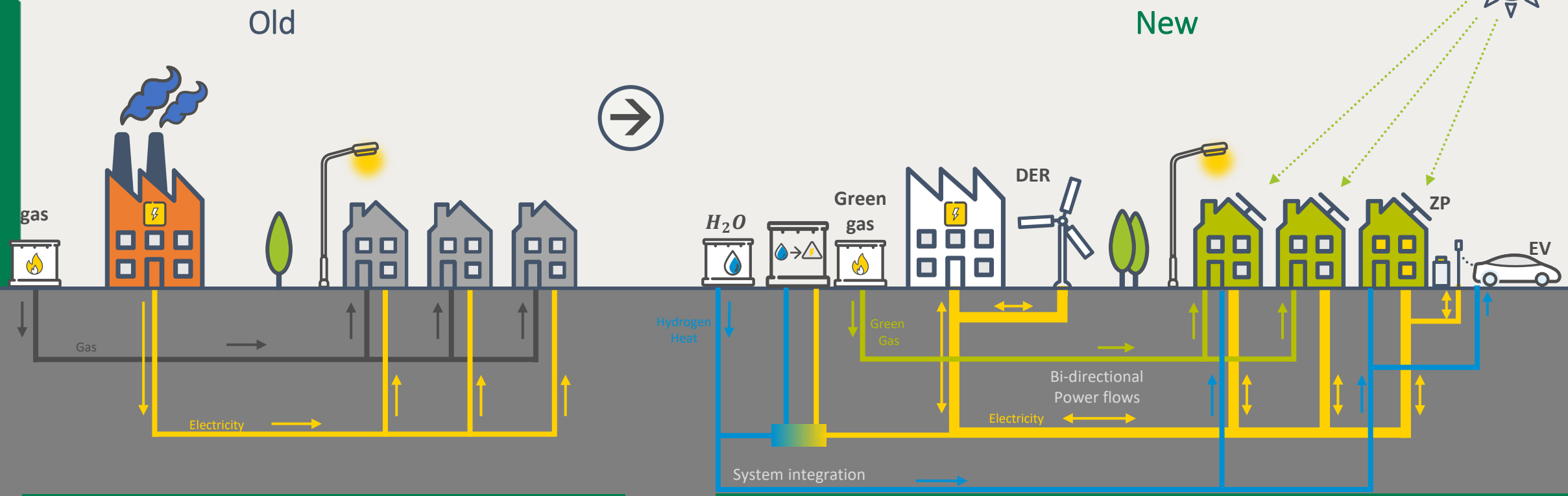
D2 Information Systems and Telecommunication

Amadou Louh (Netstrateeg Telecom, Stedin)
Alex Stefanov (Assistant Professor, TU Delft)

