SYNERIQ

Bezpečnost, design a rozumné provozování kritické komunikační infrastruktury.

Ing. Jiří Kasner, MBA
jiri.kasner@syneriq.cz

Konference SCADA Security 2026
25. března 2026

Belden | HIRSCHMANN A BELDEN BRAND | NET MODULE A BELDEN BRAND

Nač se postupně podíváme (V 409/2025 Sb.)

§ 27

Zabezpečení průmyslových, řídicích a obdobných specifických technických aktiv

Povinná osoba včetně požadavků uvedených v § 3 až 26 pro zajištění kybernetické bezpečnosti průmyslových, řídicích a obdobných specifických technických aktiv dále využívá nástroje a zavádí bezpečnostní opatření, která zajistí

a) omezení fyzického přístupu k průmyslovým, řídicím a obdobným specifickým technickým aktivům,

b) omezení oprávnění k přístupu k průmyslovým, řídicím a obdobným specifickým technickým aktivům,

c) segmentaci a oddělení komunikačních sítí průmyslových, řídicích a obdobných specifických technických aktiv od jiných prostředí a segmentaci a oddělení těchto komunikačních sítí podle § 18,

d) omezení vzdálených přístupů a vzdálené správy průmyslových, řídicích a obdobných specifických technických aktiv, včetně omezení komunikace mimo komunikační síť povinné osoby,

e) ochranu jednotlivých průmyslových, řídicích a obdobných specifických technických aktiv před využitím známých zranitelností a hrozeb a

f) dostupnost a obnovu průmyslových, řídicích a obdobných specifických technických aktiv pro zajištění dostupnosti regulované služby.

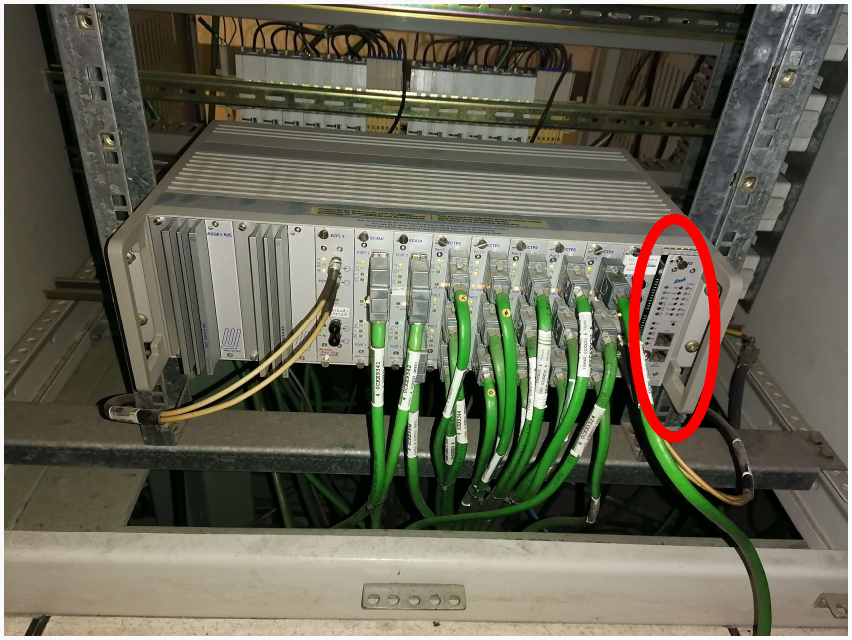
A malá poznámka:

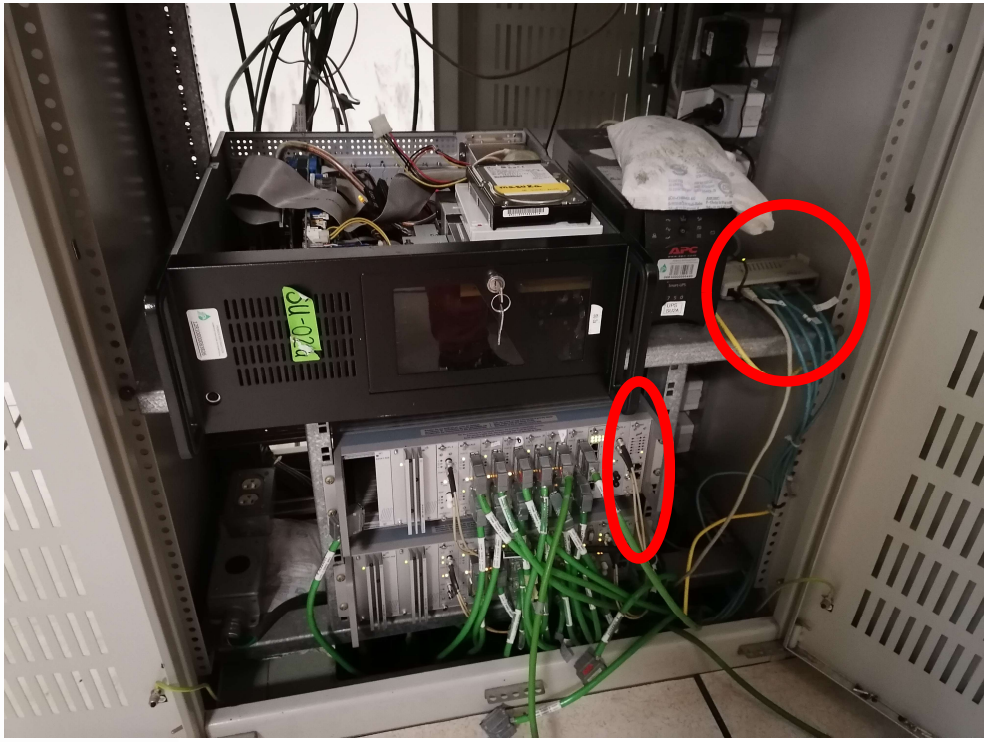
- OT se týkají i §§ 3-26,
- my se podíváme na body od §17 dál (technická opatření),
- je třeba vše integrovat do svých ISMS,
- pozor na BCM, lidi, audity, údržbu, …

