SLOVNAFT, A.S.
AND ACT 69/2018 ON CYBER SECURITY

Jana Puškáčová

IT Security Manager

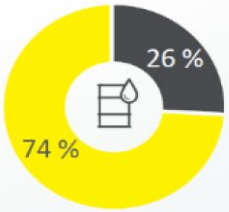
Slovnaft
MEMBER OF MOL GROUP

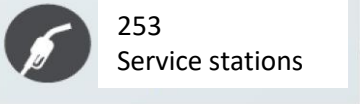
SLOVNAFT – Key Facts

- One of the biggest Slovak exporters and domestic investor
- APOLLO refinery – founded in 1895 - 1945
- SLOVNAFT – since 1946, one of the most complex petroleum refinery in Europe
- Member of MOL Group

Production

Sales





General information

Key Activities

Slovnaft
MEMBER OF MOL GROUP

Key Cyber Security Challenges of Industrial Control Systems *(2014)*

Confidence in Technology	• ICS technology historically not designed with security in mind • Selection of technology limited by ICS vendor offerings • Limited ability to intervene with parameters of deployed technology
Confidence in Systems	• Dependency on ICS systems fully operated by vendors • IT weaknesses relevant for ICS systems to be managed by ICS vendors
Confidence in Environment	• Lack of central visibility of isolated ICS systems • Lack of information on IT-related events happing in the ICS network
Confidence in Vendors	• High dependency on ICS vendors • Contracts with ICS vendors do not cover IT security requirements • Minimum IT security requirements not actively enforced
Confidence in People	• Engineers not trained in IT security • Engineers with limited knowledge on current IT threats for ICS

Slovnaft
MEMBER OF MOL GROUP

SLOVNAFT ICS Cyber Security Program Overview *(2016)*

Program Description

The objective of the SLOVNAFT ICS Cyber Security Program is to bring the cyber security of industrial control systems of SLOVNAFT to desired level. The program should deliver complex solution as a multiyear program with structured delivery and execution, consisting of several phases.

The Assessment Phase consists of 8 ICS cyber security projects and they should assess current status and propose how to close the most critical cyber security gaps in Slovnaft, a.s.

The expected deliverables of individual projects are defined for individual projects: ICS asset inventory including pilot, ICS network architecture design and implementation, ICS access and identity management, specialized ICS security awareness, ICS vulnerability and patch management, ICS procurement and third party risk management and policies development, ICS security incident management, ICS business continuity management

Business Benefits

- ICS assets identified, managed, monitored and their change under Slovnaft control
- Managing risk of users accessing the Slovnaft ICS infrastructure via proper authentication
- Managing risks related to network infrastructure reflecting the needs, security standards and ensuring the defence-in-depth security

Top Business KPIs

- Increased cyber security awareness for the whole ICS realm
- % of ICS systems managed by SLOVNAFT staff from security point of view
- Number of ICS cyber security events raised and resolved

Supported Business Strategy

- Deliver cyber security compliant ICS environment for safe, protected and reliable operations

Dependencies and Constraints

- Top management support
- Business user acceptance (e.g. of new processes)
- Vendor / 3rd party cooperation

Slovnaft
MEMBER OF MOL GROUP

SLOVNAFT ICS Cyber Security Program & Projects Addressing the Challenges

Project / Challenges	P1 ICS Asset Management	P2 ICS Network Architecture	P3 ICS Identity & Access Mgmt	P4 Security Awareness	P5 Vulnerability & Patch Mgmt	P6 Procurement & Vendor Risks
Technology	YES	YES			YES	YES
Systems	YES	YES	YES		YES	YES
Environment		YES	YES		YES	
Vendors	YES	YES	YES	YES	YES	YES
People			YES	YES		