cigre
For power system expertise

Reliable energy grids for a successful energy transition

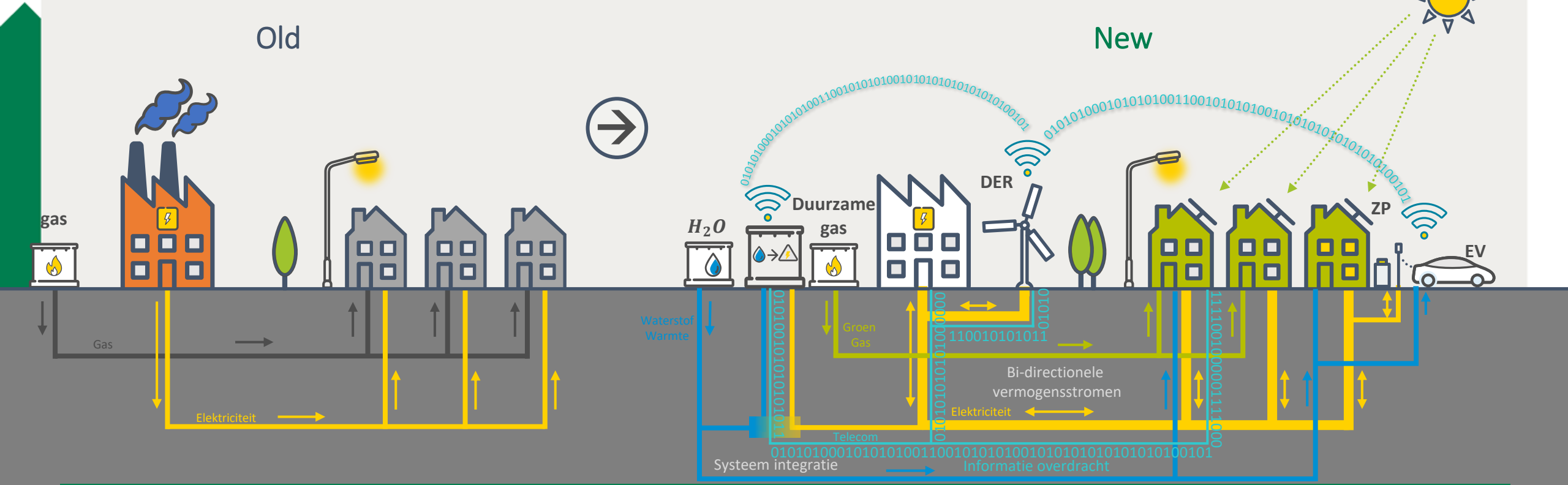


- ‘Old’, robust, reliable and deterministic
- Increase in capacity- en quality constrains/bottlenecks
- → Congestion with risk of overload

- Integrated, distributed, flexible, sustainable energy system
- More: complex, critical, dynamic and stochastic
- More sensors (condition-based maintenance) → more data
- Challenge: Get the energy where needed, on time, safely and efficiently without compromising system stability

Digital revolution in the ‘Power system of systems’

Information becomes leading and is a pre-requisite for power flows



- As the Power Grid becomes SMART, more control & automation based on ‘forecasting’ is required
- Information exchange is required to orchestrate power flows → Communication & IT/OT becomes critical and essential to assure the correct functioning of the energy infrastructure.