Asi je to jasné, raději doplňuji jako poznámku.

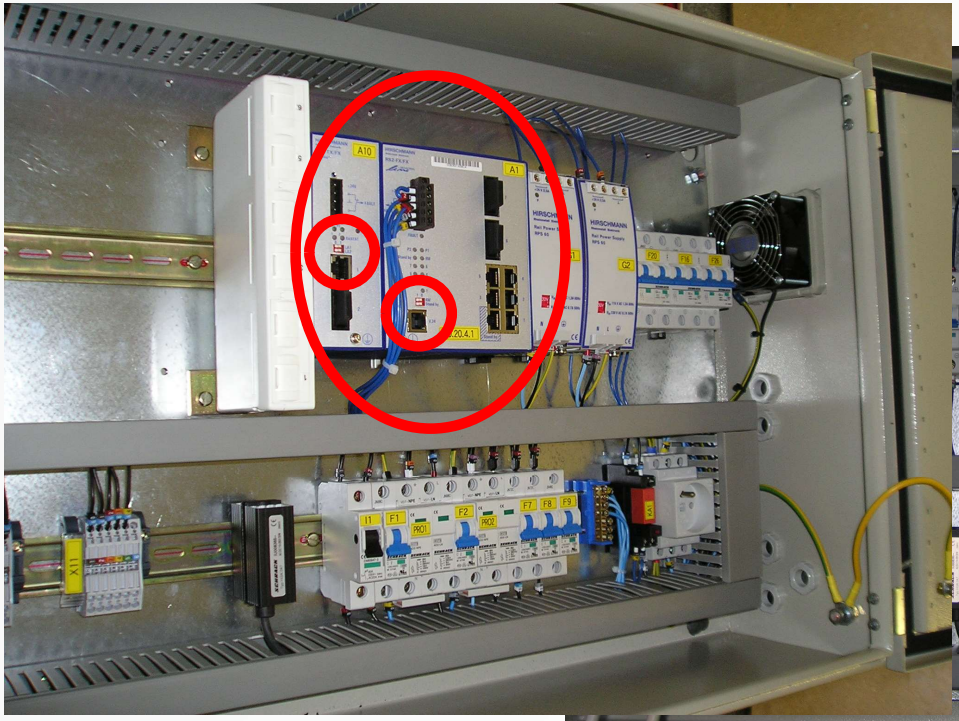
SYNERIQ Belden | HIRSCHMANN A BELDEN BRAND NET MODULE A BELDEN BRAND

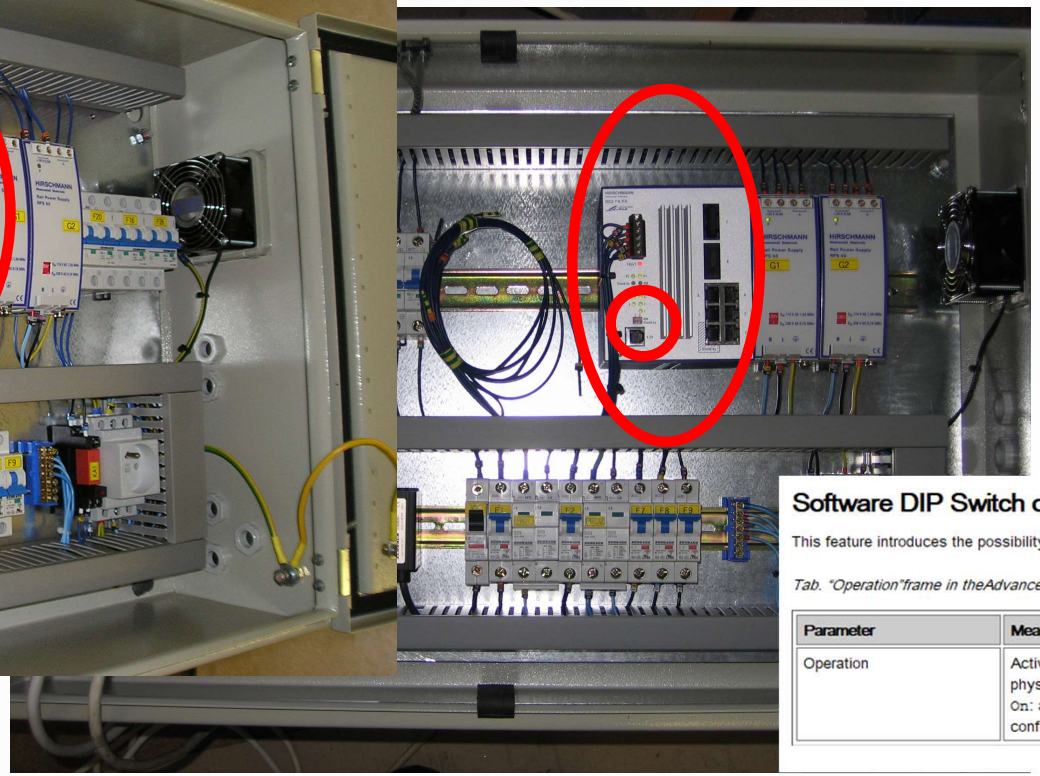
Fyzická bezpečnost a její problémy.

