Autorizujeme budoucnost

Zpracoval: Ing. Jaroslav Brabec, Ph.D.
Dne: 11/2023/ rev. 01

VÝZKUMNÝ ÚSTAV ŽELEZNIČNÍ, a. s.

Řádná péče v dodavatelském řetězci

Cíle udržitelného rozvoje OSN

Green deal

Balíček Fit for 55

...
TCFD
NFDR
SFDR
Taxonomy
CSRD
ESRS
ESG
...

NIS 2

ECM
ISO
....

IFRS

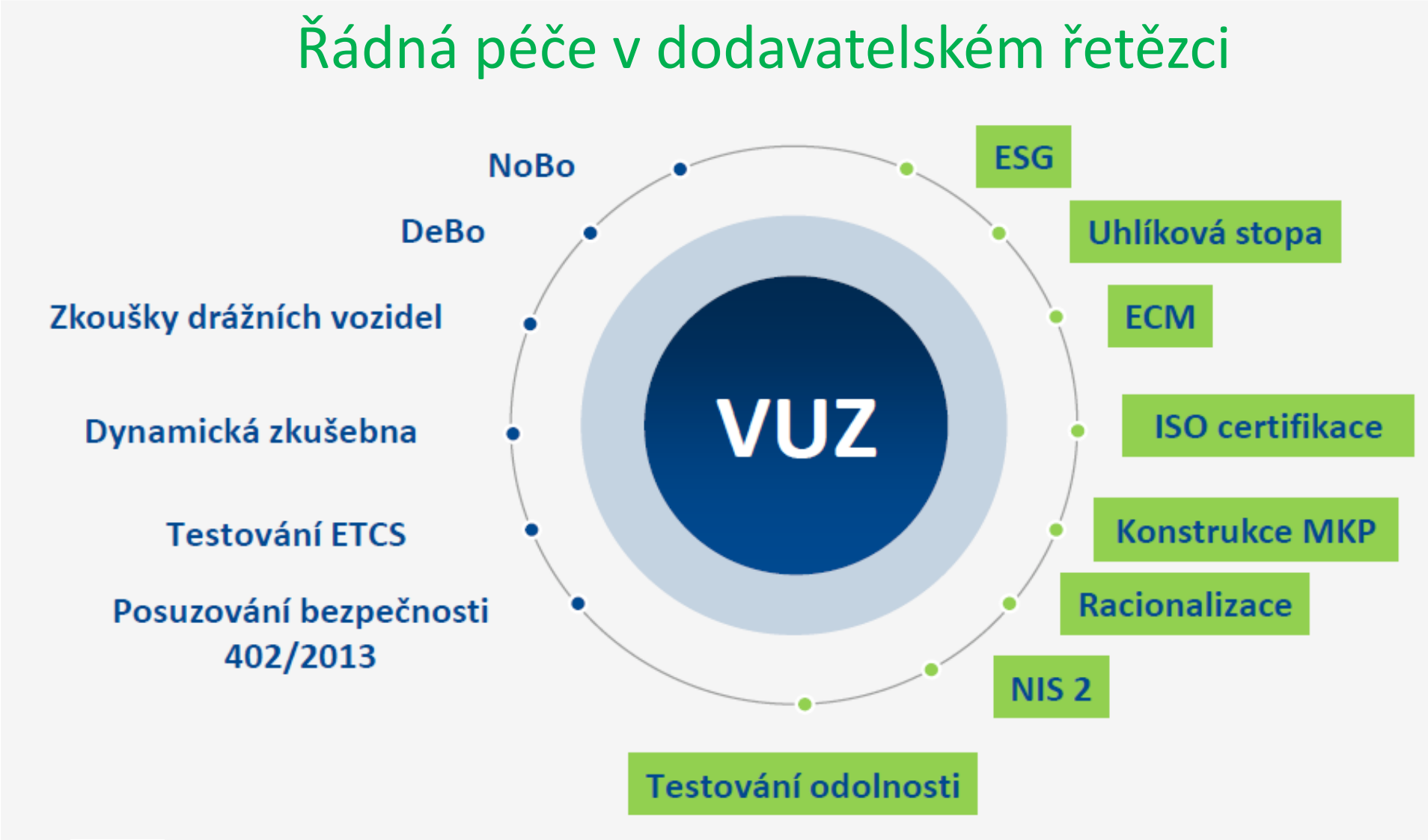
CSDDD

Řádná péče v dodavatelském řetězci

Zavádí požadavky na společnosti, aby identifikovaly a předcházely, ukončily nebo zmírnily skutečné a potenciální dopady svých činností

