Spike Talk in Power Electronic Dominated Grids

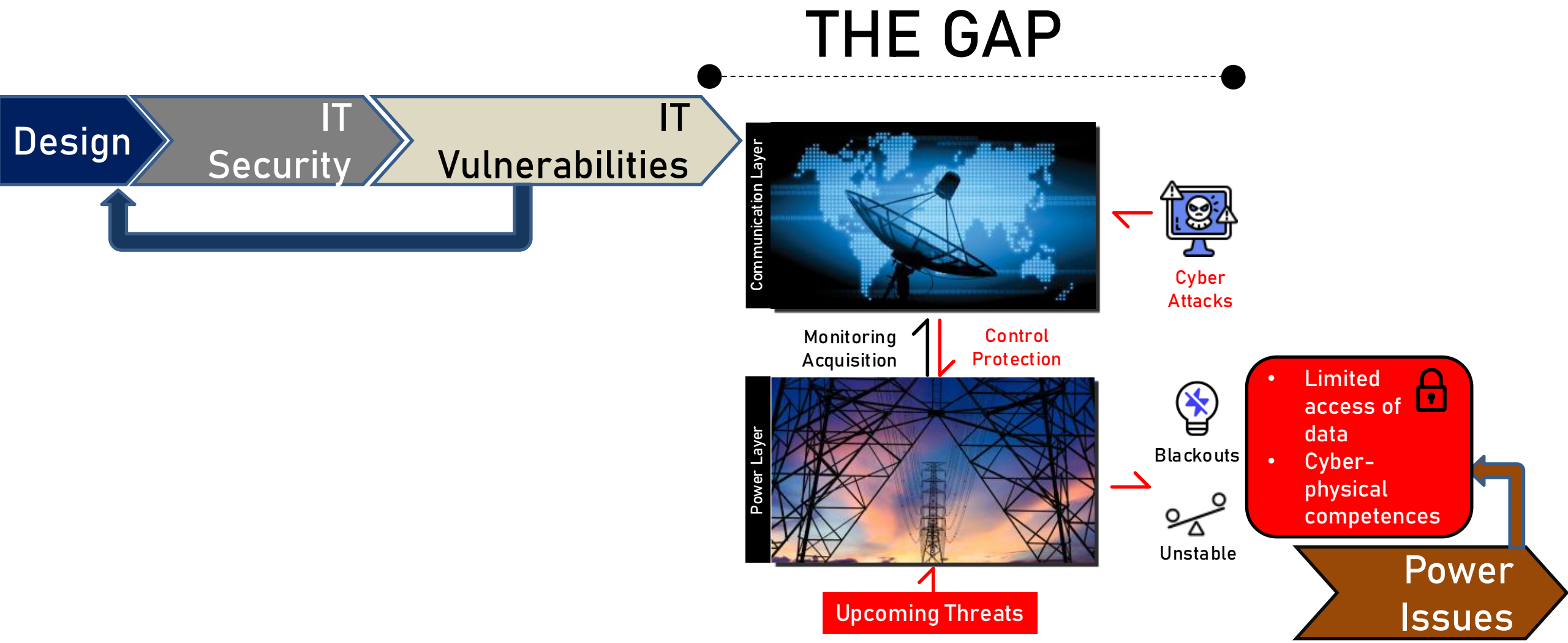
Towards a "One-Stop" Security Solution

Subham Sahoo
Assistant Professor, Aalborg University
Vice-Leader, Reliability of Power Electronic Converters (ReliaPEC Group)
Denmark

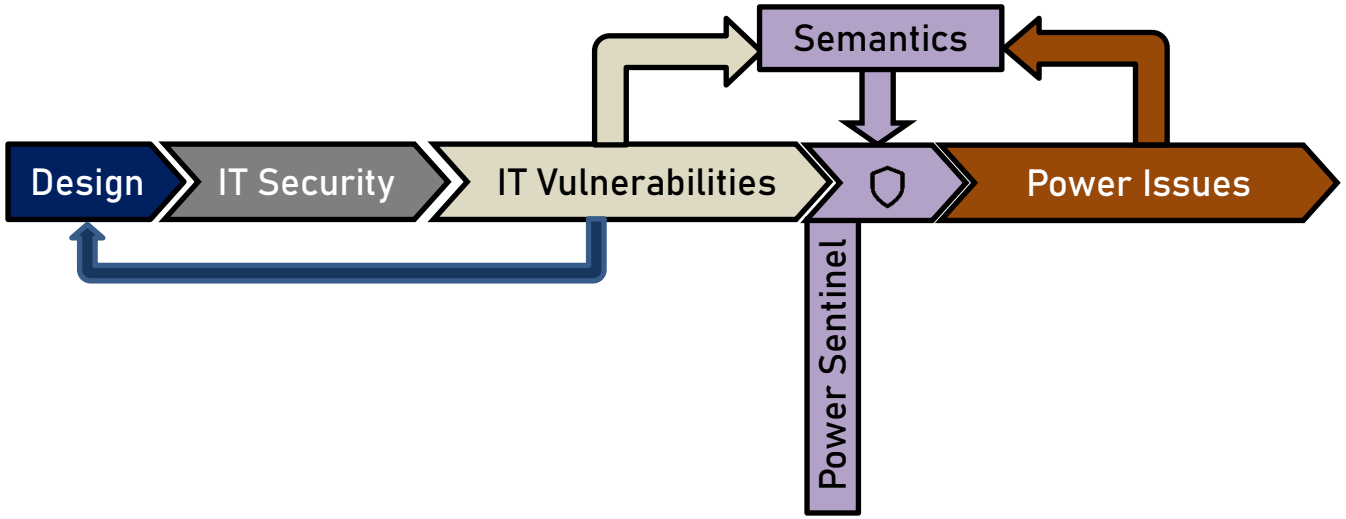
AAU ENERGY

AALBORG UNIVERSITY

▶ Closing the gap?



▶ Power Sentinel (TRL 5-6)

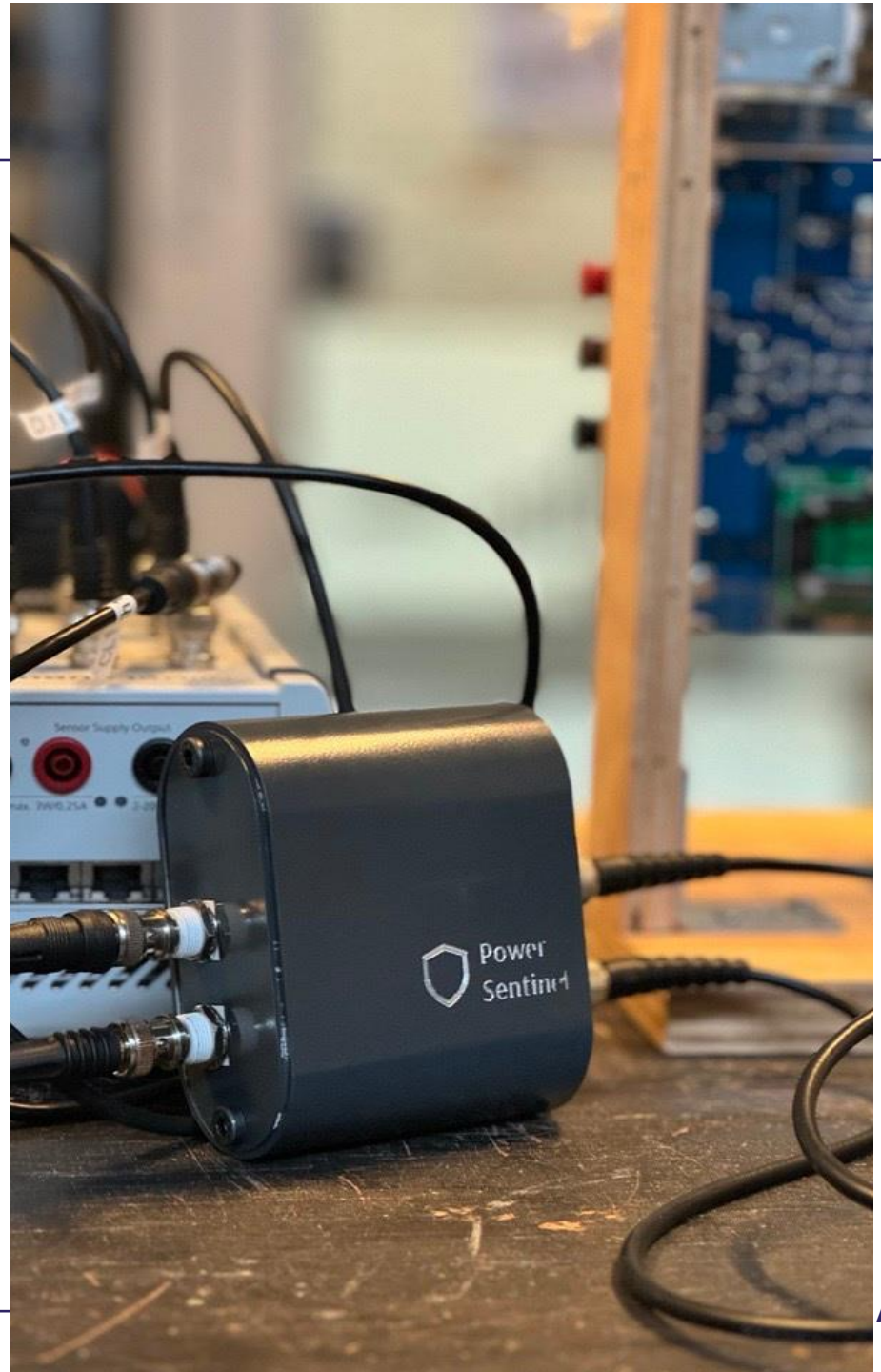


World's 1st NON-INVASIVE GRID EDGE Integrated Technology

Relevant standards passed:
IEEE 1547.3 and IEEE C37.240

Certified by:
Sandia National Laboratories

- **Resource-efficient**
- **Computationally light**
- **Plug-and-play modularity**



One Stop Solution to Digitalization Issues?

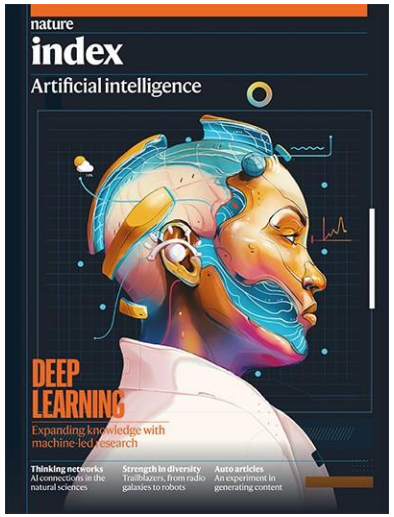
Criticality of ICT in Power Electronic Grids

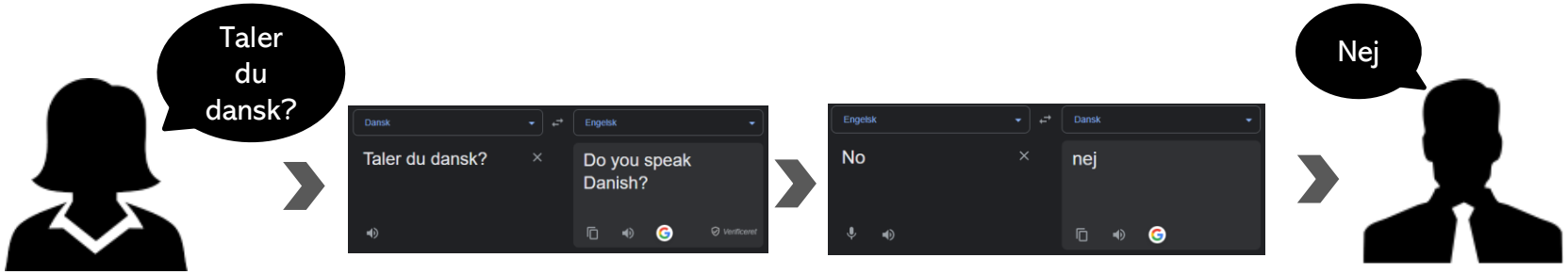
▶ Machine Learning Today

Breakthroughs in ML using (deep) Artificial Neural Networks (ANNs) have come at the expense of massive memory, energy, and time requirements

Alice

Bob



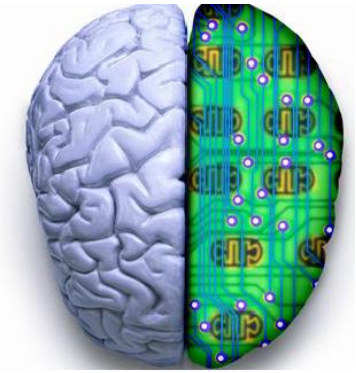


Data analysis → Training *(online)* → Testing → Deployment → Re-testing on new scenarios