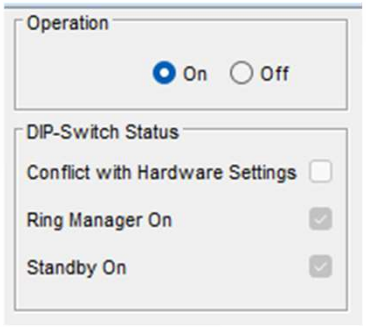




Fyzická bezpečnost a její problémy.







Software DIP Switch overwrite (MICE, PowerMICE and RS)

This feature introduces the possibility to disable the DIP switches using software.

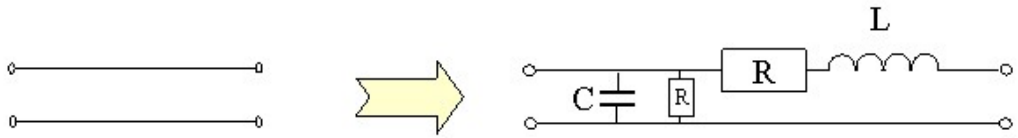
Tab. "Operation" frame in the Advanced:DIP-Switch dialog

Parameter	Meaning	Value range	Default setting
Operation	Activates/deactivates the DIP switches physically located on the device. `On`: activates hardware DIP switch configuration	`On`,`Off`	`On`

SYNERIQ Belden | HIRSCHMANN A BELDEN BRAND NET MODULE A BELDEN BRAND

Fyzická komunikační cesta – vlastnosti.

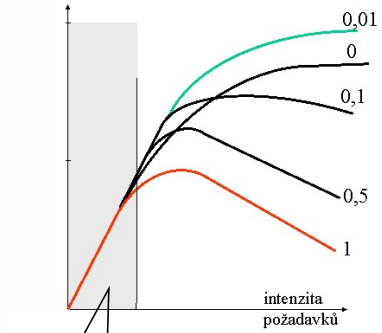
- Neexistuje ideální přenosová cesta.
  - Útlum.
  - Zkreslení.
  - Přeslech.
  - Rušení, vyzařování.
- Každá přenosová cesta se chová k signálům jinak a je třeba s tím počítat.
- Záleží na frekvenci a charakteru signálu.
- Otázkou je, co se signálem, který už je ve stavu, že danou cestou jej nemá smysl přenášet, ale třeba by to šlo jinou …



SYNERIQ Belden | HIRSCHMANN A BELDEN BRAND NET MODULE A BELDEN BRAND

Chování jako bezpečnostní vlastnost.

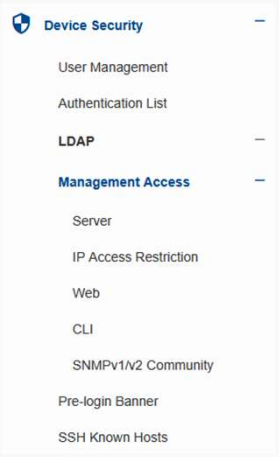
- Ethernet byl navržena jako 1-perzistentní síť.
- Z grafu je sice zřejmé, že nejhůře zatěžuje síť (sdílené médium) – ale pouze za předpokladu, že bude hodně zatížena.
- Proč byla zvolena 1-perzistentnost.
  - Předpokládal se poměrně slabý provoz.
  - Zohlednila se i latence přenosu.
    - 1-perzistence nevzdává zbytečně.
    - Uzel se od okamžiku, kdy chtěl začít vysílat dostane na médium celkem rychle.



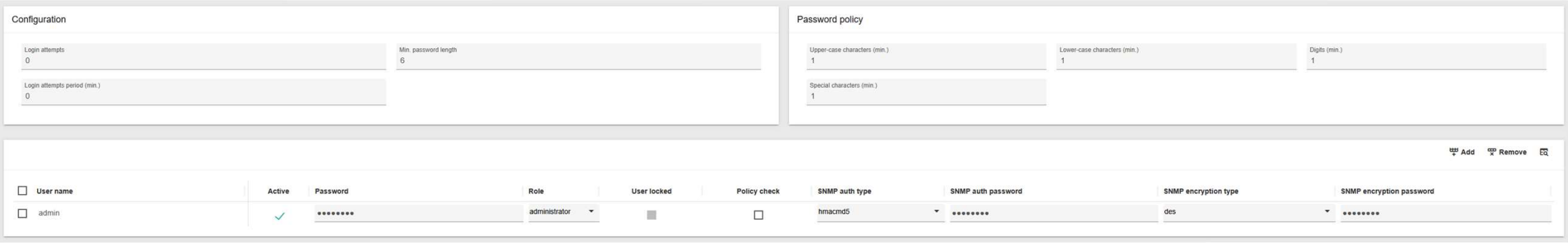
Oblast využití sítě (oblast nízkého vytížení sítě)

SYNERIQ Belden | HIRSCHMANN A BELDEN BRAND NET MODULE A BELDEN BRAND

Omezení oprávnění.