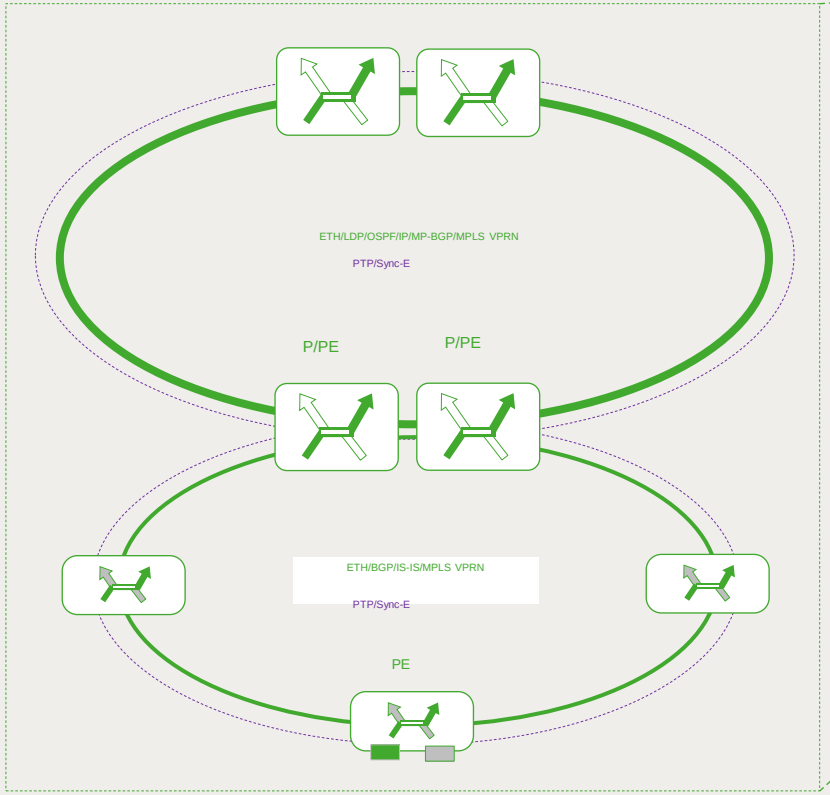
Statement

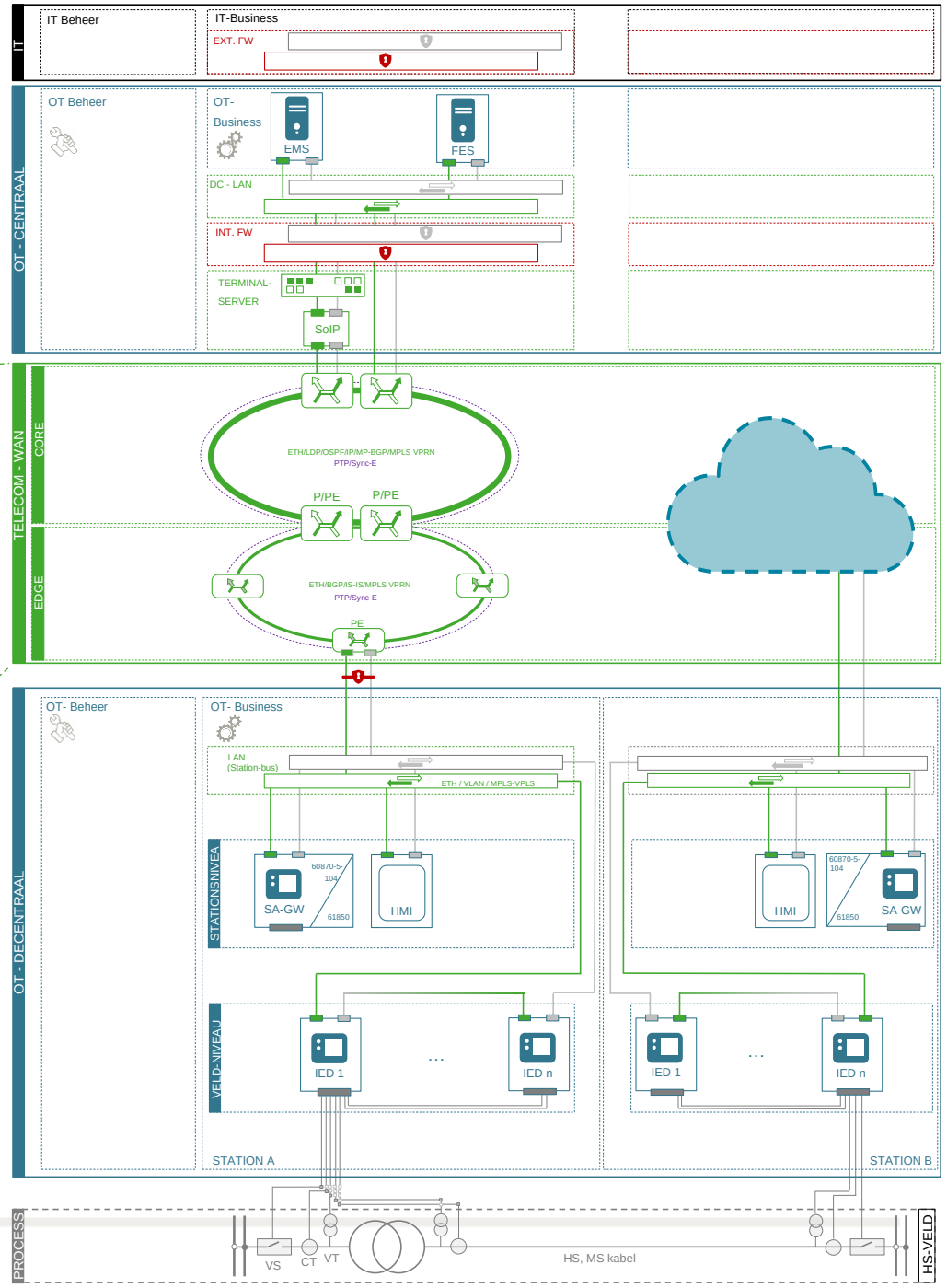
Information becomes leading and is a pre-requisite for power flows

- As the Power Grid becomes SMART, more control & automation based on ‘forecasting’ is required
- Information exchange is required to orchestrate power flows → Communication & IT/OT becomes a prerequisite, critical and essential to assure the correct functioning of the energy infrastructure.

- Therefore we need to consider cyber security of telecommunication, IT and OT-systems earlier in the system planning phase.