Ukládá povinnost provádět „due diligence“ nejen o svých vlastních provozech, ale i o aktivitách jejich dceřiných společností a **dalších subjektů v jejich hodnotových řetězcích, se kterými mají přímé i nepřímé navázané obchodní vztahy**

Produkty VUZ



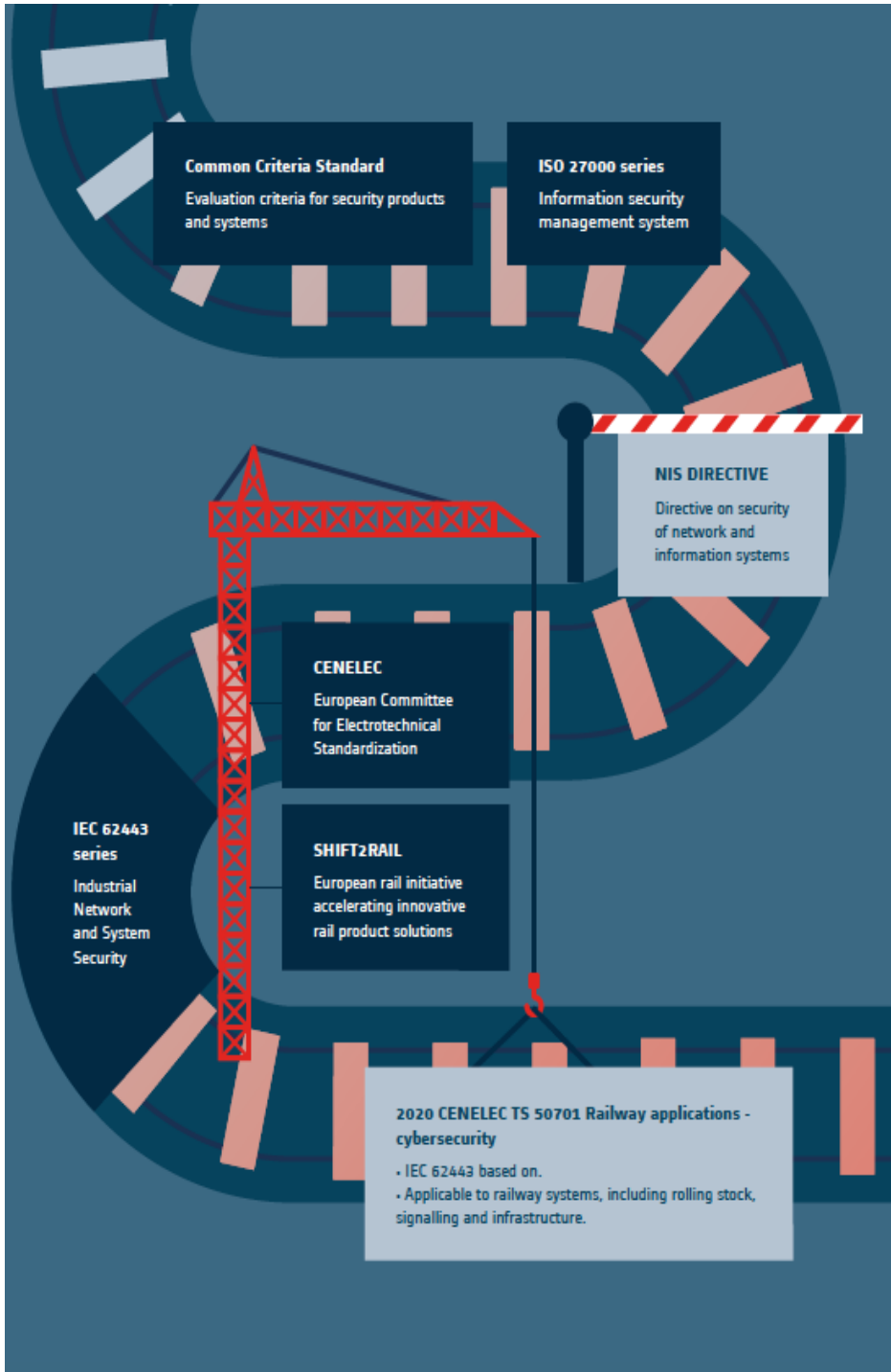
Kybernetika – testování ŽKV

VUZ od roku 2021 nabízí produkt **Testování Kybernetické bezpečnosti.**

Testujeme na základě vlastní Metodiky testování odolnosti drážních technologií a kolejových vozidel proti kybernetickým útokům.

Metodika je založena na průmyslových standardech (ISA / IEC 62443), standardech bezpečnosti informací (řada ISO 27000) a na doporučeních nejlepších bezpečnostních postupů (NIST SP800-82).

