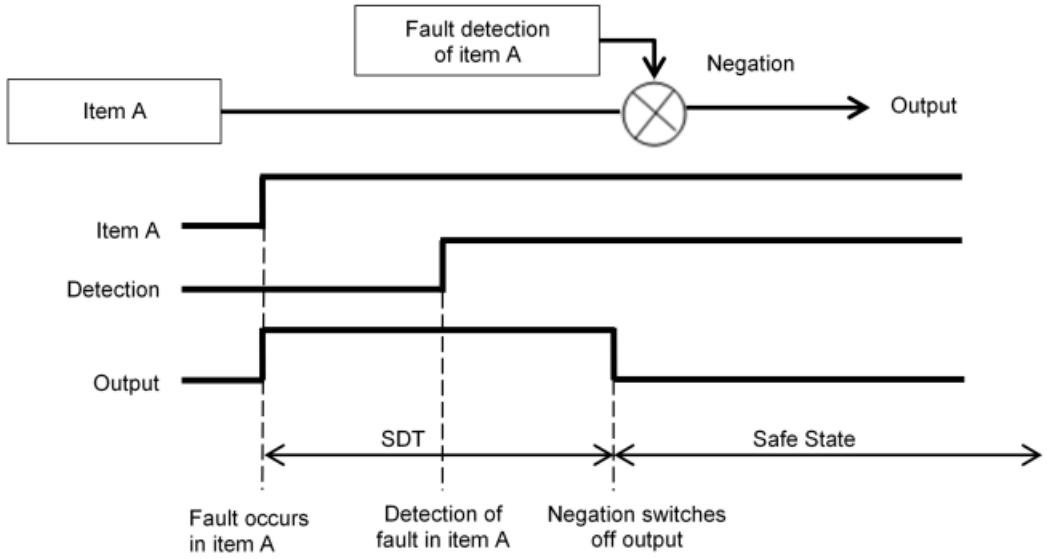


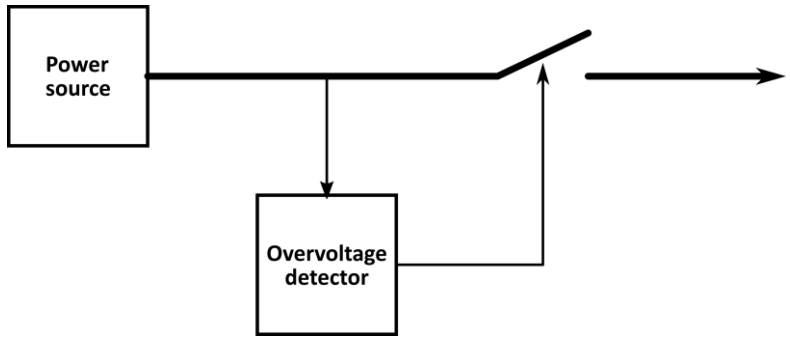
SIEMENS

Reakční systémy

- Funkce je vykonávána jednokanálově a její výstup je kontrolován
- Oba bloky musí být nezávislé
- Selhaní hlavního kanálu se může projevit na vnějším rozhraní
- U řídících systémů není nutná opakovaná výměna dat mezi procesními kanály

- Příklad: Jednoduchý zdroj s výstupní přepěťovou ochranou





Systémy s vnitřní (inherentní) bezpečností

- Nedosažitelné pro komplexní programovatelné obvody
- Použití jako součást důkazu nezávislosti v ostatních typech architektur (kanál A x kanál B, akční člen x dohledový obvod)
- Umožňuje vyloučení komponent z počítání z prvků v jednotlivých funkčních blocích (poruchové stavy pouze bezpečné nebo vyloučené)

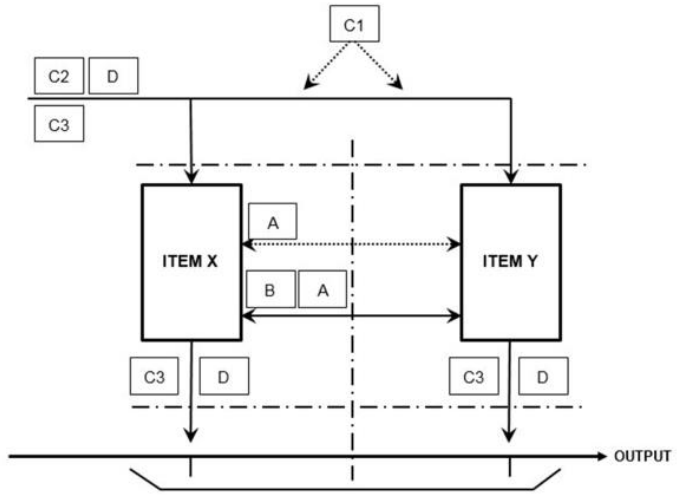
- Příklad: Neztratitelná bariéra mezi potenciály nebo funkčními bloky

Table C.11 — Fuses

Interruption	
Parallel short-circuit	(a)
Increase of rupture current	(a)
Increase of rupture time	(a)
Reconnection after rupture	(b)

(a) The fuse and its holder shall be physically constructed and mounted so as to prevent the occurrence of a parallel short-circuit. Means shall be provided to prevent the use of an incorrectly rated fuse. Clearance and creepage distances shall fulfil at least the requirements for double or reinforced insulation of EN 50124-1.