OT Architecture - WAN





Cyber Attack Scenarios

Scenario:

WAN is compromised because an attacker takes control of the network control plane

- Shuts down all the interfaces at all the routers
- Configures access lists to drop packets and prevent them to reach a specific subnet

--> All destinations unreachable

Questions:

- What is your plan B?
- How do you recover?
- How to prevent the reoccurrence of the attack?

Best practices

Management plane protection

- External firewall, management plane security, Node hardening (login control, password security, console and Management port AAA control (authorization order, exit-on-reject, TACACS+ & local authentication, Radius, IEEE802.1x, SSH, SNMPv3, etc.),, Event-logging, …

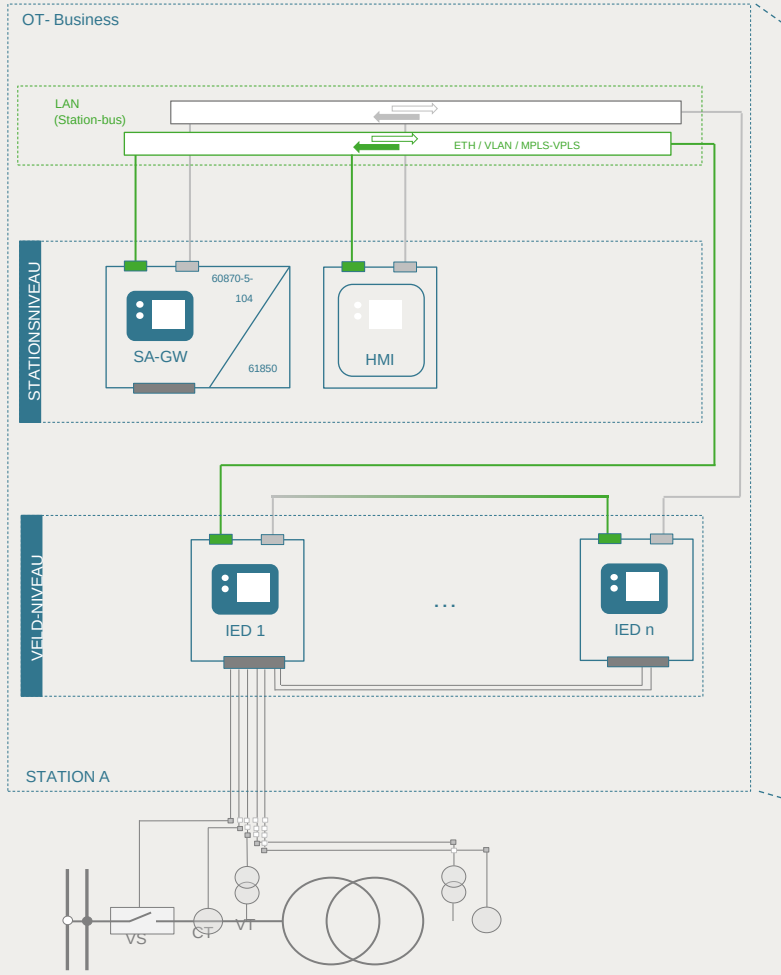
Control plane protection

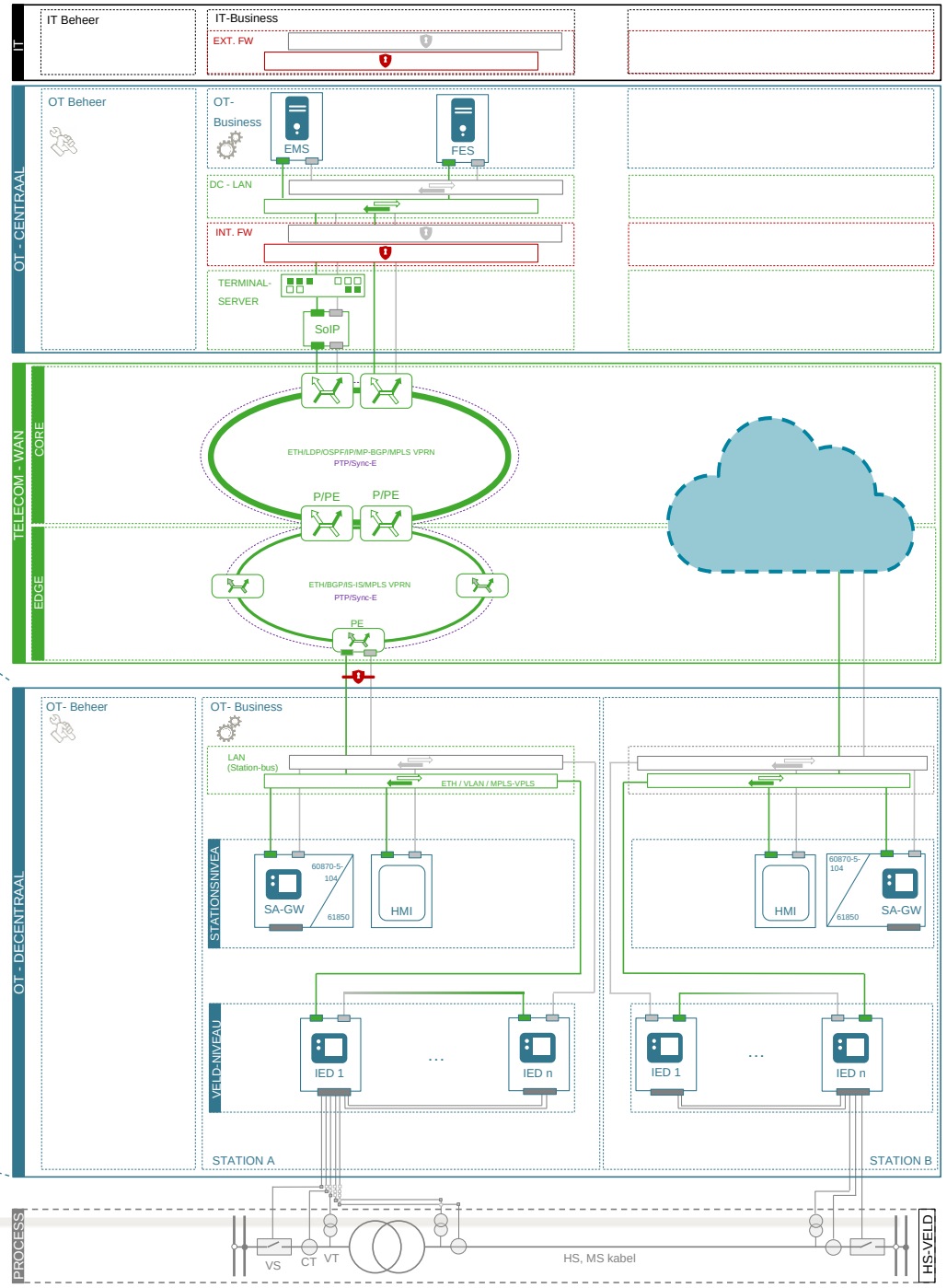
- Rate-limiting (CPU overload), CPM filter, IPv4 configuration, Encryption, keychain authentication, keychain (BGP, IS-IS, LDP, RSVP), generalized TTL, …