- Musí navazovat na celkovou strategii pro oprávnění a přístupy.
- Často se diverzifikuje výrobce nebo se řeší lokálně.
- Důležité definice rolí – dle zvyklostí u ostatních §§ (netřeba často vymýšlet kolo).
- Co když to tak nejde?



SYNERIQ Belden | HIRSCHMANN A BELDEN BRAND NET MODULE A BELDEN BRAND

Omezení dalších rizik z toho plynoucích.

- Přístupy k zařízení různými protokoly – často bez zabezpečení ☹
- Časová synchronizace – proč a jak.
- Využití a stavy portů – dokumentace (on-line?).
- Sběr provozu a analýza.
- VPN k přístupu do managementu?
  - Jak se na tohle tvářit?
  - Co vlastně potřebujete ověřit na konci VPN?
  - Řízený dodavatel a jeho důvěryhodnost?
  - Obecný postup u vzdálených přístupů a jeho bezpečnost.

Type	Status	Name	Default Pas...	HiDiscovery	Telnet	SSH V1	Tftp	Http	SNMP V1/V2	Profinet IO	IEC61850	Ethernet/IP	Time Synch...	Unused Acti...	Restricted ...	802.1X Port...	Inbound AN...	Outbound ...
—	⚠	192.168.173.132	⚠	⚠	🔒	🔒	🔒	⚠	🔒	🔒	🔒	🔒	⚠	⚠	⚠	⚠	🔒	🔒
—	⚠	192.168.173.133	⚠	⚠	🔒	🔒	🔒	⚠	🔒	🔒	🔒	🔒	⚠	⚠	⚠	⚠	🔒	🔒

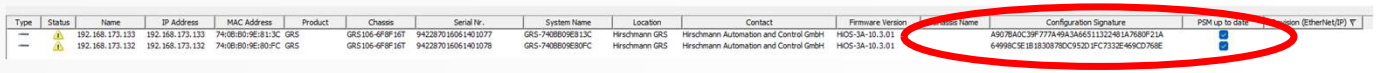
SYNERIQ Belden | HIRSCHMANN A BELDEN BRAND NET MODULE A BELDEN BRAND

Segmentace a vnitřní struktura sítě.

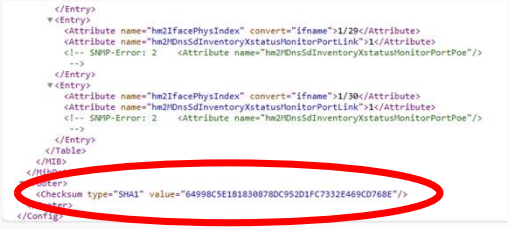
- L2 x L3?
  - Rizika.
  - Výhody a nevýhody obou řešení.
- Jak u datových prostupů v síti?
  - Analýza potřeby a rizika z toho plynoucí.
- Co se staršími zařízeními a jejich chováním (FDX, 10Mbps)?
  - Kolize CSMA/CD? Zná to ještě vůbec někdo? A že jich pořád žije…
- Vazby na dohled nad sítí.
  - Management VLAN a podobně.
  - Máme vše v ruce?

Technická aktiva a jejich parametry.

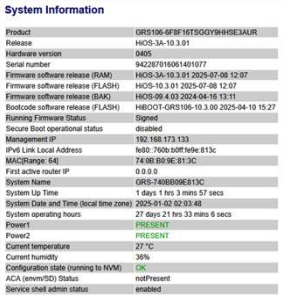
- Je zcela zásadní mít v ruce správné informace o aktivech a jejich parametrech.
- Parametry musí vycházet z návrhu a korespondovat s dokumentací.
- A je dobré vědět, co máte vlastně v ruce.
- Jak tohle hlídat?



Type	Status	Name	IP Address	MAC Address	Product	Chassis	Serial Nr.	System Name	Location	Contact	Firmware Version	Chassis Name	Configuration Signature	PSM up to date	Revision (EtherNet/IP)
—	⚠	192.168.173.133	192.168.173.133	74:08:B0:9E:81:3C	GRS	GRS106-6F8F16T	942287016061401077	GRS-740BB09E813C	Hirschmann GRS	Hirschmann Automation and Control GmbH	HiOS-3A-10.3.01		A9078A0C39F777A49A3A6651132248	☑	
—	⚠	192.168.173.132	192.168.173.132	74:08:B0:9E:80:FC	GRS	GRS106-6F8F16T	942287016061401078	GRS-740BB09E80FC	Hirschmann GRS	Hirschmann Automation and Control GmbH	HiOS-3A-10.3.01		64998C5E1B1830878DC952D1FC7332E469CD768E	☑	



```
    </Entry>
  ▼<Entry>
      <Attribute name="hm2IfacePhysIndex" convert="ifname">1/29</Attribute>
      <Attribute name="hm2MDnsSdInventoryXstatusMonitorPortLink">1</Attribute>
      <!-- SNMP-Error: 2    <Attribute name="hm2MDnsSdInventoryXstatusMonitorPortPoe"/>
       -->
    </Entry>
  ▼<Entry>
      <Attribute name="hm2IfacePhysIndex" convert="ifname">1/30</Attribute>
      <Attribute name="hm2MDnsSdInventoryXstatusMonitorPortLink">1</Attribute>
      <!-- SNMP-Error: 2    <Attribute name="hm2MDnsSdInventoryXstatusMonitorPortPoe"/>
       -->
    </Entry>
  </Table>
 </MIB>
</Adapter>
<Checksum type="SHA1" value="64998C5E181830878DC952D1FC7332E469CD768E"/>
</Config>
```