(b) The fuse shall not have self-resetting or self-healing capability.



"AND" condition for the non-restrictive state of the output

SIEMENS

EN 50129 příloha F. – Programovatelné integrované obvody

F.3.2 Protection against random faults – architectural principles

Similarly to non-programmable HW components the implementation of SIL 3 and SIL 4 safety-related functions within a UPIC implies special care, using composite or reactive fail-safe techniques or data transmission coding strategy protection related techniques.

— **SIL 3 & 4 UPIC development**

Similarly to non-programmable HW components, it is necessary to ensure that SIL 3 and SIL 4 systems, whose functions are carried out by UPIC, remain safe in the event of any kind of single random hardware fault which is recognised as possible. This principle, which is known as fail-safety, can be achieved for UPICs in two different ways:

a) Composite fail-safety structure;

b) Reactive fail-safety structure;

NOTE As UPIC failure modes are not known, it is not deemed possible to demonstrate that each of them is non-hazardous (or justified as incredible). Thus the inherent fail-safe principle is not deemed applicable.

SIEMENS

Dopad zvolené architektury do důkazu bezpečnosti

Systémy s vnitřní (inherentní) bezpečností

- Prokázání zvláštní konstrukce komponenty
- Důkaz provozních podmínek komponent (dimenzování)
- Doložení souladu s požadovanou normou (např. EN 50124-1, EN 61810-3)

Redundantní systémy

- Nezávislost mezi procesními kanály (výměna dat, napájení)
- Defenzivní (bezpečná) komparace výstupů

Reakční systémy

- Důkaz přijatelné SDT pro každé rozhraní (mitigace)
- Nezávislost mezi procesním kanálem a dohledovým prvkem

SIEMENS

Požadavky zákazníků

Typické současné zadání:

- Nízké THR nezávislé na konfiguraci
- Dlouhé test intervaly
- Vysoká pohotovost (tolerance poruchy do opravy, rychlost opravy)
- Škálovatelnost instalace (omezení velikosti minimální instalace)
- Rozsáhlá diagnostika
- Zpětná kompatibilita s nahrazovanými systémy
- V souladu s CRA

SIEMENS

Realita vývoje

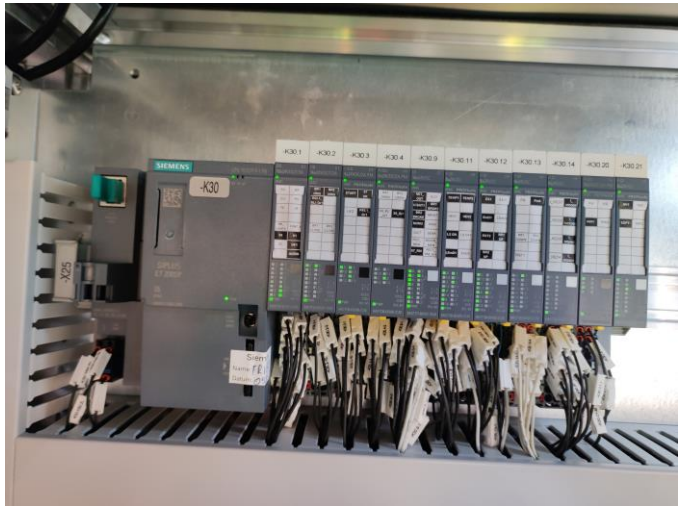
Bolesti vývojáře (architekta)

- Zákazník zná požadovaný SIL ale není schopen definovat funkci (minimální kritéria úspěchu)
- THR vs. MDT
- Jednoduchý vs. Bezúdržbový
- Nutnost integrovat existující komponenty, často bez existujících CENELEC důkazů bezpečnosti
- Každý provozovatel má jiné provozní předpisy a přístup
- Schvalovací proces v SAC (EBA - Německo)

SIEMENS

Shrnutí aktuálního stavu

- Konstantní tlak na snižování alokovaného THR/TFFR
- Velmi pomalé sjednocování THR požadavků mezi zeměmi (technická historie vetknutá do národních analýz rizik hraničící s protekcionismem)
- V roce 2027 začíná platit CRA (Akt o kybernetické odolnosti -> zvyšující se komplexnost systémů - > extrémní potenciál pro vygenerování plošného výpadku (vazba na centrální infrastrukturu)



SIEMENS

Kontakt

Luboš Piterka
RAMS Manager

SMO RI LCE CZ HW RAMS
Anglické nábřeží 2434/1
301 00 Plzeň, Česká Republika
Mobile: +420 727 897 640

E-mail lubos.piterka@siemens.com

SIEMENS