Na praktickém testování jsme prokázali plnou funkčnost navrhované metodologie.



Kybernetika – testování ŽKV

V roce 2024 vstoupí v účinnost nová **evropská směrnice NIS 2.**

Určuje nová pravidla při řešení kybernetické bezpečnosti uvnitř subjektů.

Implementace NIS 2 bude povinná, maximální pokuta za její nedodržení bude 10 000 000 Kč, nebo 2 % z celkového celosvětového ročního obratu společnosti.

Doprava (letecká, **železniční**, vodní a silniční) je zahrnuta mezi **subjekty zásadního významu.**

Kybernetika – testování ŽKV

Testujeme : Infrastrukturu

Vozidla ŽKV (například Pendolina, vozy Sysel a další)

Součást testů:

- seznámení se s dokumentací
- kompletní prohlídka vozidla
- testování
- vytvoření metodiky
- vypracování zprávy

Kybernetika – testování ŽKV

Testování odolnosti systému Telerail

Penetrovali jsme systém přímo ze stojícího a jedoucího vozu.
Testování probíhalo několik dnů a výstupem byla zpráva s výsledky testů a doporučení.

Testováním jsme přišli na mnoho bodů k nápravě.

Výsledkem testování byly např. opatření k zamezení zastavení vozidla.

Kybernetika – testování ŽKV

Crash řídícího počítače

Opakované zahlcení řídícího počítače dotazy (např. ping) vede k jeho pádu / restartu.

Doporučení: segmentace sítě a dostatečné oddělení vlakových komponent od internetu

1345/2000	z	29.07.'23 18:19:47,985	Ztráta komunikace s IS JCA	D_JCA_SlaveState_E=0
1346/2000	v	29.07.'23 18:41:30,546	Porucha nabíječe	BU_CZE_PorDocDC12=1,BU_CZE_PorTrvDC12=1
1347/2000	v	29.07.'23 18:41:30,546	Porucha střídače 2	BU_CZE_PorDocSt2=1,BU_CZE_PorTrvSt2=1
1348/2000	v	29.07.'23 18:41:30,546	Porucha střídače 1	BU_CZE_PorDocSt1=1,BU_CZE_PorTrvSt1=1
1349/2000	v	29.07.'23 18:41:30,546	Porucha VN měniče	BU_CZE_PorDocVNm=1,BU_CZE_PorTrvVNm=1
1350/2000	v	29.07.'23 18:41:30,546	Interní porucha komunikace CZE	BU_CZE_CAN_ERR=1,BU_CZE_VNm_CAN_ERR=1,BU_CZE_St1_CAN_ERR=1,BU_CZE_St2_CAN_ERR=1,BU

Kybernetika – testování ŽKV

Navržená opatření:

- Provedení penetračních testů z a do vlaků na úrovní IP sítí a systému Telerail.
- Nastavení segmentů sítě, které odizolují systém Telerail.
- Nastavení MFA pro přístup k systému Telerail.
- Vypnutí nepotřebných služeb na periferních zařízeních uvnitř vlaku
- Prověření fungování řídícího počítače a jeho stability v případě nestandartní komunikace.

Kybernetika – testování ŽKV

Test zranitelnosti CAN zařízeni přes přímé připojeni do CAN počítačů ovládaní dveří

- Vyvolaní chybových hlášeni na ovladačích prvcích
- Crash ovládaní dveří
- Zablokovaní zavíraní dveří (potenciální zranitelnost)
- Ovládaní jednotlivých prvků
- Ovládnutím aplikace GPS na Telerailu (potenciální zranitelnost)