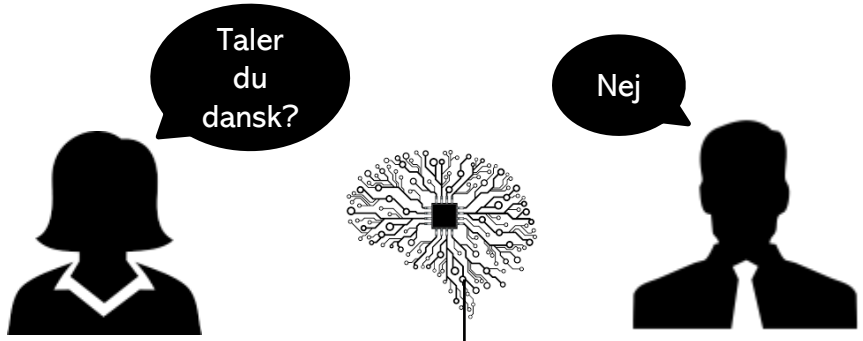
▶ Beyond ANN

13 Million Watts
5600 sq. ft. & 340 tons
10^{10} ops/J

20 Watts
2 sq. ft. & 1.4 Kg
10^{15} ops/J



A sustainable fast-track process



Data analysis → Training / Plastic Cognition / Online updates

- Energy-efficient
- Sparse and dynamic
- Event-driven learning and inferences
- Online actions

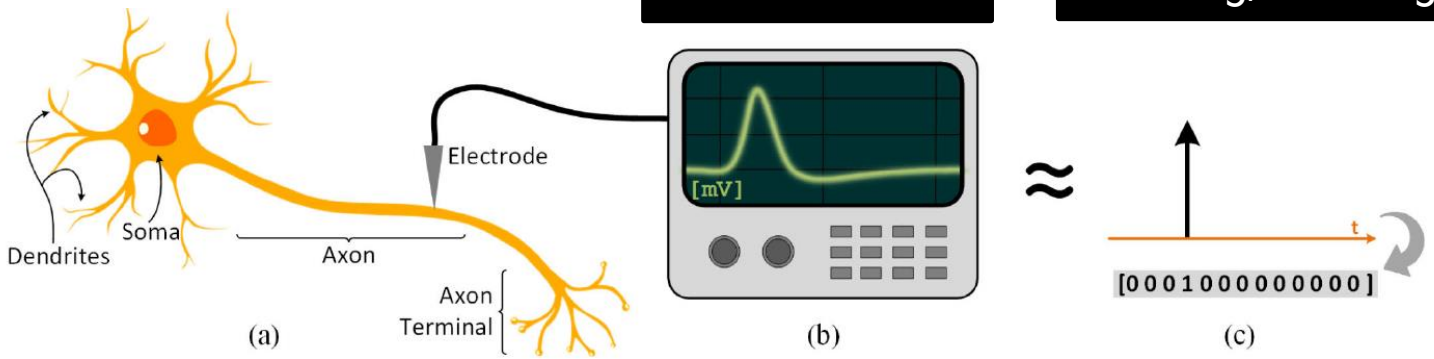
▶ Actually..

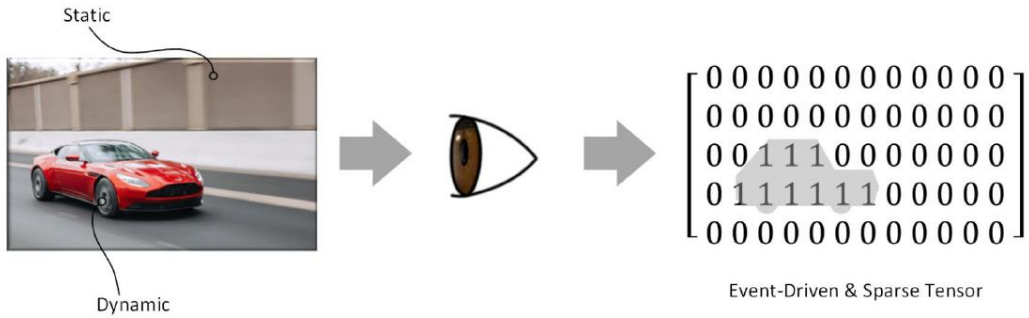
The electrical modeling of neurons in our brain are quite different from the ones using in a typical ML algorithm.

- Neurons in the brain sense, process, and communicate over time using sparse binary signals (spikes or action potentials).
- This results in a dynamic, sparse, event-driven learning and inference.
- Spiking signals minimize energy per bit.

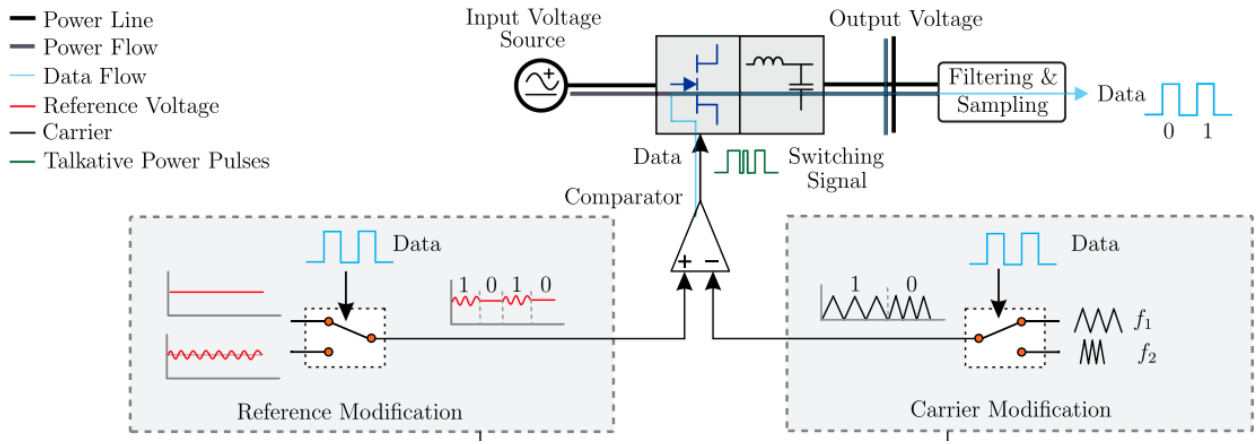
Data Translation

Encoding/Decoding





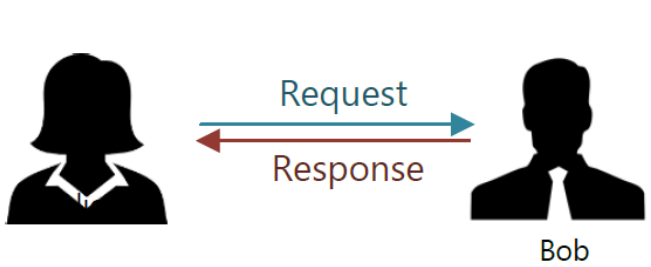
▶ Information Embedded in Power



Talkative Power[1,2]

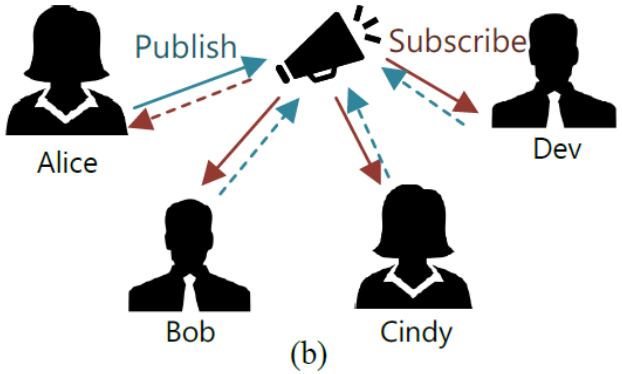
1. M. Liserre, H. Beiranvand, Y. Leng, R. Zhu and P. A. Hoeher, "Overview of Talkative Power Conversion Technologies," *IEEE Open Journal of Power Electronics*, vol. 4, pp. 67-80, 2023, doi: 10.1109/OJPEL.2023.3237709.
2. M. Angjelichinoski, Č. Stefanović, P. Popovski and F. Blaabjerg, "Power talk in DC micro grids: Constellation design and error probability performance," 2015 IEEE International Conference on Smart Grid Communications (SmartGridComm), Miami, FL, USA, 2015.

Inferential Communication



(a)

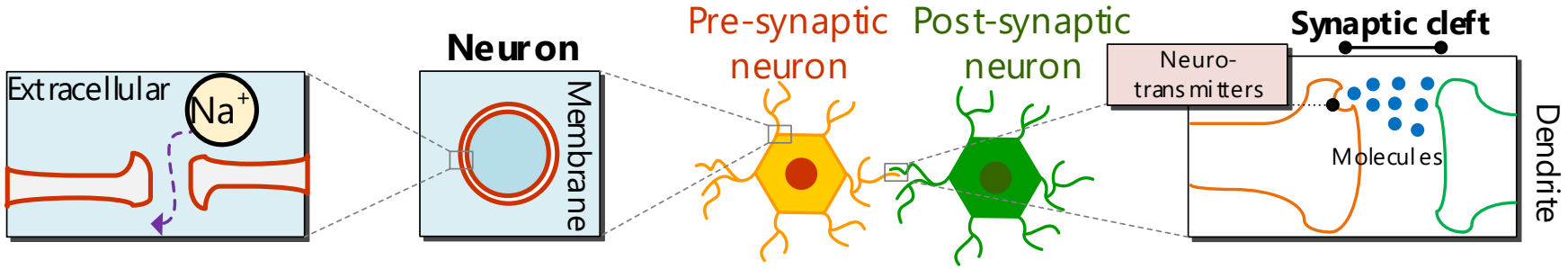
Request-response protocol



(b)