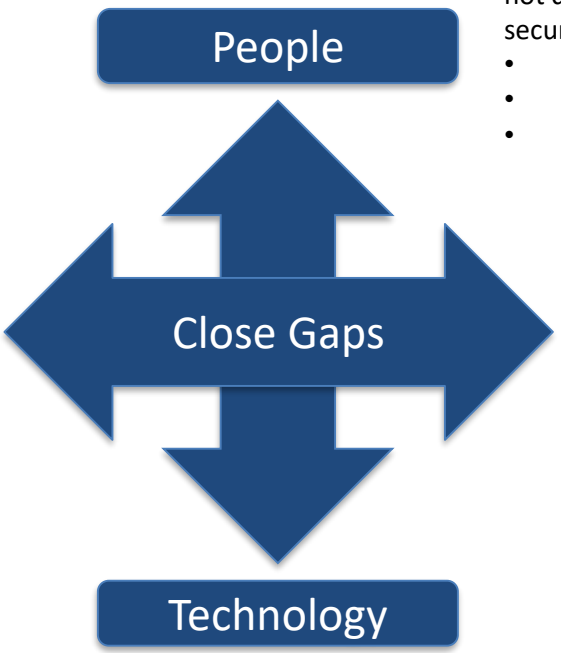
"Security Cycle"

P7
ICS Incident and Event Management

P8
ICS Business Cont. Management

Slovnaft
MEMBER OF MOL GROUP

How Closing of Identified Gaps Leads to Compliance with Act on Cyber Security



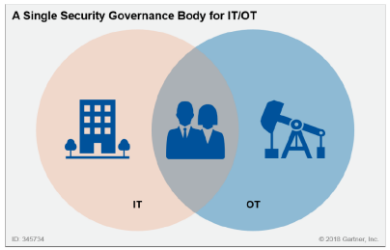
not dealing with cyber security at all and non cyber security experts, like

- Engineers
- ICS Vendors
- other 3rd parties

Governance

defines how people are organized:

- Integrated IT&ICS Cyber Security



- Technology operations model to manage Daily Use / RUN the business and CHANGE the Business and Technology

Tasks

supporting cyber security:

- review of access rights for ICS
- input and support for security awareness
- monitor status of vulnerability remediation, antimalware and patching
- report unusual events impacting their work also to IT security
- enforce Information Slovnaft Information Security Standards for ICS contracts
- involve security assurance in business projects
- ….

people should work with:

- ICS Configuration Management
- Asset Inventory Solution
- Threat Protection for ICS
- Security Architecture compliance
- ….

Slovnaft
MEMBER OF MOL GROUP

Essential Services of SLOVNAFT, a.s.

Business functions

Zákon o kybernetickej bezpečnosti:

- Storing of oil and refinery products
- Production of gasoline and diesel
- REACH chemicals production
- Refinery supervisory ICS
- Fuel pipeline to terminals
- Heat and energy production
- Waste water management
- Railway infrastructure operations
- Aviation fuel services at the airport

To be mapped

Prevádzka			Control room	DCS room	Control System
P1	BCDU6		SO3402	SO3402	Honeywell TDC
	BMFPU		SO5145	SO5145	Honeywell TDC
P2	BLGS1,2 BPPP1/4 BCSS BFGR2			SO6802 SO8804 SO7711 SO9808	Yokogawa Centum VP
	EXAR		SO5145	SO6208	Yokogawa Centum CS1000
	BSRU	SRU	SO571901	SO581802	Honeywell TDC
	BGRU1,2	DBP1,2		SO6731	
	BGDS1,2,3	OP1,2,3			
P3	BRHCK	RHC	SO571901	SO571102	Honeywell TDC
	BVGHT	VGH+HPP		SO561202	Honeywell TDC
	BADU5	AD5		SO5703	Honeywell Experion
P4	BFCCU	FCC	SO571901	SO661302	Honeywell TDC
	BGHCK	KHK	SO5609	SO5609	Yokogawa Centum VP
P5	BREFC BNHT4 BRRED BLNIS	CCR5 HRR4 RREF IZO	SO5433	SO5433	Honeywell TDC (Experion)
	BGHT7	HRP7	SO6518	SO6518	Honeywell TDC
	BAEDB	ARO	SO5433	SO5412	Honeywell Experion
	BNHT2+BKHT6	HRP2,6		SO5535	Honeywell Experion
	BGHT5	HRP5		SO5535	Yokogawa Centum VP (povodne C
EJ	BSC2	EJ2	SO8311	SO8506, SO8532	Honeywell TDC (Experion)
P7	BCACR	ÚKV	SO6404	SO6414	Foxboro IA 8.4.3
P8	BPE2	PE2	SO8311	SO8407	Honeywell TDC
	BPP3	PP3		SO8203	Honeywell Experion
	BPE4	LDPE4		SO7258	Yokogawa Centum VP
	BPE3	PE3		SO8414	Emerson DeltaV
					etylen mark VI
					ABB
					Emerson
					ABB
P*	safety bez				
*	logistika_				
	teplaren				
	schneider				