Data plane protection

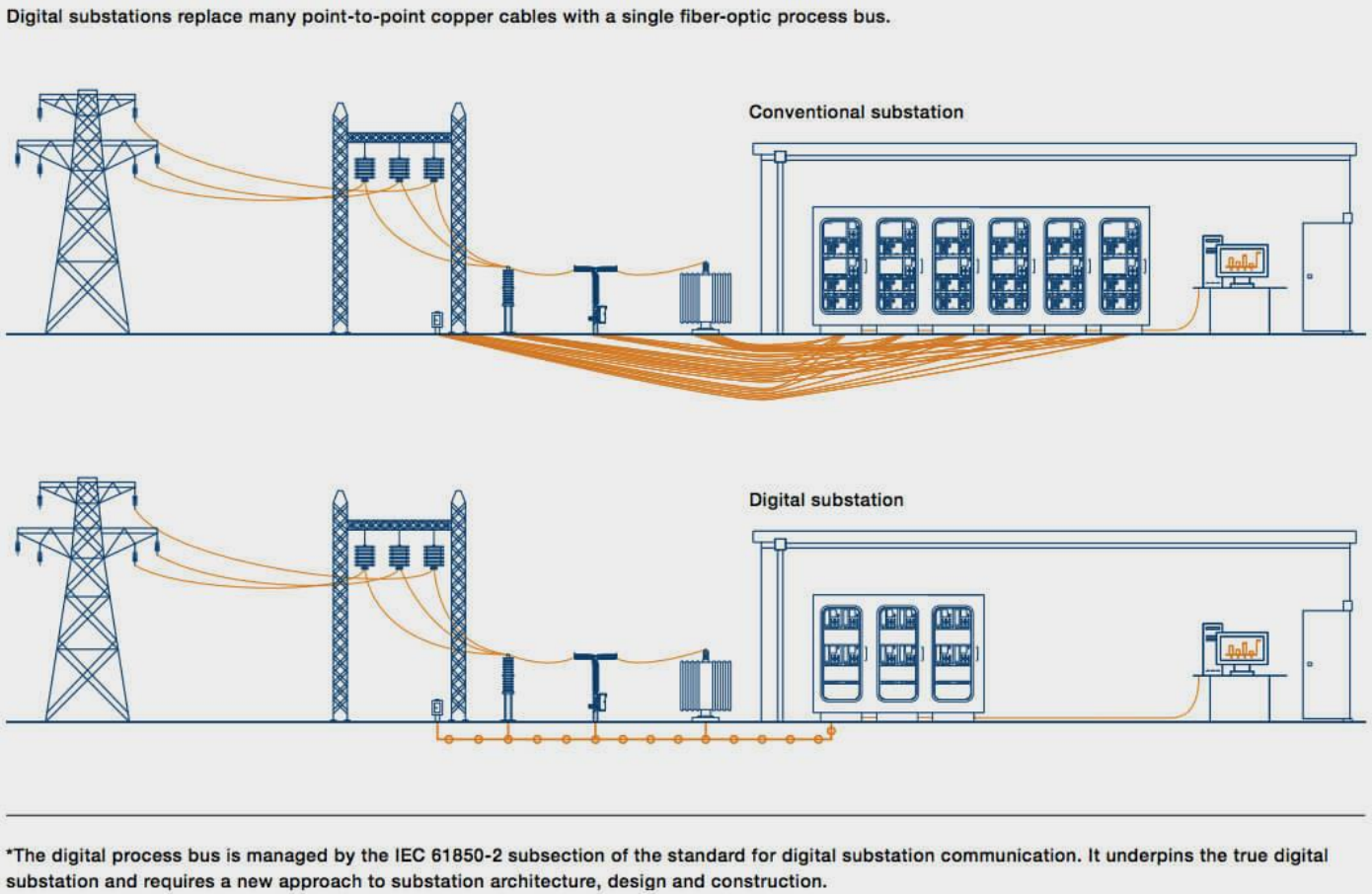
- Network segregation (L1, L2, L3, …), zones, segments, …
- Encryption, MAC learning, DHCP snooping, IPS, IDS, …