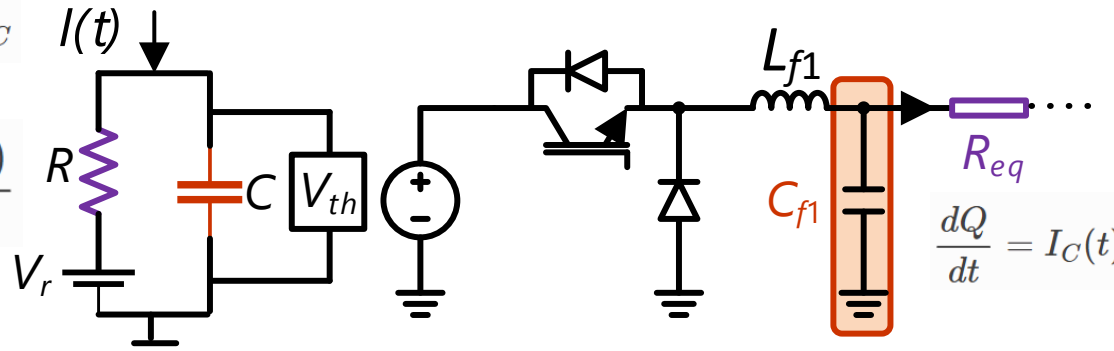
Publish-subscribe protocol

▶ Biologically Plausible Neurons/Converters

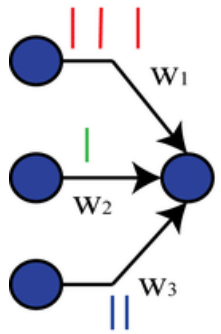


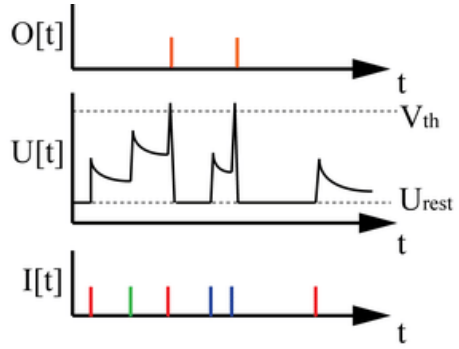
$$I_{\text{in}}(t) = I_R + I_C$$

$$I_R(t) = \frac{U_{\text{mem}}(t)}{R}$$



$$\frac{dQ}{dt} = I_C(t) = C\frac{dU_{\text{mem}}(t)}{dt}$$

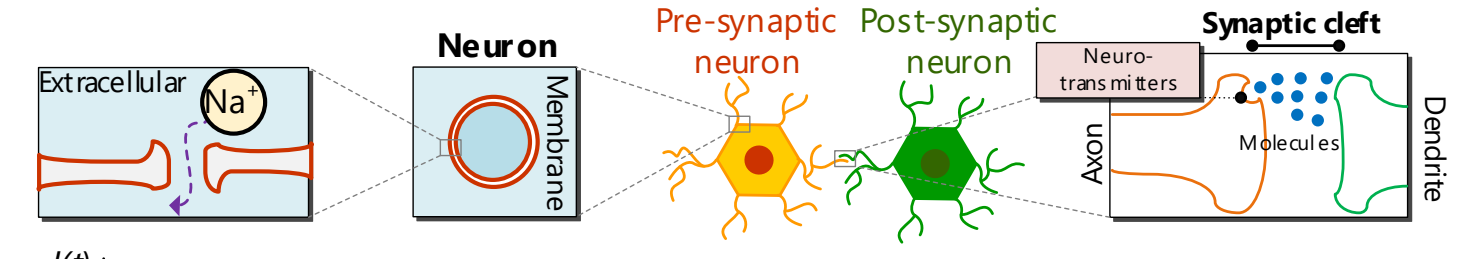


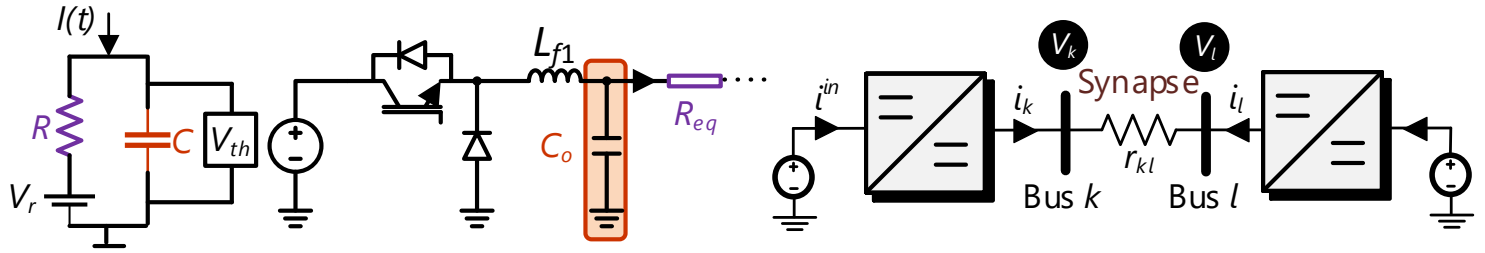


Leaky Integrate-and-Fire (LIF) Neuron

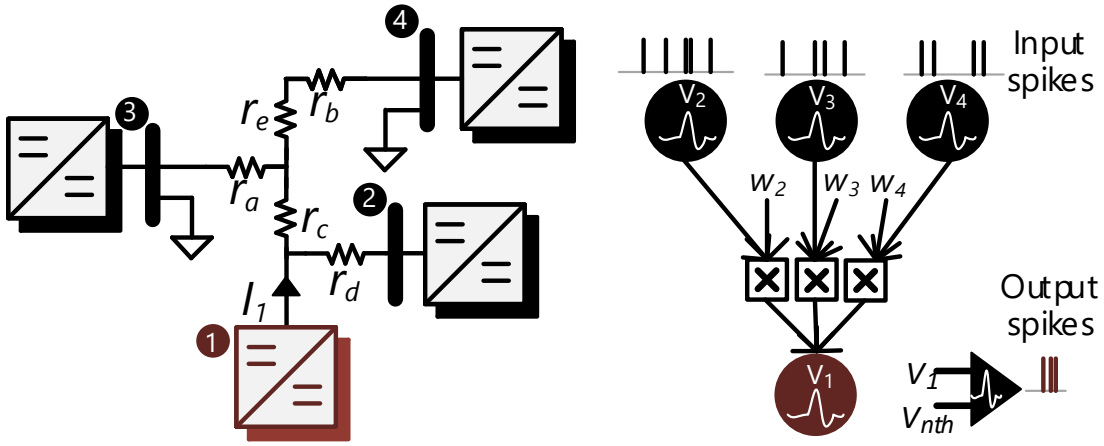
$$RC\frac{dU_{\text{mem}}(t)}{dt} = -U_{\text{mem}}(t) + RI_{\text{in}}(t)$$

▶ Fine Grained Parallelism



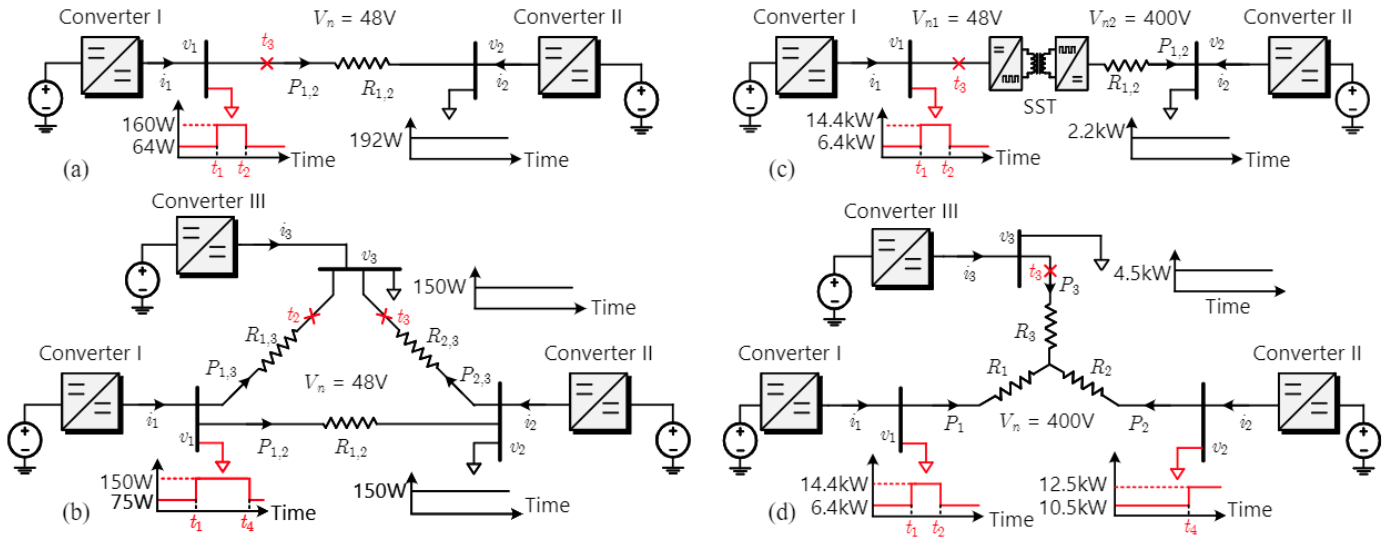


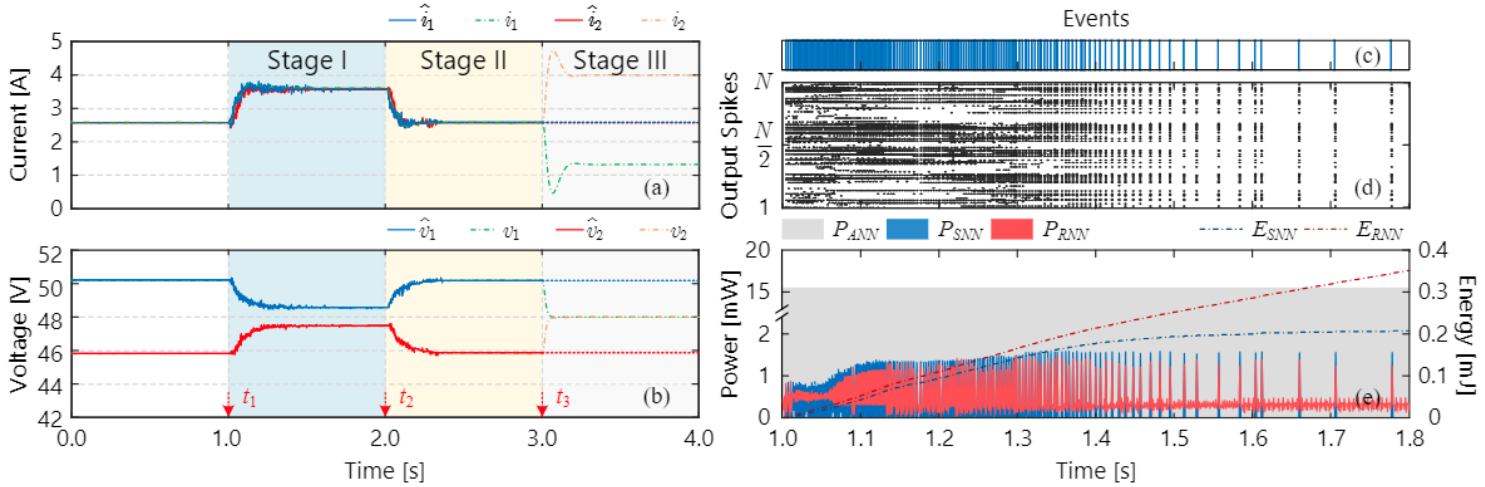
Brain	Power Grid
Neuron	DER
Synpase	Tie-Lines
Synaptic Current	Tie Line Currents
Neuron Membrane	Output Capacitence
Ion Channels	Equivalent Resistance
Ions	Electrons



Network of Converters have now become a network of neurons

▶ Performance Evaluation

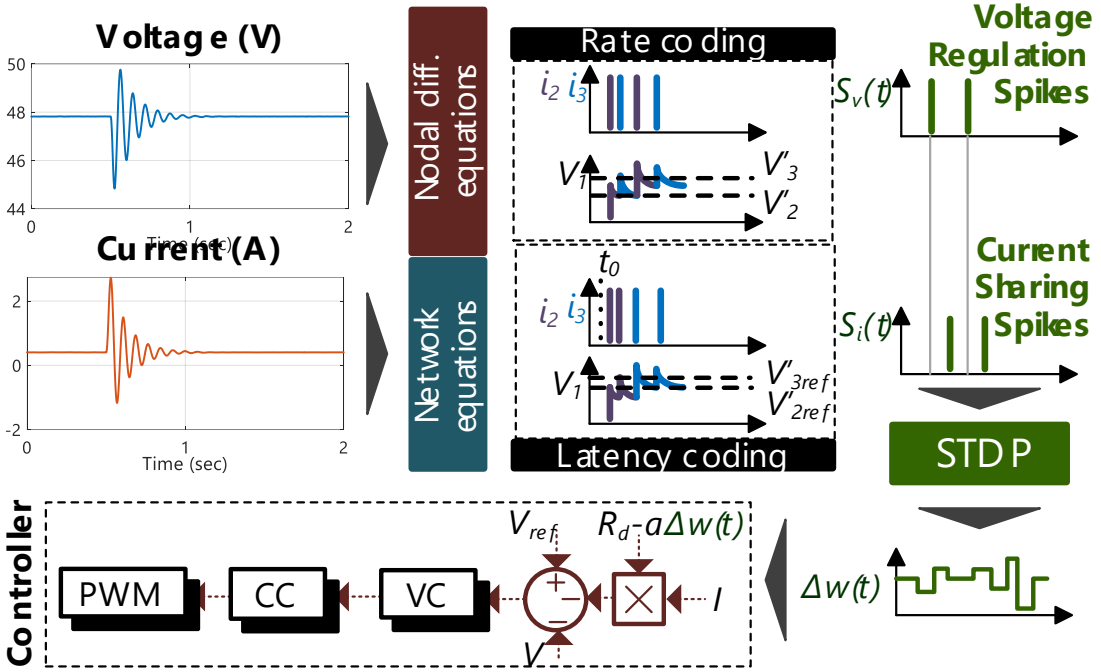




Source: X Diao, Y Song, S Sahoo, Y Li, « Neuromorphic Event-Driven Semantic Communication in Microgrids» *IEEE Trans. Smart Grid*, vol. 15, no. 5, pp. 4300-4314, 2024.

Upto 84% "compute" energy savings due to computation for a given mission profile

▶ Spiking Neuron Replicated as Energy Source

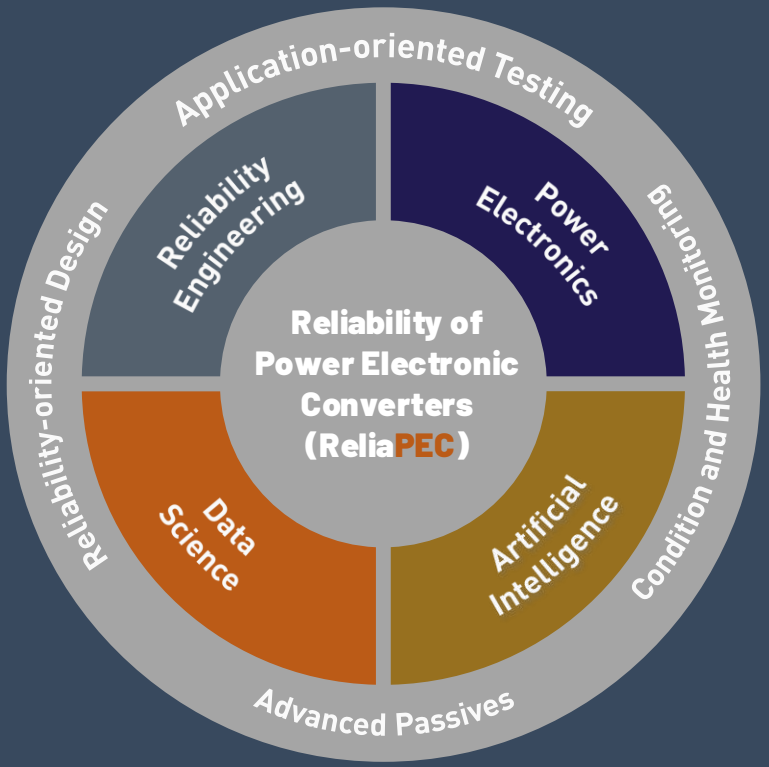


- We model each source as a LIF neuron
- It can respond to both input and output disturbances
- Only the remote sources will respond to a given disturbance based on the voltage fluctuations and its spatial decay
- Timing based learning rules to change the conductance of the modeled neuron and change power generation
- Multi-agent networked control, adaptation, protection, flexibility is possible with minimal energy consumption per inference

Source: S Sahoo, "Spike Talk – Genesis and Neural Coding Scheme Translations", *arXiv preprint arXiv:2408.00773*, 2024.