Kybernetika – testování ŽKV

Test CAN sběrnice plus řídicí počítač CAN na toaletě

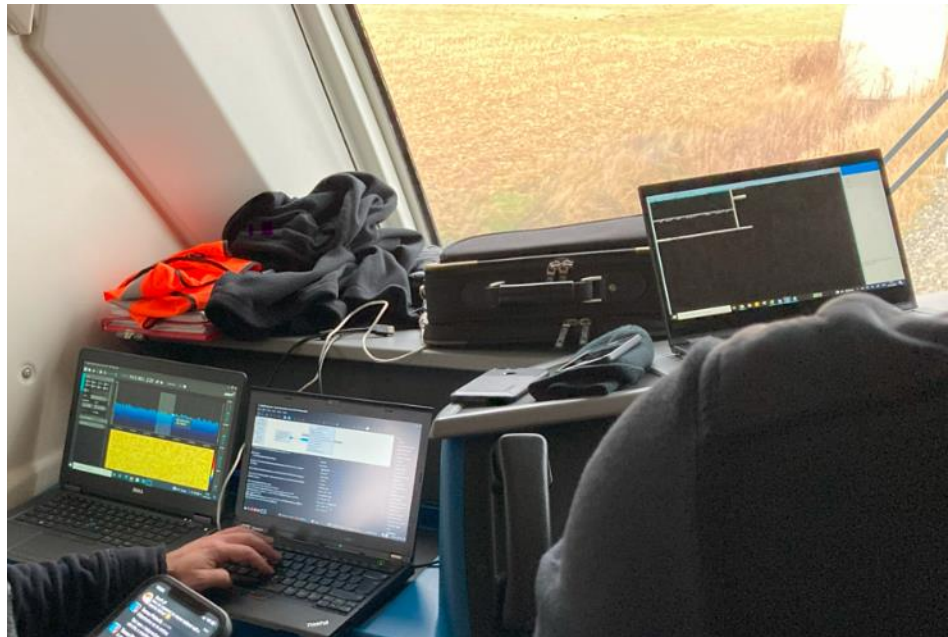
- Pomocí volání příkazů na CAN sběrnici se podařilo restartovat funkce toalety a vyvolat splachování.

- Dlouhodobé opakování této zranitelnosti může vést k poškození toalety a faktickému vyřazení vlaku z provozu.

Kybernetika – testování ŽKV

Test ECTS na lokomotivě Siemens Vectron

- Lokomotiva disponuje dvěma jednotkami pro příjem GSM-R signálu.
- Pomocí softwarově definovaného rádia a správně umístněné antény dojde k rušení signálu.
- Pokud je toto rušení delší než 18 vteřin, tak může dojít k vyřazení systému.



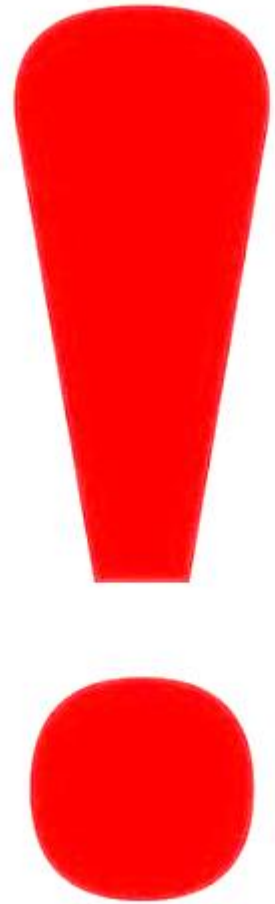
Kybernetika – testování ŽKV

Testování zachycení IMSI jednotlivých SIM ve vlaku

- Pomocí modifikovaného softwarového rádia bylo možné zachytit a odposlechnout IMSI jednotlivých SIM karet používaných při komunikaci v rámci GSM-R sítě.
- Při znalosti IMSI SIM karet je možné provést IMSI datach útok, který odpojí dané zařízení od sítě a znemožní se mu znovu připojit.

Kybernetika – testování ŽKV

- Při každém testu se odhalí slabé stránky a možné chyby, přes které se hacker může dostat do sítě a zaútočit.
- Na základě testů se může zajistit zlepšování a odstraňování potencionálních kritických míst.
- Jestliže sítě nejsou řádně zabezpečeny, mohou být bránou pro kybernetické útoky, které mohou mít katastrofální důsledky – od krádeže citlivých informací až po rozsáhlé výpadky služeb.



Kybernetika – testování ŽKV

Je v zájmu každé společnosti chránit svá aktiva a zajišťovat, že její technologická infrastruktura je bezpečná a funkční.

Ten, kdo pravidelně netestuje vlastní sít vystavuje společnost obrovskému riziku a tím jí poškozuje.

Standardizace v oblasti IT (směrnice, předpisy, rizika, proces zlepšování, standardizace zálohování a jiné) je dnes základní kámen k ochránění aktiv a know-how.

Nálezy prokazují zásadní nedostatky v SW a HW infrastruktuře dopravních prostředků a infrastruktury, na které jsou provozovány. **Doporučuje se provádět pravidelné a časté testování všech prvků dopravní infrastruktury a vozidel.**

Kybernetika – testování ŽKV

Požadavek na standardizaci a zlepšování v oblasti Kybernetiky

Nejenom požadavky NIS2:

- stanovit rozsah řízení kybernetické bezpečnosti,
- zavádět bezpečnostní opatření,
- hlásit kybernetické bezpečnostní incidenty,
- informovat zákazníky o incidentech a hrozbách,
- provádět protiopatření,
- plnit povinnosti mechanismu řízení bezpečnosti dodavatelského řetězce.

Nepřinášíme poradenské papíry – **přinášíme změnu**

Děkuji za pozornost

brabecj@cdvuz.cz