OT Architecture – Substation level





Digital Substations & IEC 61850 Standard



Source: ABB, IEC 61850 in Digital Substation and Cyber security

IEC 61850 protocols

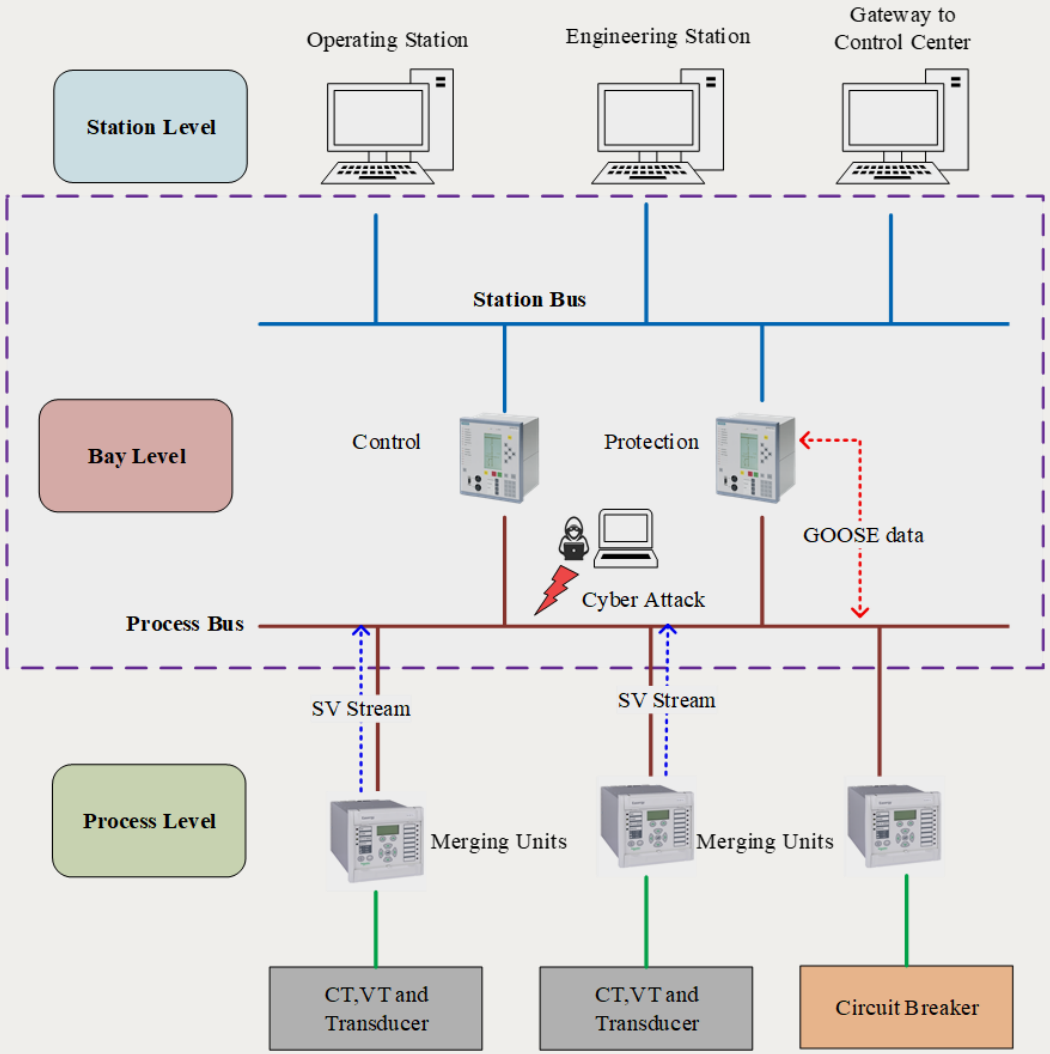
- Generic Object-Oriented Substation Event (GOOSE)
- Sampled Values (SV)
- Manufacturing Messaging Service (MMS)