Production units & ICS Platforms

Mapped

Security Requirements

Antivirus
Patching
Backup & Recovery
...

Mapped

INFORMATION SECURITY STA[illegible]FOR CONTRACTUAL PARTNER OF SLOVNAFT, A.S.

These Information Security Standards for Contractual Partners of SLOVNAFT, a.s. (hereinaf[illegible] referred as "the Standards") contain a list of security controls and measures that all Contra[illegible] Partners of SLOVNAFT, a.s. are required to adopt and must apply to:

a) third party equipment accessing the environment of SLOVNAFT, a.s. via VPN access

b) [illegible]

c) [illegible]

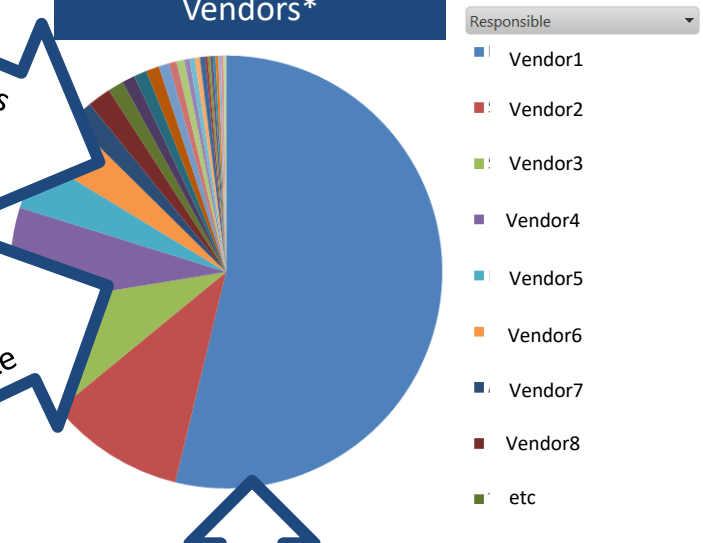
d) [illegible]