Contact

Subham Sahoo
ReliaPEC Group
sssa@energy.aau.dk
+45 9141 0380



Cybersecurity in Power Electronic Dominated Grids

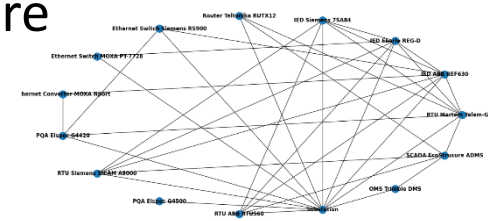
Challenges and Advances in Cybersecurity of Electricity Distribution Ecosystems: the Case of Slovenia

Andrej Bregar

INFORMATIKA

Cybersecurity in energy ecosystems

- Critical infrastructure is strategically important
- Increase in the attack surface of energy systems
- High-impact cyber-attacks result in the disruption of business continuity in energy distribution, cascading effects, and substantial damage to infrastructure
  - Stuxnet, Ukrainian electricity grid …
  - Hybrid war
- NIS 2 Directive: Boosting the protection of essential infrastructure by tightening risk assessments and reporting requirements



IT network

ADMS/ SCADA

OT network

- The estimated global cost of the cyber criminal in 2025 is 10.5 billion EUR
- The average response time to a cyber-attack is 280 days, which includes 210 days to detect the incident and 70 days for eradication, containment, and recovery

A large-scale cyber-attack on the energy grid: a recent case

Preparation and vulnerability identification

D_0 System intrusion Ransomware virus

$D_0 + 2$ Attack intensified

Locked access 120.000 files, 127 GB

A ransom demanded, online auction

Documents published on the dark web

Attack identified

Counter-measures

Business reports, control reports, internal business documentation, contracts, personal data, metering data, revisions, etc.

IT network

Only the IT infrastructure was affected: business systems, control systems, fire alarm systems, web pages, etc.

OT and physical network

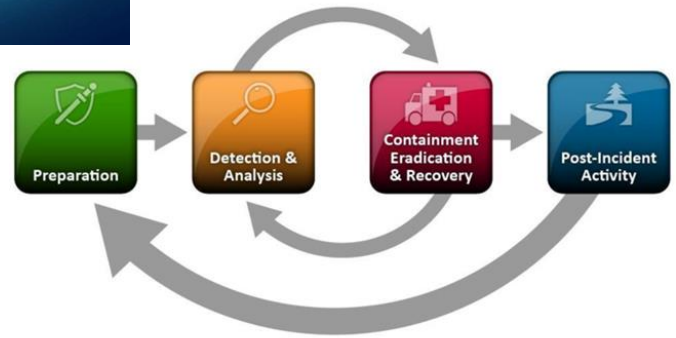
No escalation into the physical space and the OT network – limited losses

Only public information is presented, no technical details are provided!

INFORMATIKA

Cyber-attack countermeasures

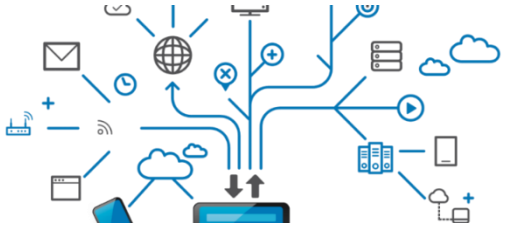
- Reporting
  - National CSIRT
  - Government Information Security Office
  - Other relevant governmental institutions and offices
  - Owners and stakeholders in the EPES ecosystem



- Incident response
  - Participation of relevant internal, external, and national cybersecurity teams
  - Technical countermeasures for incident analysis, containment, and eradication
  - Recovery of targeted business systems, identification and analysis of IoCs
  - Generic instructions for all EPES stakeholders
- What was achieved?
  - IT and OT systems operational, energy production and supply not disrupted
  - Business data recovered, no major business damage

Cybersecurity requirements for energy grids

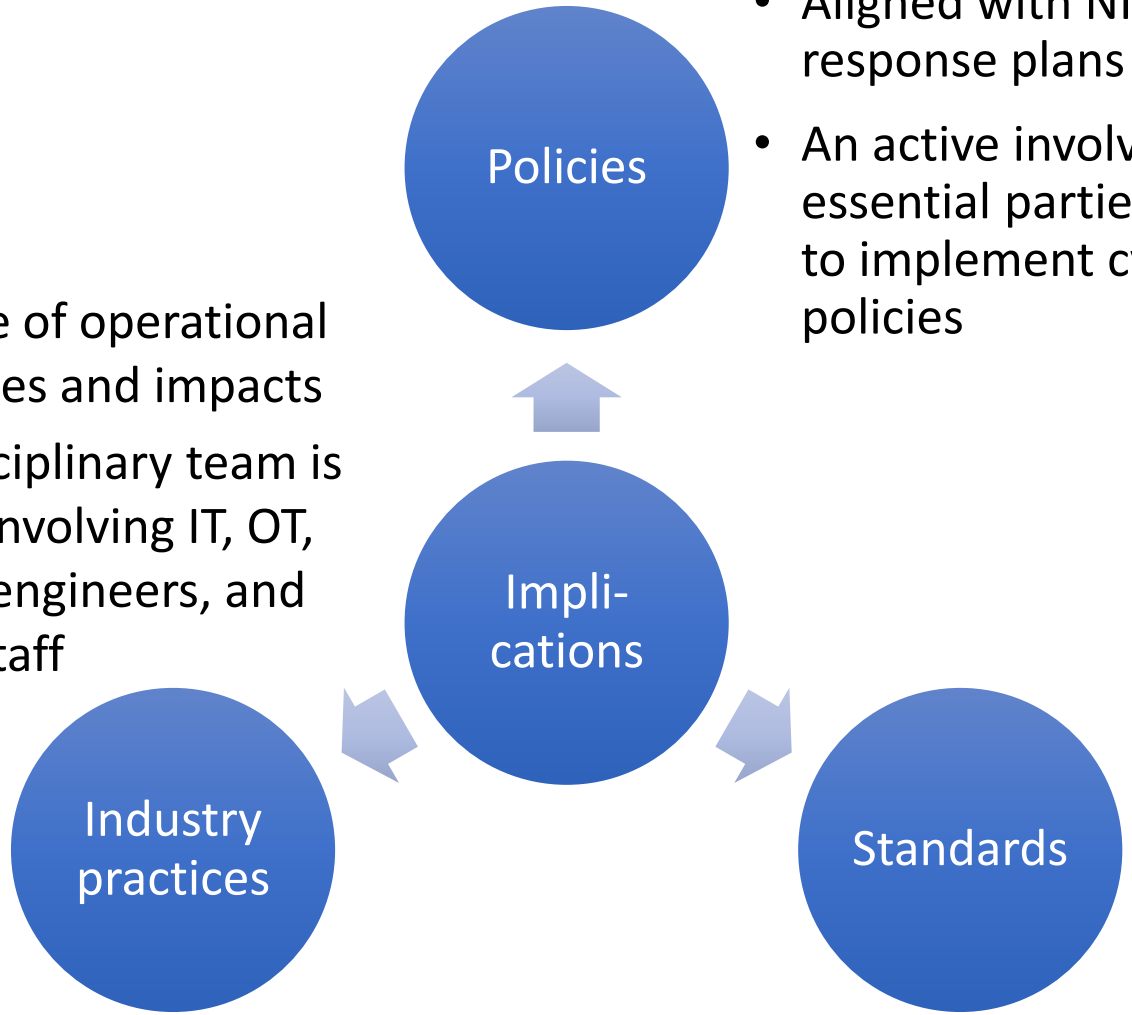
MAXIMIZED AVAILABILITY				MINIMIZED RISKS			
Application resilience	Network resilience	Access control	Information security	Change management	Vulnerability assessment	Incident reporting	Training
Continuous operations	Real-time demands	Cascading effects	Integration of new and legacy technologies	Recovery from attacks	Identification of anomalies	Process network (OT)	Counter-attacks



INFORMATIKA

Implications

- Knowledge of operational technologies and impacts
- A multidisciplinary team is required, involving IT, OT, industrial engineers, and business staff

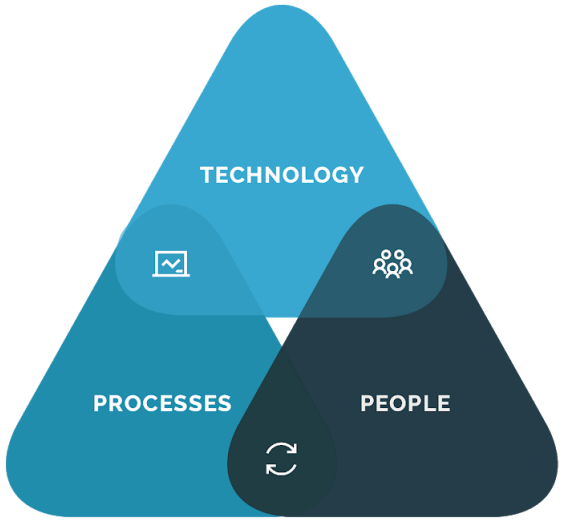


- Aligned with NIST and SANS response plans
- An active involvement of all essential parties is necessary to implement cybersecurity policies

- Specific standards, e.g., ISO/IEC 62443-4-1 (secure development of products used in industrial automation and control systems)
- Generic standards, e.g., ISO 27035, Part 3 (guidelines for IR operations)
- NIS 2 Directive
- NCC (Network Code on Cybersecurity)
- CER Directive (Critical Entities Resilience)
- CRA (Cyber Resilience Act)

National energy SOC

- National SOC for the energy ecosystem
- SOCs of major energy stakeholders
- SOCs of other major providers of critical infrastructure
- National CSIRT
- Governmental offices and institutions
- Communities

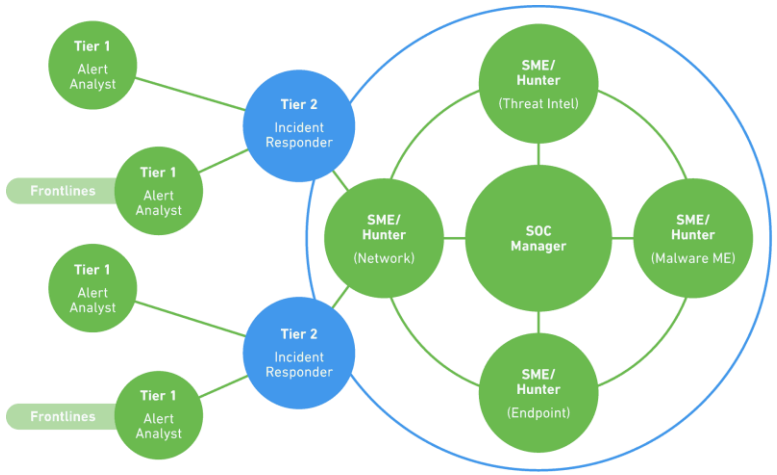


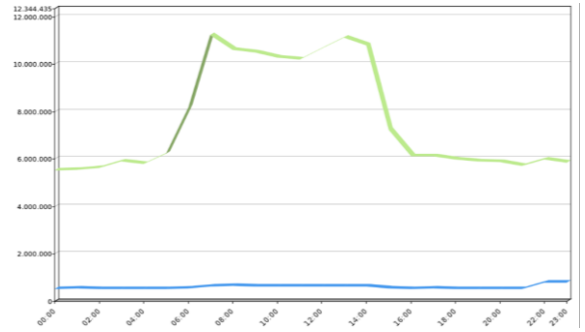
- Consolidation of resources and capabilities
- Improved and more agile detection and response
- Enhanced CTI exchange, stakeholder coordination, and alerting
- Centralized cyber risk management
- Single entering point
- Uniform protocols for reporting, collaboration, and response
- Regulatory compliance

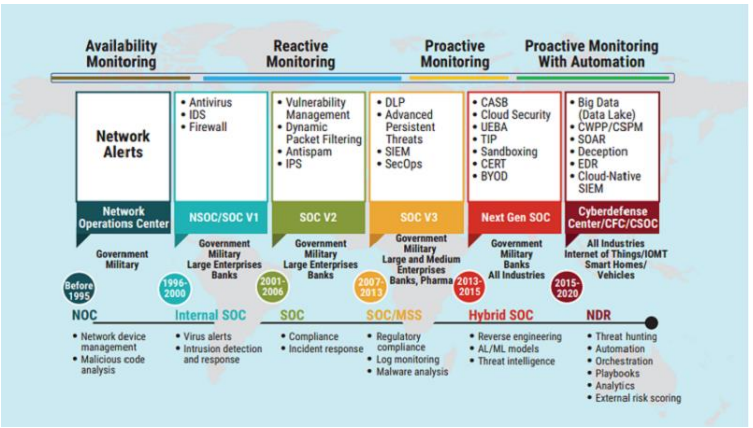
INFORMATIKA

Proactive NG-SOC of Informatika

- Proactive cyber defense – acting in anticipation of attacks, getting in front of them, neutralizing them early instead of waiting for the damage to occur
- 24/7/365, HA (High Availability)
- Slovenian DSOs
- IT-OT integration
- Multi-tier organization
- Large number of events
  - 5k+/- EPS
  - June: 7.189.513.374 events
  - July: 6.909.223.750 events
  - August: 6.625.410.913 events