System Information

Product	GRS106-6F8F16TSGQY9HHSE3AUR
Release	HiOS-3A-10.3.01
Hardware version	0405
Serial number	942287016061401077
Firmware software release (RAM)	HiOS-3A-10.3.01 2025-07-08 12:07
Firmware software release (FLASH)	HiOS-10.3.01 2025-07-08 12:07
Firmware software release (BAK)	HiOS-09.4.03 2024-04-16 13:11
Bootcode software release (FLASH)	HiBOOT-GRS106-10.3.00 2025-04-10 15:27
Running Firmware Status	Signed
Secure Boot operational status	disabled
Management IP	192.168.173.133
IPv6 Link Local Address	fe80::760b:b0ff:fe9e:813c
MAC[Range: 64]	74:0B:B9:9E:81:3C
First active router IP	0.0.0.0
System Name	GRS-740BB09E813C
System Up Time	1 days 1 hrs 3 mins 57 secs
System Date and Time (local time zone)	2025-01-02 02:03:48
System operating hours	27 days 21 hrs 33 mins 6 secs
Power1	PRESENT
Power2	PRESENT
Current temperature	27 °C
Current humidity	36%
Configuration state (running to NVM)	OK
ACA (envm/SD) Status	notPresent
Service shell admin status	enabled

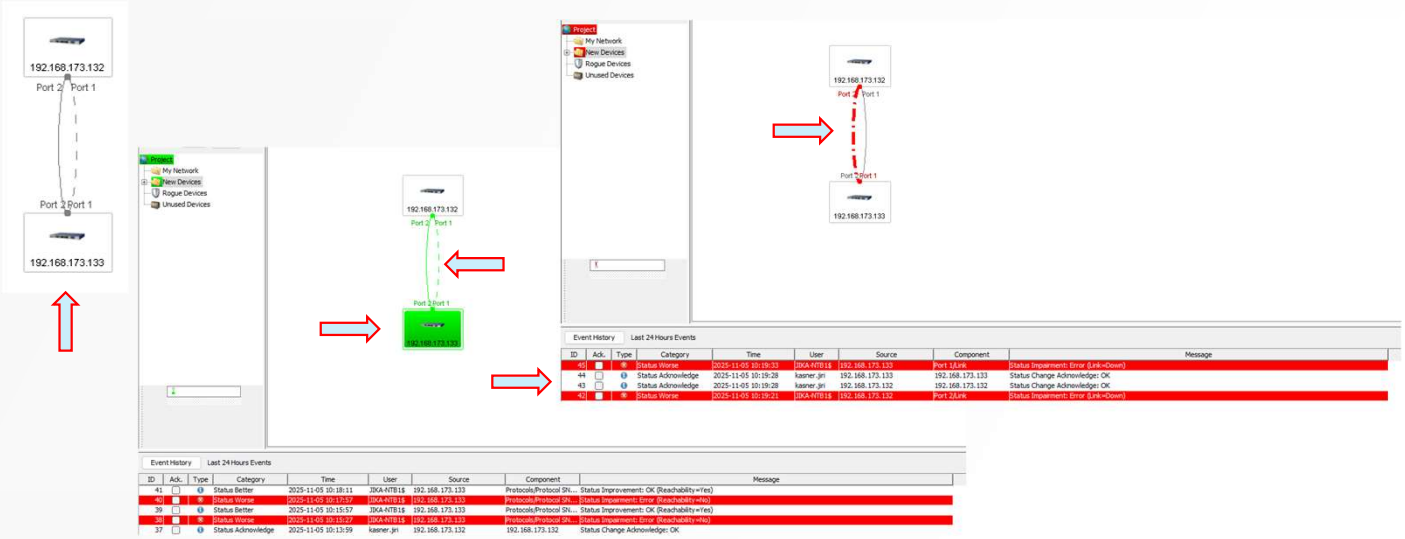
```
119: Notice Jan 2 2025 02:03:40 [0x00040003] CfgMgr Action copy script system remote result=ok user='admin' Ready
118: Notice Jan 2 2025 02:03:35 [0x00040003] CfgMgr Action copy config running-config remote result=ok user='admin' Ready
117: Notice Jan 2 2025 02:03:06 [0x00040003] CfgMgr Action copy script system remote result=ok user='admin' Ready
116: Notice Jan 2 2025 02:03:01 [0x00040003] CfgMgr Action copy config running-config remote result=ok user='admin' Ready
115: Notice Jan 2 2025 02:03:01 [0x001400c6] HTTP(S) Login via web interface successful for user 'admin', role 'Administrator', from '192.168.173.42'.
114: Notice Jan 1 2025 23:21:44 [0x00040003] CfgMgr Action copy script system remote result=ok user='admin' Ready
113: Notice Jan 1 2025 23:21:38 [0x001400c6] HTTP(S) Login via web interface successful for user 'admin', role 'Administrator', from '192.168.173.42'.
112: Notice Jan 1 2025 23:21:32 [0x00030004] SNMP Set by admin: sysContact.0 = Hirschmann Automation and Control GmbH
111: Notice Jan 1 2025 23:21:26 [0x00030004] SNMP Set by admin: hm2DevHpGetActionReset.0 = 1
110: Notice Jan 1 2025 00:00:25 [0x0001000b] System timezone offset changed from 0 to 60. Time is now 2025-01-01 01:00:25.
109: Info Jan 1 2025 00:00:22 [0x00790009] Signed firmware infrastructure successfully installed.
108: Notice Jan 1 2000 00:00:33 [0x0001000a] System time set to 2025-01-01 00:00:00.
107: Notice Jan 1 2000 00:00:33 [0x0003001d] Selected firmware HiOS-3A-10.3.01 build 2025-07-08 12:07.
106: Notice Jan 1 2000 00:00:33 [0x0003000a] System started.
105: Emergency Jan 4 2025 02:56:55 [0x00010004] System power is failing.
```