Vendor Contracts

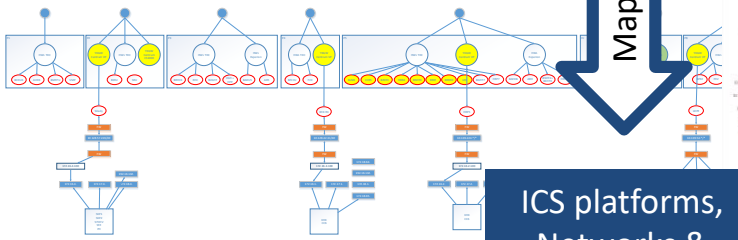
Real status reviews

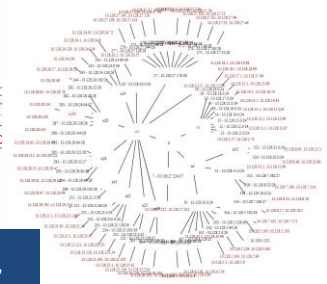
Reviewed In Update

Responsible Units and Vendors*



Mapped

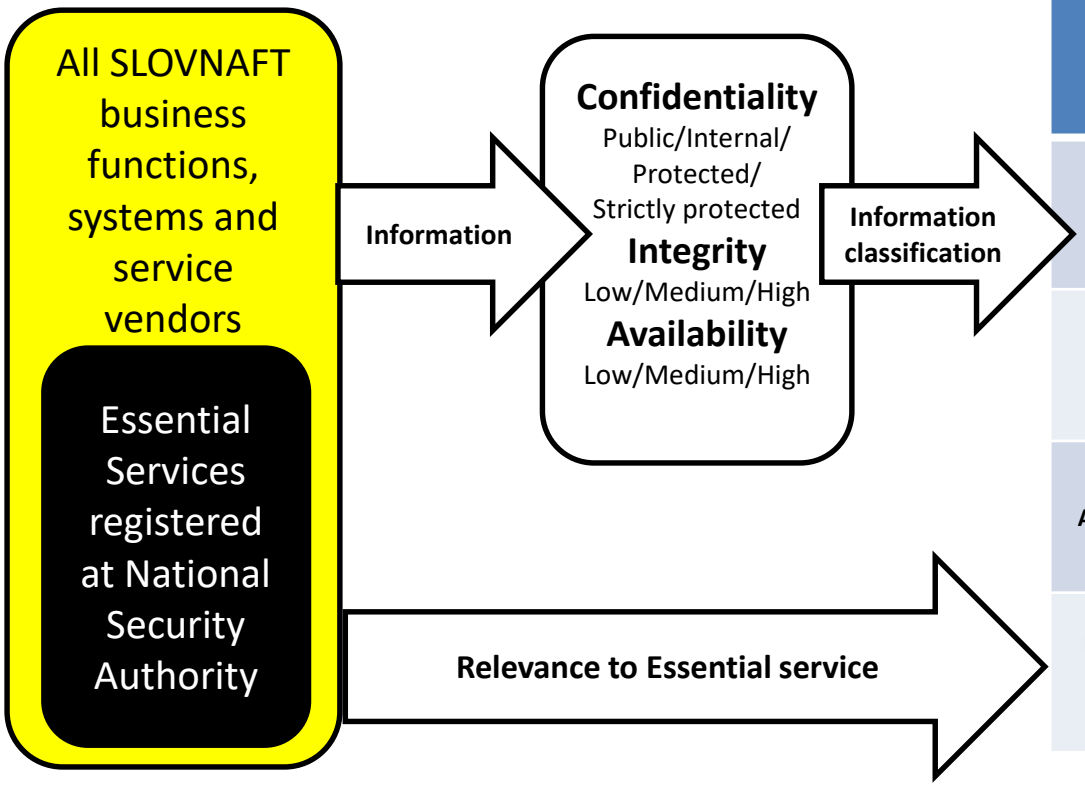




ICS platforms, Networks & Systems

Slovnaft
MEMBER OF MOL GROUP

NextStep: Categorization of ALL IT and ICS Systems of SLOVNAFT, a.s.



	Category I	Category II	Category III
Confiden-tiality	Public or Internal	Internal to Protected	Strictly protected
Integrity	Low to Medium	Medium to High	High
Availability	Low to Medium	Medium to High	High
Impact on essential service	No impact on essential service	May cause minor disruptions	Required to provide essential service

- The above mapping table is a **simplified version** according to the Decree of the National Security Authority n. 362/2018
- The way the mapping is defined in a way that **EVERY SYSTEM** operated by the company will be on **ONE OF THE CATEGORIES**

Slovnaft
MEMBER OF MOL GROUP

Šťastnú cestu

Slovnaft
MEMBER OF MOL GROUP