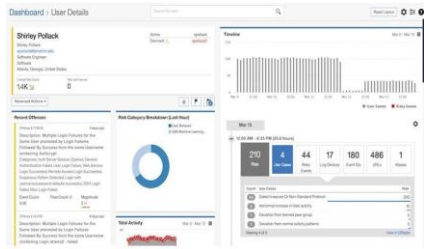


INFORMATIKA

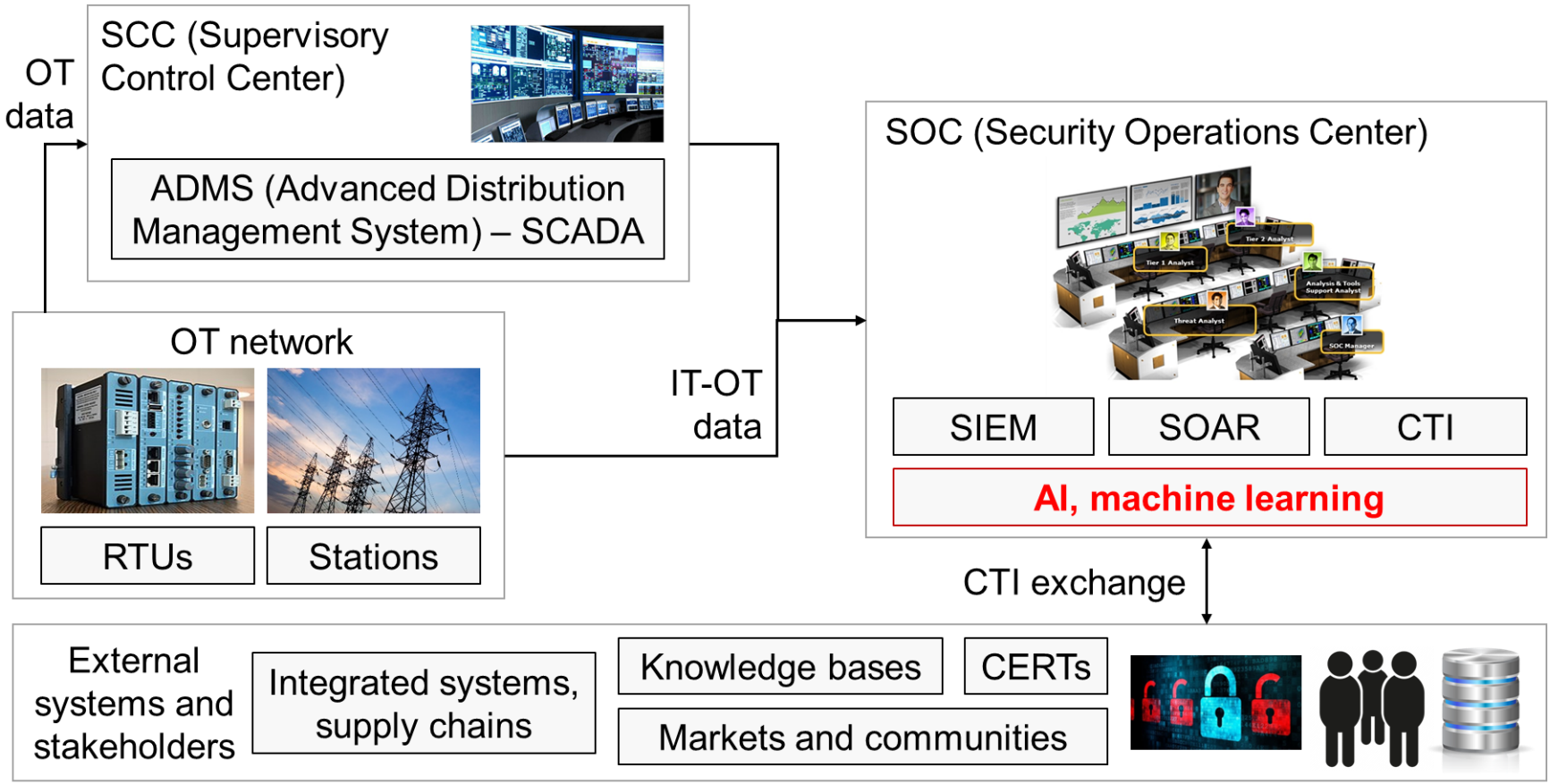
Protecting the IT-OT integrated energy system