SYNERIQ Belden

Dohled a sledování provozu.

- Dohled je u redundantních systémů podstatnou částí nasazení a provozování KKI.
- Typicky je nasazen na společných velínech, dozornách a podobně, přičemž velínář je první linie detekce chyby a následně musí pokračovat procesy incident response a další.
- Sledování provozu a chování systému jako celku je podstatné z důvodu zátěží, nastavení sond pro IDS a podobně.
- Provozní stav by měl projít důkladnou analýzou provozu, aby bylo jasné a jisté, že provozní stav je ten správný startovací a cílový stav.

Dohled a sledování provozu.



Zranitelnosti a postupy s tím související.

- Každý výrobce by měl sledovat zranitelnosti svých zařízení a dodávat o tom informace.
- Každá zranitelnost pro uživatele představuje různě podstatné či nepodstatné ohrožení.
  - Není třeba obvykle bláznit.
  - Je moudré mít svoje testovací pracoviště + znalé vlastní pracovníky + řízeného bezpečného dodavatele.
  - Ne každá zranitelnost automaticky znamená nějakou akci nebo nutný zásah (tím méně krizový).
  - Často se u průmyslových systémů stává, že rozhodnutí o opravě zranitelnosti přijde v nesmyslný okamžik nebo v rámci hurá akce, která nadělá více škody než užitku. Toto je nutné pečlivě vážit.

Zranitelnosti a postupy s tím související.

Dobrý den,

zasíláme informace z oblasti sledování bezpečnostních hrozeb a postupů komponent HIRSCHMANN.

1. Nové zranitelnosti.
   a. V období 01-02/2025 nebyly výrobcem reportovány žádné nové známé zranitelnosti.

2. Nové informace ohledně software.
   a. Výrobce uveřejnil novou stránku k zajištění dostupnosti software HiOS vč. starších verzí na https://www.doc.hirschmann.com/releasemap.html?filter=undefined
   b. Nové verze software:
      i. HiOS generace 10 (10.0.02 pro GRS/BRS ze dne 11.2.2025) - zde doporučuji zvážit provedení upgrade kvůli opravám v řádku 649, 651, 661, 663 – viz příloha,
      ii. Classic generace 9 (09.1.15 ze dne 14.2.2025) – zde doporučuji zvážit upgrade z důvodů funkčních oprav – viz příloha,
      iii. HiSecOS – upgrade na verzi 05.1.01 (ze dne 17.2.2025) – zde obecně doporučujeme upgrade na generaci software 5 – se zvážením funkčnosti, jedná se o nekritické opravy.
      iv. Vše k dispozici na stránkách podpory https://hirschmann-support.belden.com/en-US

Všechna doporučení musí podléhat úvaze provozovatele systému dle konkrétní bezpečnostní strategie a provozní situace konkrétního projektu, z naší strany se jedná o obecná doporučení po našich interních testech!

HIRSCHMANN
A BELDEN BRAND

List of issues
HiOS

ID	Since	Fixed in	Variant	Description	Workaround	Correction
1	05.0.00	05.0.01	2A 3A 3S	The operator for TCP/UDP Ports of an existing ACL rule cannot be changed to "eq".	Delete the rule and recreate it with the operator "eq".	Fixed in release 05.0.01.
2		04.0.02	EES RSP RSPE RSPS	PRP dialog is missing in web interface.	-	Fixed in release 04.0.02.
	01.0.00	No fix	EES EESX GRS1020_1030 RED RSPL	The management agent is reachable with untagged packets, even the VLAN acceptable frametype is set to tagged frames only (admitOnlyVlan).	-	Hardware related limitation.
						Fix in release 05.0.00.
						No fix planned.
						Fix planned in future release.

Belden

Belden Security Advisory
PSIRT-2

Web Interface Vulnerability in HiOS

Date: 2025-10-09
Version: 1.0

Summary

A vulnerability has been identified in the HiOS Switch Platform where an HTTP GET request to a specific endpoint causes the device to perform a reboot.
The severity is rated Critical with a CVSS v3.1 score of 9.3. [1]

Affected Products

Brand	Product Line	Version(s)
Hirschmann	HiOS Switch Platform	Since 09.1.00

Mitigation

Hirschmann – HiOS Switch Platform

Update to version 09.4.05, 10.3.01 or higher.

Zranitelnosti a postupy s tím související.

Certificate

Cyber Security Management

Certificate No. 968/CSM 120.01/24

Certificate Holder: BELDEN Inc.
1 N. Brentwood Blvd., 15th Floor
St. Louis, MO 63105
USA

Certified Locations(s): see certificate appendix

Scope of Certification: IEC 62443-4-1:2018 (Edition 1.0)
Security for industrial automation and control systems –
Part 4-1: Secure product development lifecycle requirements

The certified company has successfully demonstrated that their Security Development Lifecycle "Agile Product Development Process" for product manufacturers complies with the applicable requirements of the standard IEC 62443-4-1.

The organization readiness to use the processes and procedures achieves:

Maturity Level 4: Improving

This certification refers to the company locations listed in the current appendix to the certificate.

Validity: This certificate is valid until 2027-08-13

Cologne, 2024-08-13 Dipl.-Ing. (FH) Sergei Biberdorf

TÜV Rheinland Industrie Service GmbH
Bereich Automation
Funktionale Sicherheit
Am Grauen Stein, 51105 Köln

www.fs-products.com
www.tuv.com

TÜVRheinland®
Precisely Right.

Certificate

No.: 968/CSP 1040.00/25

Product tested: Industrial Switch
Certificate holder: BELDEN Inc. 1 N. Brentwood Blvd., 15th Floor St. Louis, MO 63105 USA

Type designation: BOBCAT BRS-Family
OCTOPUS 8TX-EEC-M Family
BXS-Family

Codes and standards: IEC 62443-4-1:2018 (Edition 1.0) IEC 62443-4-2:2019 (Edition 1.0)

Intended application: The Industrial Switches BOBCAT BRS-Family, OCTOPUS 8TX-EEC-M Family and BXS-Family comply with the network requirements according to IEC 62443-4-1 and Security Level Capability 2 (SL-C:2) according to IEC 62443-4-2.

Specific requirements: The Industrial Switches BOBCAT BRS-Family, OCTOPUS 8TX-EEC-M Family and BXS-Family are only valid in the dedicated security context as documented in the user manuals.

The instructions of the associated user manuals released by manufacturer must be considered.

The current versions of the product are specified in the currently valid Revision List. The Revision List is released by the manufacturer in cooperation with the certification body.

Valid until 2030-07-17

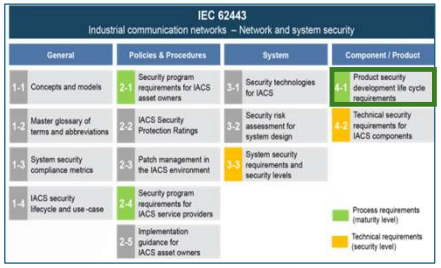
The issue of this certificate is based upon an evaluation in accordance with the Certification Program CERT CB1 V3.0:2021 in its actual version, whose results are documented in Report No. 968/CSP 1040.00/25 dated 2025-07-17. This certificate is valid only for products, which are identical with the product tested, issued by the certification body accredited by DAkkS according to DIN EN ISO/IEC 17065. The accreditation is only valid for the scope listed in the annex to the accreditation certificate D-ZE-11652-02-00.

TÜV Rheinland Industrie Service GmbH
Bereich Automation
Funktionale Sicherheit
Am Grauen Stein, 51105 Köln

Köln, 2025-07-17 Dipl.-Ing. (FH) Sergei Biberdorf
Certification Body Safety & Security for Automation & Grid

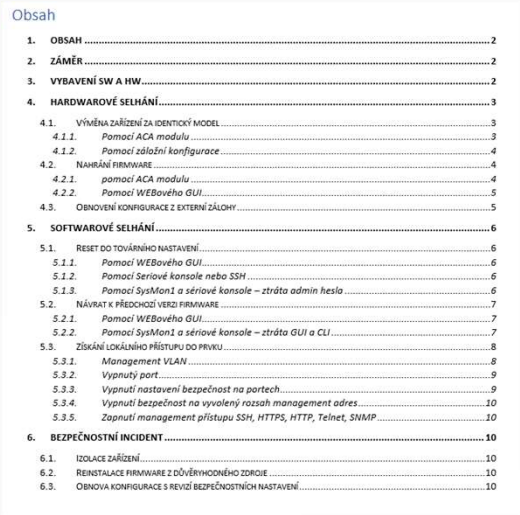
www.fs-products.com
www.tuv.com

TÜVRheinland®
Precisely Right.