Automated detection and information management

User behavior analytics



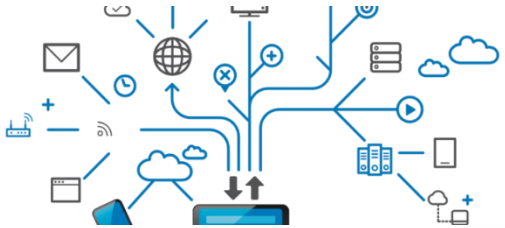
Automated response and playbooks



INFORMATIKA

Complementary reactive and proactive approach

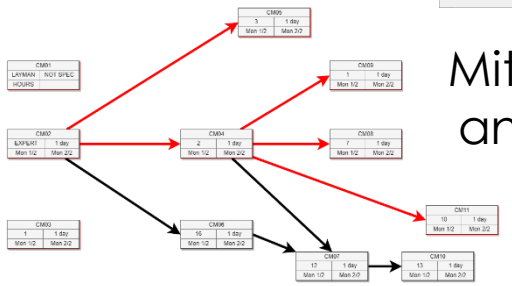
Cyber threats & attacks



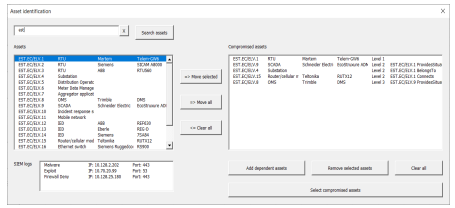
Assets

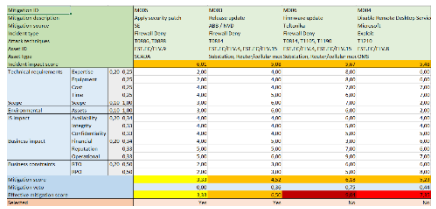
EPES stakeholders

Cybersecurity cooperation governance

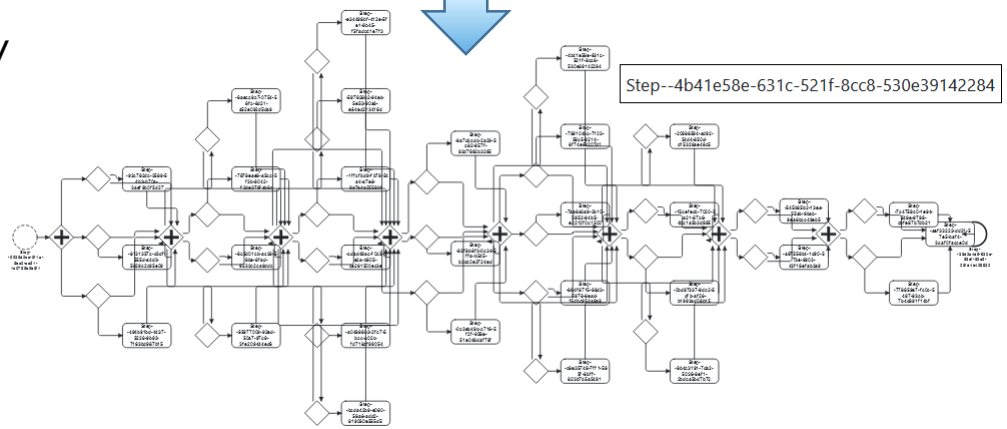


Mitigations framework and decision support





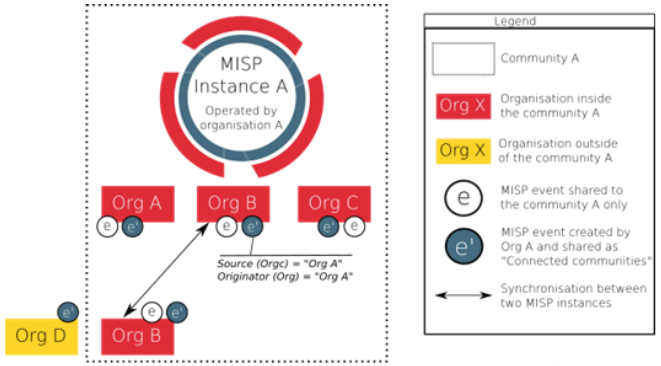
Processes and technology



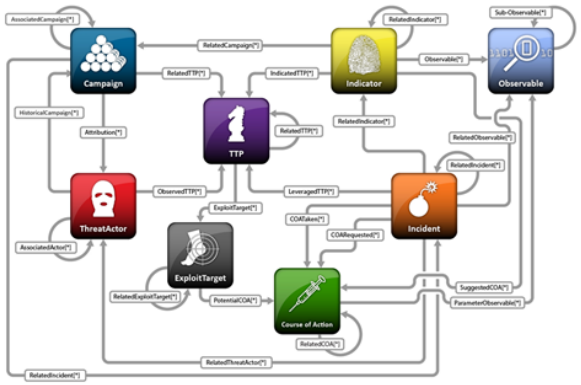
Incident response, reporting, and CTI

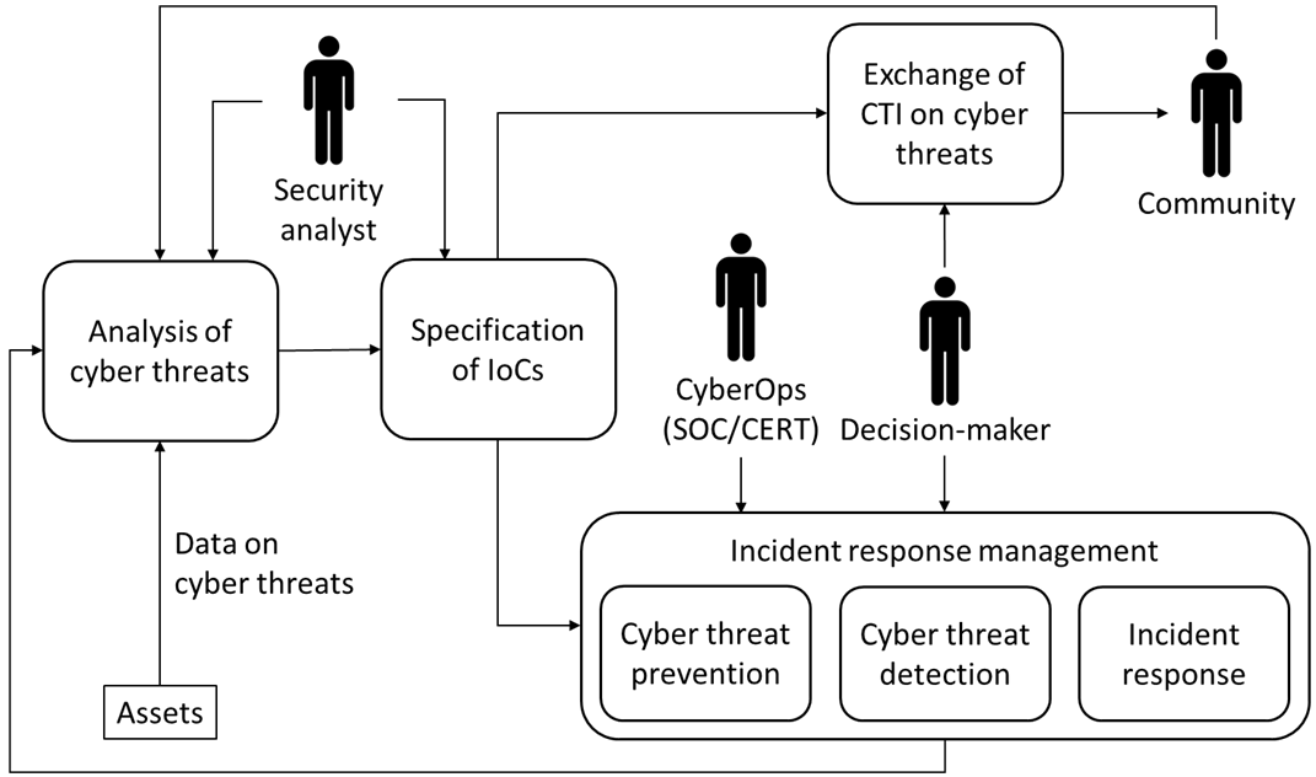
INFORMATIKA

CTI exchange in the communities



MISP Threat Sharing



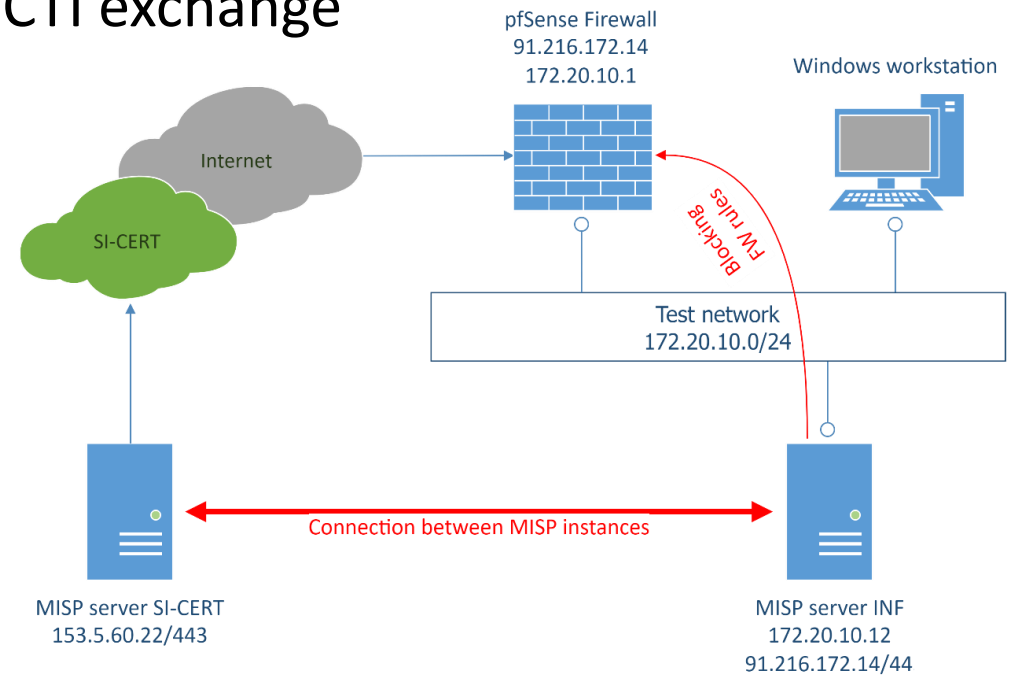


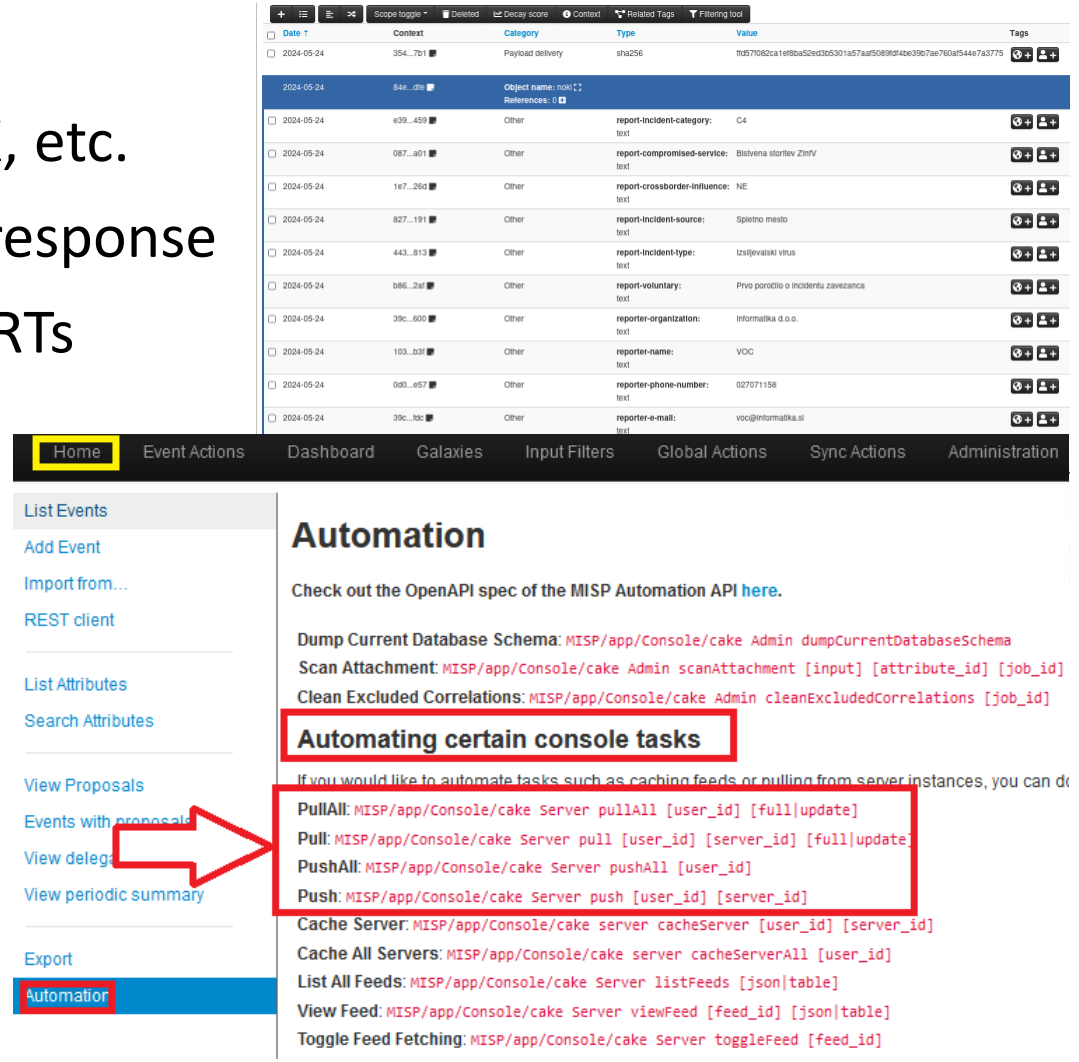
Tactical intelligence → Operational intelligence → Strategic intelligence

INFORMATIKA

Integration of security systems and tools

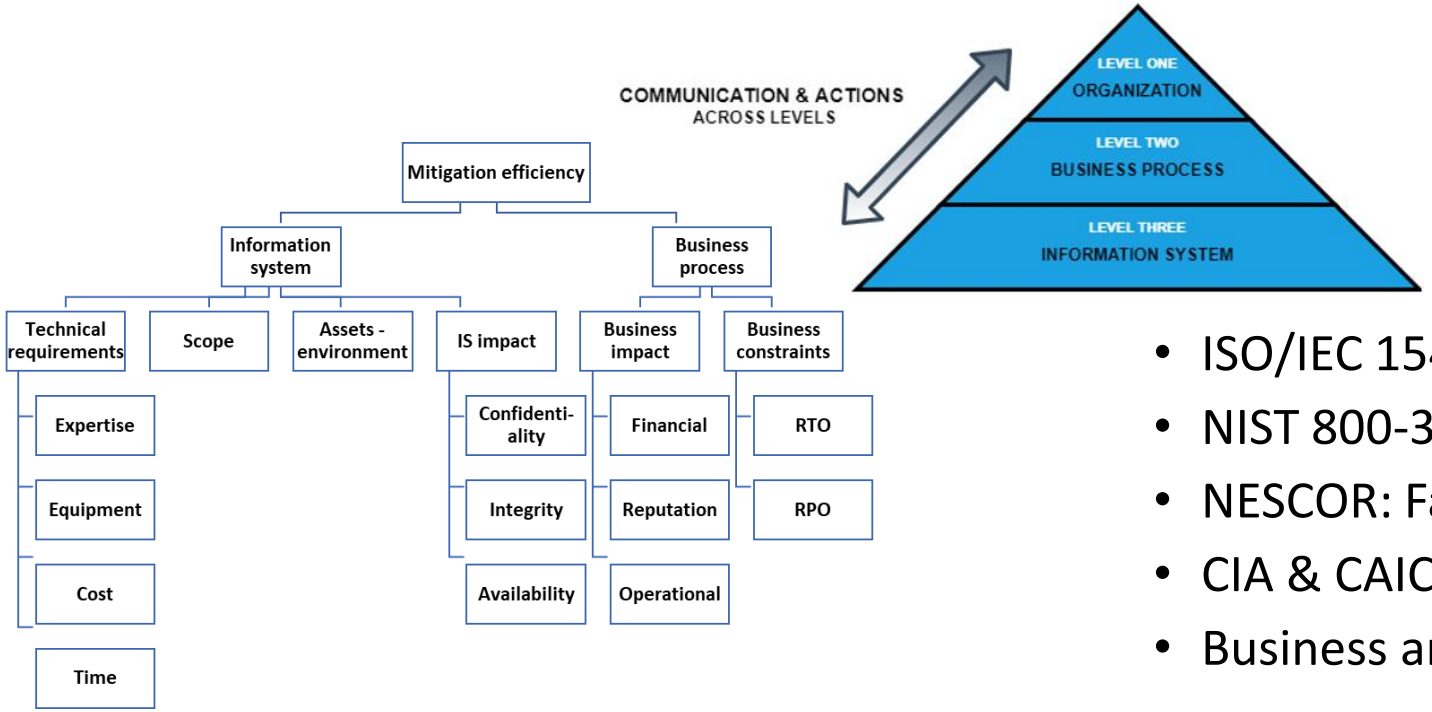
- Tools: MISP, SIEM, NG-FW, etc.
- Standard databases: NVD, MITRE ATT&CK, etc.
- Automated cyber-attack prevention and response
- Standardized reporting of incidents to CERTs
- Coordination between SOCs and CERTs
- CTI exchange





INFORMATIKA

Decision strategy and MCDM model



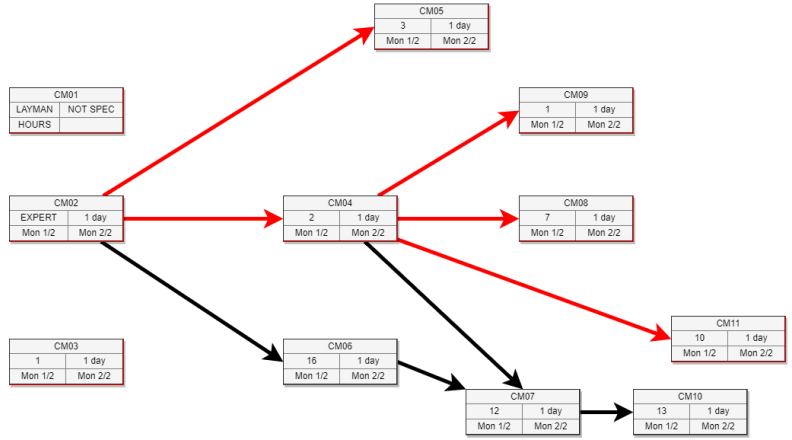
- ISO/IEC 15408: Common Criteria
- NIST 800-39: Managing Information Security Risks
- NESCOR: Failure Scenarios and Impact Analysis
- CIA & CAIC: Confidentiality, Integrity, Availability, Control
- Business and organizational requirements and constraints

1st model: Incident impact assessment

2nd model: Mitigation assessment and selection

High-level criteria	Sub-criteria
Measured impact	SIEM magnitude
	CVSS V2.0/V3.1
Safety concern	Public safety concern
	Workforce safety concern
Ecological concern	
System scale	
Impact on EPES	Negative impact on generation capacity
	Negative impact on energy market
	Negative impact on transmission system
	Negative impact on customer service
	Destroys goodwill toward utility
	Privacy loss of stakeholders
Financial impact	Financial impact on utility
	Restoration costs
	Immediate economic damage
	Long term economic damage
Asset criticality	Resilience of the compromised asset
	Relevance of the compromised asset

CSE_i = {T1087.001, T1087.002, T1087.003, T1087.004, T1110.002}

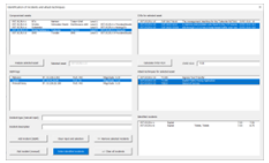


INFORMATIKA

Decision process

Asset CPEs, CVEs, and dependencies

Identification of compromised assets and vulnerabilities



Proactive

Reactive

Vulnerabilities

Assets			
	$CVSS(a_1,v_1)$	...	$CVSS(a_1,v_m)$
	...	...	...
	$CVSS(a_n,v_1)$	...	$CVSS(a_n,v_m)$

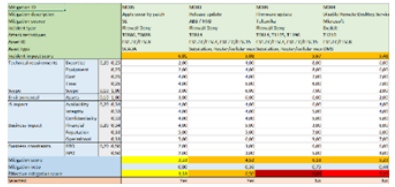
Score aggregation

Identification of incidents (analysis and enrichment of information/IoCs)

Incident impact assessment

Incidents

Assets			
	$S(a_1,i_1)$	...	$S(a_1,i_m)$
	...	...	...
	$S(a_n,i_1)$	...	$S(a_1,i_m)$



IoCs on cybersecurity events (SIEM)

Group decision-making

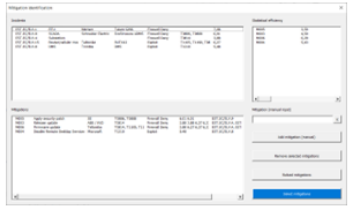
Identification of mitigation actions and strategies

Mitigation assessment

Efficiency

Mitigations	
	$E(m_1)$
	...
	$E(m_p)$

Selection and implementation of mitigation actions and strategies



Mitigations, TTPs

Implementation efficiency feedback

INFORMATIKA

MCDM analysis

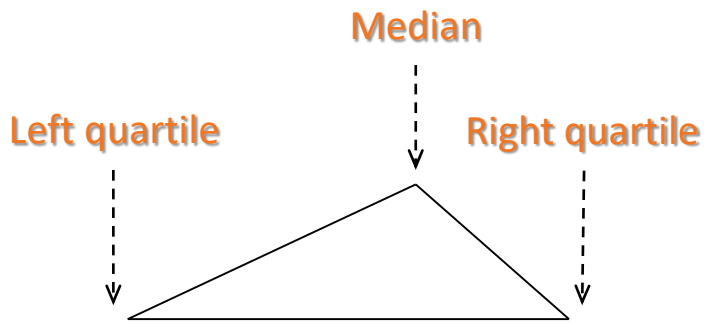
$$\Delta_w = \min \frac{\left[\sum_{j=1}^{n} \left| w_j - \widetilde{w}_j \right|^P\right]^{1/P}}{\Delta_w^{\max}}$$

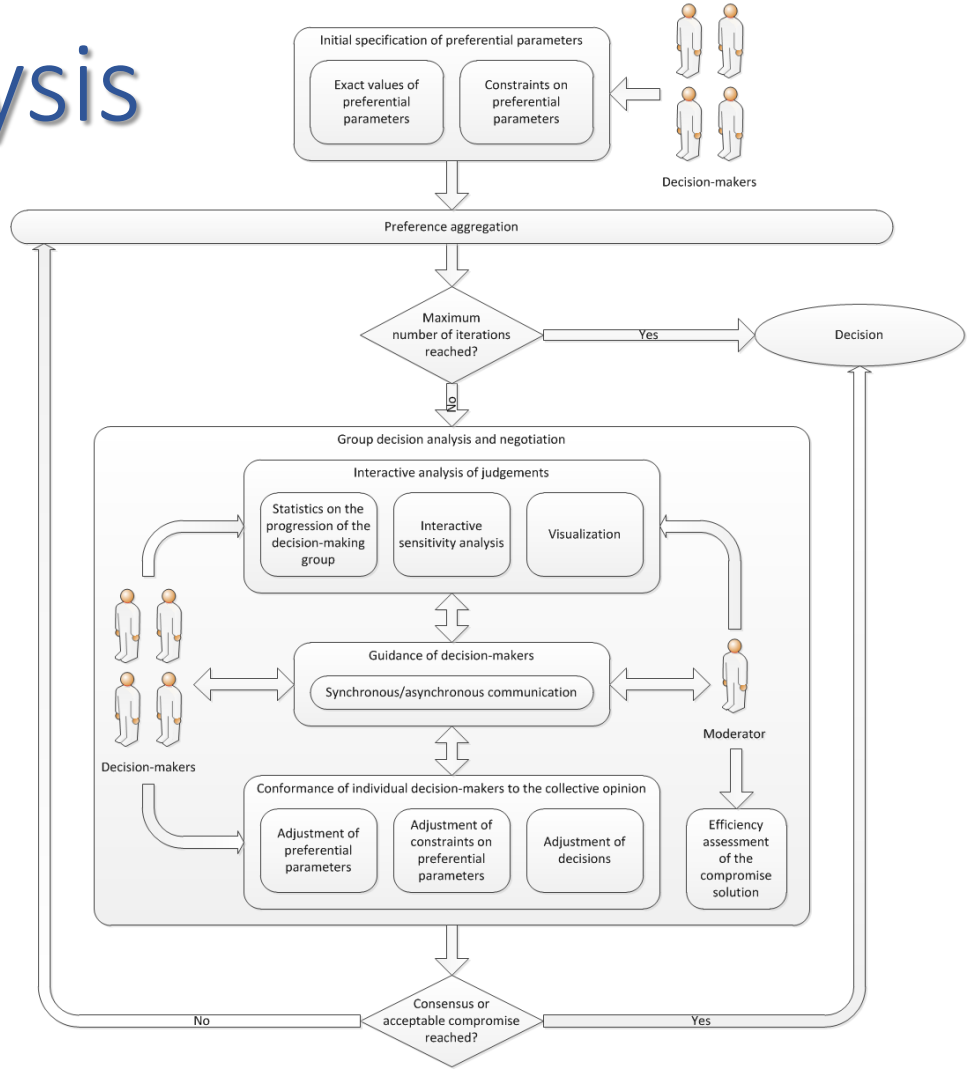
subject to

$$s^E(M_k) = \sum_{j=1}^{n} w_j s_j^E(M_k) = C_q$$

$$\sum_{j=1}^{n} w_j = 1$$

$$0 \le w_j \le 1, \forall j = 1, \dots, n$$





Compromised (in)dependent assets

$$(A_j DA_k) \vee \neg(A_j DA_k), \forall p \le j < k \le q, j \ne k$$

Qualitative Delphi statistics

$$\forall(CSE_i, A_j): (C^I_{\min}, C^I_{\text{median}}, C^I_{\max}) \text{ for } \{DM_1, \dots, DM_m\}$$

$$\forall(CSE_i, A_j, M_k): (C^E_{\min}, C^E_{\text{median}}, C^E_{\max}) \text{ for } \{DM_1, \dots, DM_m\}, M_k \in \{MA_k, RS_k\}$$

Quantitative Delphi statistics

$$\forall(CSE_i, A_j): (s^I_{\min}, s^I_{\text{avg}}, s^I_{\max}) \text{ for } \{DM_1, \dots, DM_m\}$$

$$\forall(CSE_i, A_j, M_k): (S^E_{\min}, S^E_{\text{avg}}, S^E_{\max}) \text{ for } \{DM_1, \dots, DM_m\}, M_k \in \{MA_k, RS_k\}$$

None	Negligible	Low	Medium	High	Critical
0.0	0.1 to 1.0	1.1 to 4.0	4.1 to 7.0	7.1 to 9.0	9.1 to 10.0

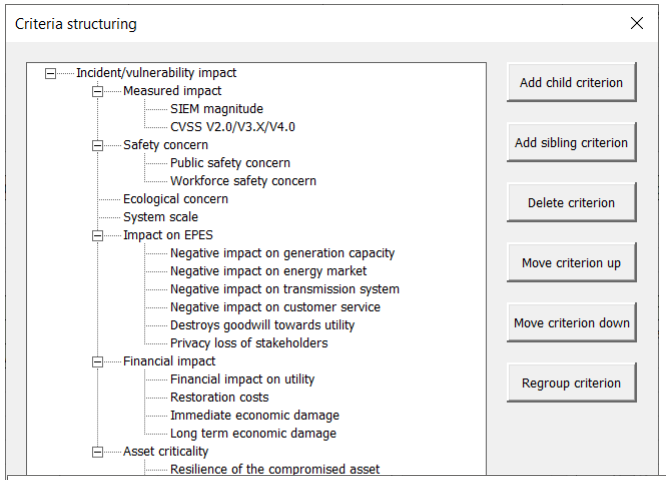
INFORMATIKA

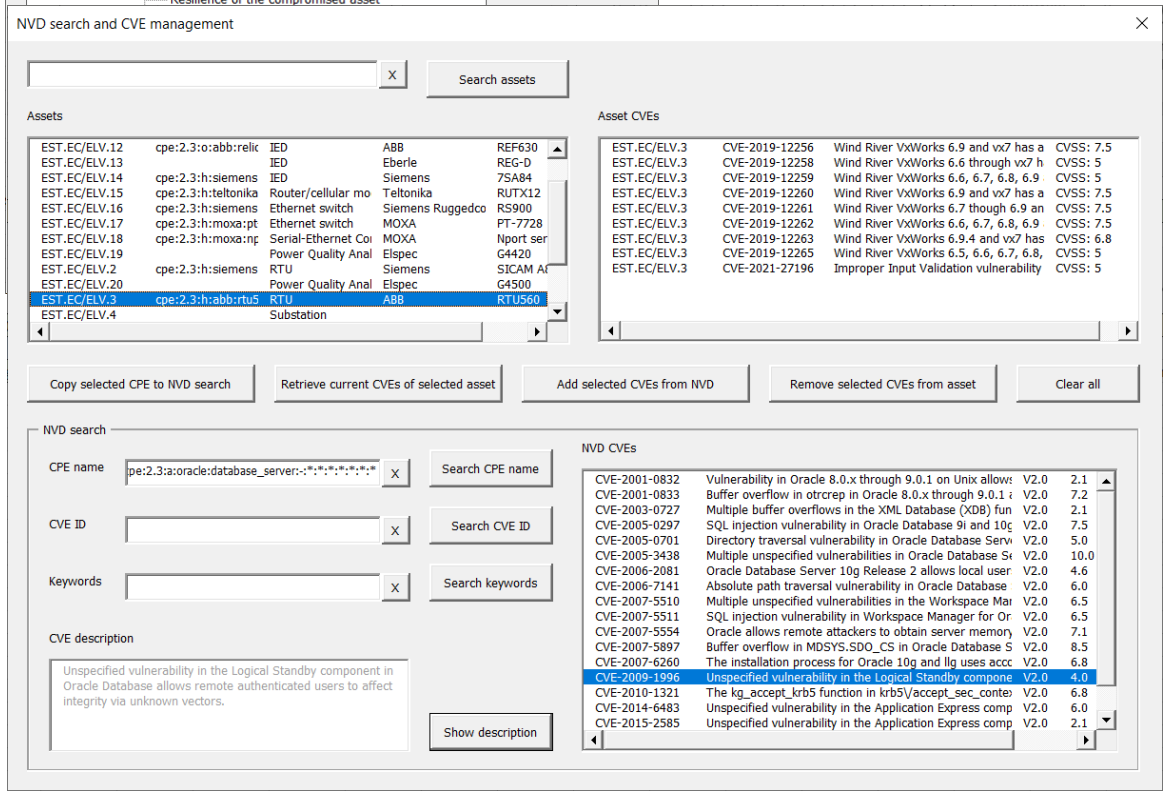
	A	B	D	E	F	G	H
1		Asset ID	EST.EC/ELV.1	EST.EC/ELV.9	EST.EC/ELV.4	EST.EC/ELV.15	EST.EC/ELV.8
2		Asset type	RTU	SCADA	Substation	Router/cellular modem	OMS
3		Asset vendor	Martem	Schneider Electric		Teltonika	Trimble
4		Asset product	Telem-GW6	EcoStruxure ADMS		RUTX12	DMS
5		Asset level	Level 1	Level 2	Level 2	Level 2	Level 3
6		Dependency		EST.EC/ELV.1 ProvidesSituatio	EST.EC/ELV.1 BelongsTo	EST.EC/ELV.1 Connects	EST.EC/ELV.9 ProvidesSituatio
7		Incident type	Exploit	Exploit	Firewall Deny	Firewall Deny	Exploit
8		Attack techniques		T0886, T0888	T0814	T0814, T1105, T1190	T1210
9	25	Incident/vulnerability impact	Medium	High	High	Low	Medium
10	26	Impact	Low	High	High	Low	Medium
11	27	Measured impact	High	High	Low	High	High
12	28	SIEM magnitude	Medium	High	Low	High	High
13	29	CVSS V2.0/V3.X/V4.0	High	High	Medium	Medium	High
14	30	Impact on EPES	Low	Medium	High	Low	Medium
15	31	Negative impact	Low	High	High	Low	Medium
16	32	Negative impact on generation capacity	Medium	h	High	Low	Medium
17	33	Negative impact on energy market	Low	Medium	High	Medium	Low
18	34	Negative impact on transmission system	Medium	High	High	Medium	High
19	35	Negative impact on customer service	High	High	Medium	Low	Medium
20	36	Destroys goodwill towards utility		Medium	High	Low	Medium
21	37	Privacy loss of stakeholders	Low	Medium	Medium	Medium	Low
22	38	Financial impact	Low	High	High	Low	Medium
23	39	Financial impact on utility	Low	High	High	Low	Medium
24	40	Restoration costs	Low	Medium	High	Low	Medium
25	41	Immediate economic damage	Medium	High	High	Medium	Low
26	42	Long term economic damage	Medium	Medium	Medium	Low	Medium
27	43	Concern	Medium	Medium	High	Low	Low
28	44	Safety concern	High	High	High	Low	Medium
29	45	Public safety concern	Medium	High	High	Low	Medium
30	46	Workforce safety concern	High	High	High	Medium	Medium
31	47	Ecological concern	Low	Low	High	Low	Low
32	48	System scale	Medium	High	High	Low	Medium
33	49	Asset criticality	Medium	High	High	Medium	High
34	50	Resilience of the compromised asset	Medium	Medium	Medium	High	High
35	51	Relevance of the compromised asset	Medium	High	High	Low	Medium
36		Impact score	Medium	High	High	Low	Medium