SYNERIQ Belden | HIRSCHMANN A BELDEN BRAND NET MODULE A BELDEN BRAND

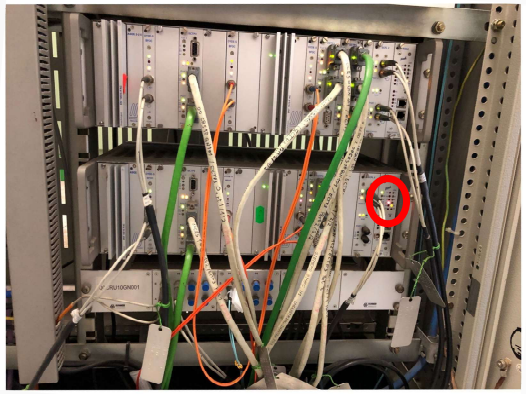
Postupy k dostupnosti a obnovení + IRP a DRP.

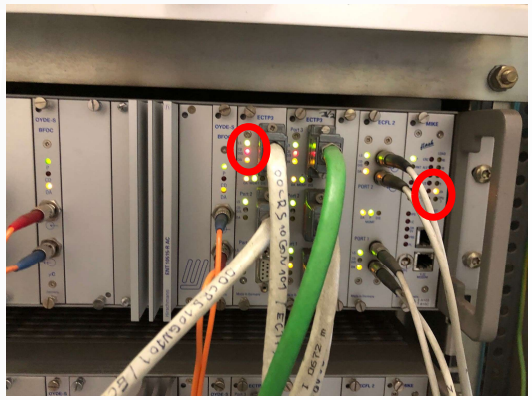


Obsah

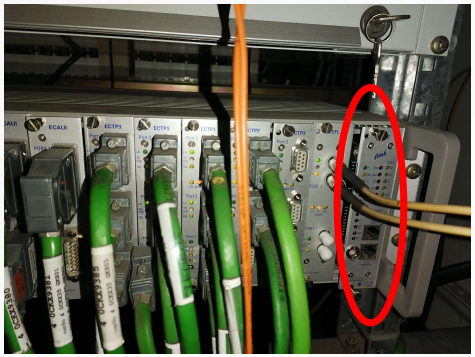
- IRP a DRP není neslušná zkratka.
- Incident může být i úplně normální porucha, se kterou si musí správce daného technického aktiva poradit.
- Je rozumné mít více úrovní reakcí na incidenty nebo zásadní poruchy systému.
- Startovacím bodem je typicky obsluha dohledového systému – velín, dozorna.
- A pár věcí k diskusi:
  - testovací pracoviště,
  - náhradní díly,
  - minimální provozní stav,
  - postupy obnovení.
- A poznámka – ne vždy je všechno hned a často hned znamená ve zmatku a s většími škodami – v průmyslu obzvlášť.

Jak ne #1

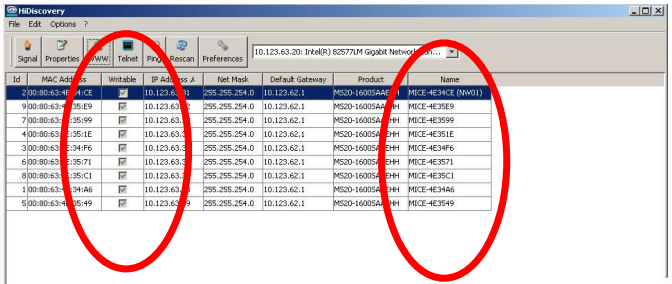


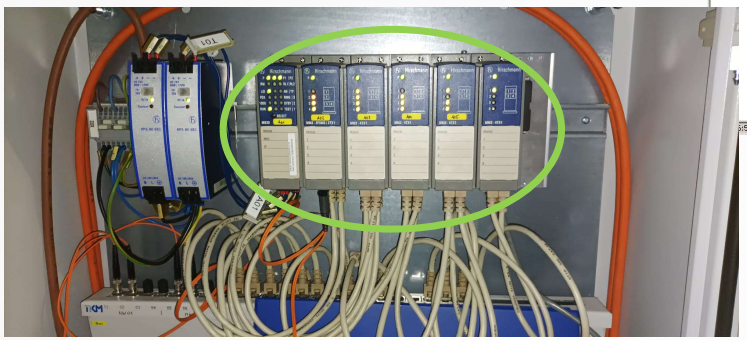


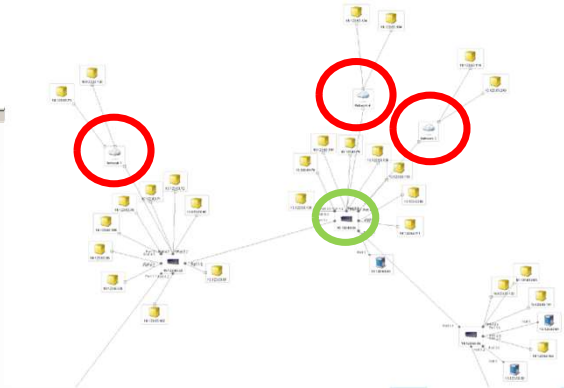
Jak ne #2



Jak ne #3


HiDiscovery
File Edit Options ?
Signal
Properties
HTTP
Telnet
Ping
Rescan
Preferences
Id
Writable
Net Mask
Default Gateway
Product
Name





Kontakt

Ing. Jiří KASNER, MBA
předseda představenstva

SYNERIQ, a.s.
Huťská 1294
272 01 Kladno

M +420 728 839 579
E jiri.kasner@syneriq.cz
W www.syneriq.cz