Low
Medium
High

		Delphi statistics		Min	Mean	Max	Min	Mean	Max	Min	Mean	Max	Min	Mean	Max	Min	Mean	Max
8																		
9	1	Incident/vulnerability impact	1,00	5,99	6,99	8,67	3,93	5,81	7,08	3,20	5,53	6,93	4,29	6,26	8,11	3,32	5,45	7,26
10	2	Measured impact	0,15	7,42	7,42	7,42	8,17	8,17	8,17	2,67	2,67	2,67	7,33	7,33	7,33	8,67	8,67	8,67
11	3	SIEM magnitude	0,50	7,33	7,33	7,33	7,33	7,33	7,33	5,33	5,33	5,33	5,33	5,33	5,33	7,33	7,33	7,33
12	4	CVSS V2.0/V3.X/V4.0	0,50	7,50	7,50	7,50	9,00	9,00	9,00	0,00	0,00	0,00	9,33	9,33	9,33	10,00	10,00	10,00
13	5	Safety concern	0,10	5,50	7,00	9,00	3,00	5,50	6,50	3,00	6,50	8,00	3,50	6,50	8,00	2,00	5,50	7,00
14	6	Public safety concern	0,50	6,00	7,00	9,00	2,00	6,00	7,00	3,00	6,00	8,00	3,00	6,00	8,00	2,00	5,00	7,00
15	7	Workforce safety concern	0,50	5,00	7,00	9,00	4,00	5,00	6,00	3,00	7,00	8,00	4,00	7,00	8,00	2,00	6,00	7,00
16	8	Ecological concern	0,10	3,00	5,00	10,00	6,00	7,00	8,00	6,00	8,00	9,00	4,00	8,00	10,00	5,00	6,00	9,00
17	9	System scale	0,10	7,00	8,00	9,00	4,00	6,00	7,00	5,00	6,00	7,00	5,00	6,00	9,00	2,00	5,00	6,00
18	10	Impact on EPES	0,20	5,40	6,90	8,15	2,15	4,05	5,80	2,15	4,65	6,65	2,60	4,45	6,80	1,50	3,65	5,55
19	11	Negative impact on generation capacity	0,15	8,00	8,00	8,00	3,00	6,00	7,00	3,00	6,00	7,00	5,00	6,00	8,00	2,00	5,00	6,00
20	12	Negative impact on energy market	0,15	7,00	8,00	9,00	2,00	5,00	7,00	3,00	6,00	8,00	5,00	6,00	8,00	2,00	5,00	6,00
21	13	Negative impact on transmission system	0,15	4,00	7,00	8,00	1,00	4,00	5,00	2,00	3,00	7,00	1,00	3,00	6,00	1,00	2,00	3,00
22	14	Negative impact on customer service	0,15	5,00	7,00	8,00	3,00	4,00	5,00	1,00	4,00	5,00	1,00	4,00	6,00	1,00	3,00	6,00
23	15	Destroys goodwill towards utility	0,20	6,00	8,00	10,00	3,00	4,00	7,00	2,00	6,00	9,00	3,00	6,00	9,00	2,00	5,00	8,00
24	16	Privacy loss of stakeholders	0,20	3,00	4,00	6,00	1,00	2,00	4,00	2,00	3,00	4,00	1,00	2,00	4,00	1,00	2,00	4,00
25	17	Financial impact	0,20	6,00	7,25	9,25	3,00	5,50	7,50	3,00	6,25	8,00	3,75	6,25	8,00	2,25	4,75	7,25
26	18	Financial impact on utility	0,25	8,00	8,00	9,00	3,00	6,00	7,00	3,00	6,00	7,00	3,00	6,00	7,00	2,00	5,00	7,00
27	19	Restoration costs	0,25	6,00	8,00	10,00	4,00	6,00	7,00	3,00	8,00	10,00	3,00	8,00	9,00	3,00	6,00	7,00
28	20	Immediate economic damage	0,25	6,00	7,00	10,00	4,00	6,00	10,00	5,00	8,00	10,00	7,00	8,00	10,00	3,00	6,00	9,00
29	21	Long term economic damage	0,25	4,00	6,00	8,00	1,00	4,00	6,00	1,00	3,00	5,00	2,00	3,00	6,00	1,00	2,00	6,00
30	22	Asset criticality	0,15	7,00	7,00	8,50	2,50	5,50	7,00	2,50	6,00	8,00	4,50	6,50	9,00	2,50	5,50	8,00
31	23	Resilience of the compromised asset	0,50	6,00	6,00	8,00	2,00	6,00	7,00	3,00	6,00	9,00	4,00	6,00	9,00	3,00	5,00	6,00
32	24	Relevance of the compromised asset	0,50	8,00	8,00	9,00	3,00	5,00	7,00	2,00	6,00	7,00	5,00	7,00	9,00	2,00	6,00	10,00
33		Impact score		5,99	6,99	8,67	3,93	5,81	7,08	3,20	5,53	6,93	4,29	6,26	8,11	3,32	5,45	7,26

1	Incident/vulnerability impact							
2	Criterion ID	2	5	8	9	10	17	22
3	Current weight	0,16	0,13	0,03	0,09	0,31	0,14	0,14
4		Measured impact	Safety concern	Ecological concern	System scale	Impact on EPES	Financial impact	Asset criticality
5	Measured impact	1/1	2/1	6/1	4/1	1/4	1/2	1/1
6	Safety concern	1/2	1/1	4/1	2/1	1/2	2/1	1/2
7	Ecological concern	1/6	1/4	1/1	1/4	1/8	1/6	1/6
8	System scale	1/4	1/2	4/1	1/1	1/3	1/1	1/1
9	Impact on EPES	4/1	2/1	8/1	3/1	1/1	4/1	2/1
10	Financial impact	2/1	1/2	6/1	1/1	1/4	1/1	2/1
11	Asset criticality	1/1	2/1	6/1	1/1	1/2	1/2	1/1





common platform enumeration

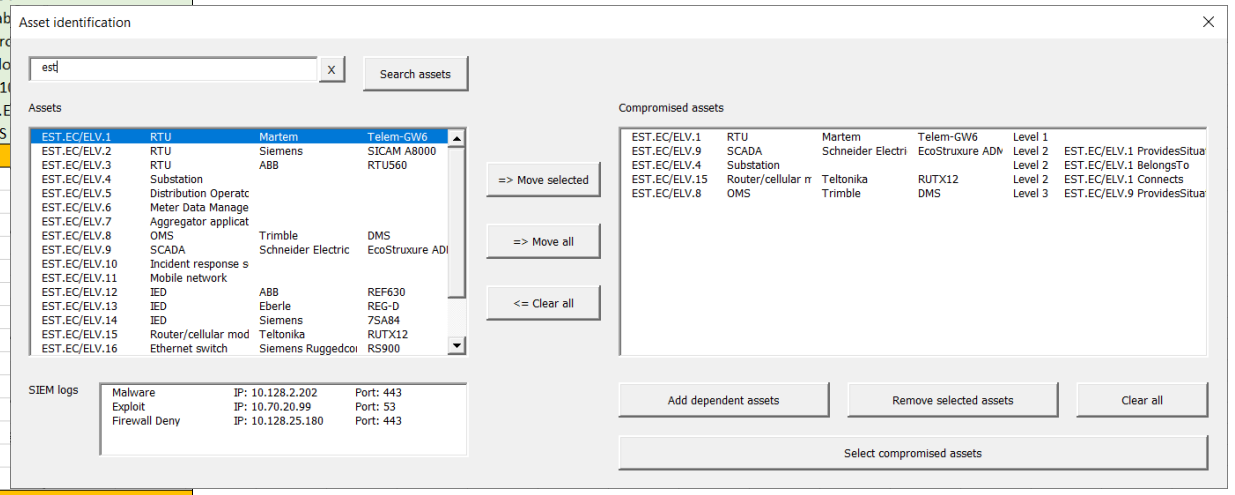
NATIONAL VULNERABILITY DATABASE NVD

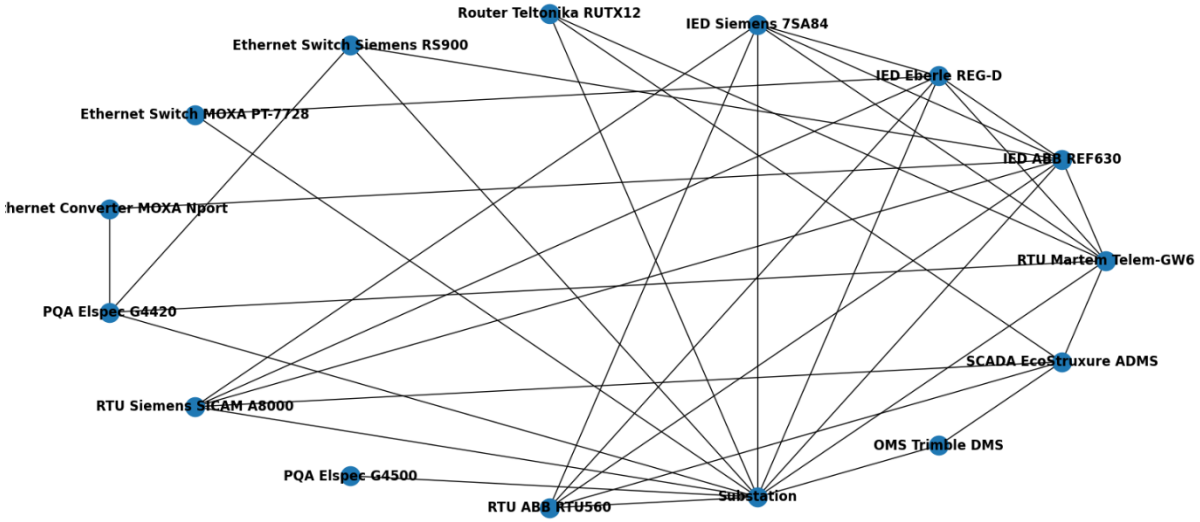
MITRE | ATT&CK®

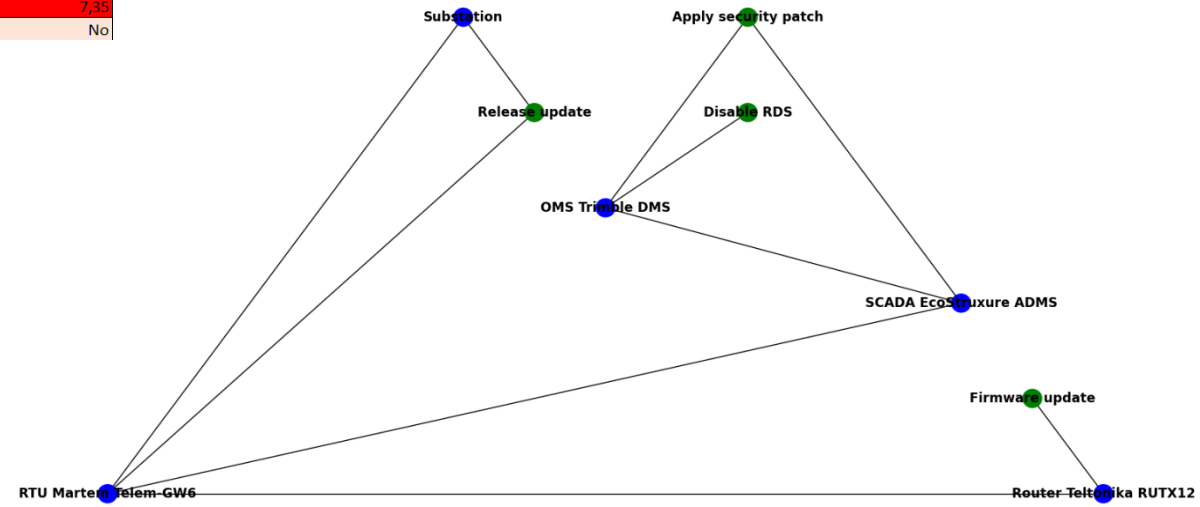
INFORMATIKA

Remediation of cascading effects

Mitigation ID				M005	M003	M006	M004
Mitigation description				Apply security patch	Release update	Firmware update	Disab
Mitigation source				SE	ABB / NVD	Teltonika	Micro
Incident type				Firewall Deny	Firewall Deny	Firewall Deny	Explo
Attack techniques				T0886, T0888	T0814	T0814, T1105, T1190	T121
Asset ID				EST.EC/ELV.9	EST.EC/ELV.4, EST.EC/ELV.15	EST.EC/ELV.4, EST.EC/ELV.15	EST.E
Asset type				SCADA	Substation, Router/cellular moc	Substation, Router/cellular moc	OMS
Incident impact score				6,01	5,08	5,67	
Technical requirements	Expertise	0,20	0,25	2,00	4,00	8,00	
	Equipment		0,25	2,00	4,00	8,00	
	Cost		0,25	4,00	4,00	7,00	
	Time		0,25	4,00	5,00	6,00	
Scope	Scope	0,10	1,00	3,00	6,00	7,00	
Environmental	Assets	0,10	1,00	3,00	6,00	6,00	
IS impact	Availability	0,20	0,34	4,00	4,00	6,00	
	Integrity		0,33	4,00	4,00	5,00	
	Confidentiality		0,33	4,00	4,00	5,00	
Business impact	Financial	0,20	0,34	4,00	5,00	3,00	
	Reputation		0,33	5,00	5,00	7,00	
	Operational		0,33	5,00	6,00	9,00	
Business constraints	RTO	0,20	0,50	2,00	3,00	6,00	
	RPO		0,50	2,00	3,00	5,00	
Mitigation score				3,33	4,52	6,18	5,23
Mitigation veto				0,00	0,36	0,75	0,44
Effective mitigation score				3,33	6,50	9,04	7,35
Selected				Yes	Yes	No	No







INFORMATIKA

Discussion

INFORMATIKA d.o.o.
Vetrinjska ulica 2 | 2000 Maribor | Slovenija
T: +386 2 707 10 00
E-mail: info@informatika.si
www.informatika.si

Andrej Bregar
andrej.bregar@informatika.si