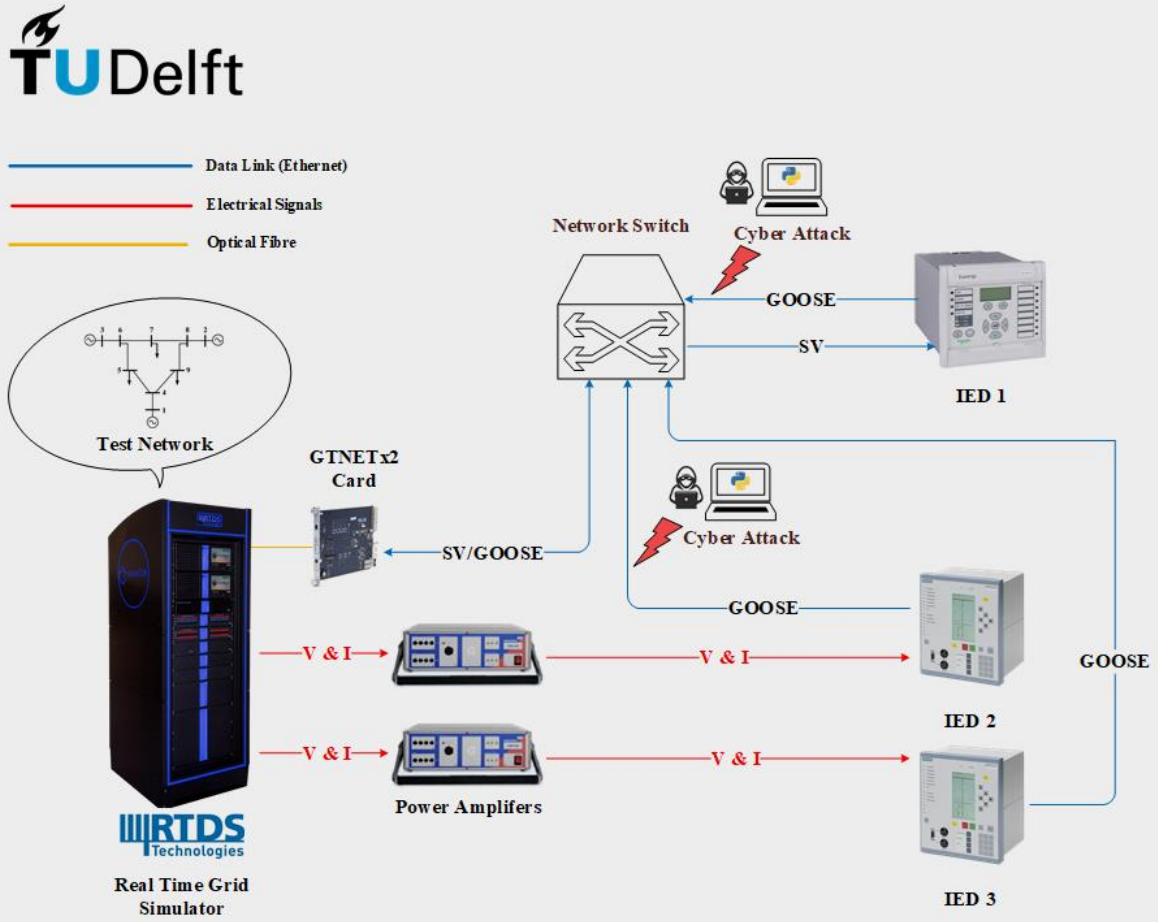
IEC 61850 cyber threats

- GOOSE and SV susceptible to spoofing and man-in-the-middle attacks
- MMS susceptible to session hijacking, replay, and packet sniffing and spoofing attacks

IEC 62351-6 standard developed to secure IEC 61850 protocols

Cyber Attacks on IEC 61850 in Digital Substations





Control Room of the Future (CRoF) Technology Centre at TU Delft

Director: Dr Alex Stefanov, e-mail: A.I.Stefanov@tudelft.nl

Control Room of the Future (CRoF) Technology Centre at TU Delft

Director: Dr Alex Stefanov, e-mail: A.I.Stefanov@tudelft.nl

Control Room of the Future (CRoF) Technology Centre at TU Delft

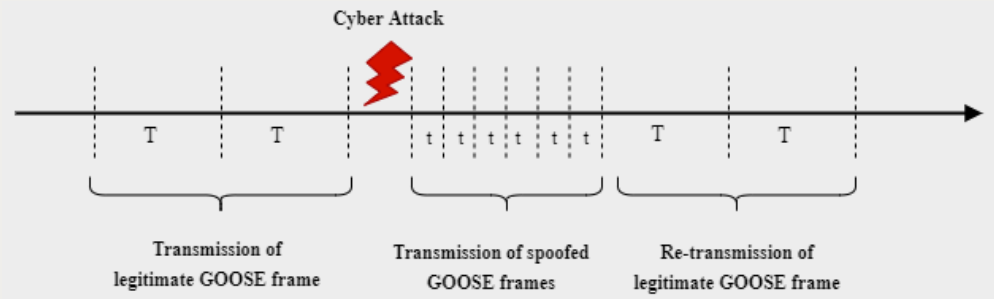
Director: Dr Alex Stefanov, e-mail: A.I.Stefanov@tudelft.nl

Cyber Attacks on IEC 61850 in Digital Substations

Pseudocode: Injection of spoofed IEC 61850 traffic

```
Monitor network interface;
Filter packet based on type 0x88b8 (GOOSE);
Filter packet based on type 0x88ba (SV);
Capture filtered packets as p_cap;
i= 0, n= number of p_cap;
src = source MAC address;
dst = destination MAC address;
while (i < n) do
        p_spoof = Get and modify payload of p_cap;
        Send packet (src, dest, VLAN, p_spoof);
        i++;
end
```

Cyber attacks on GOOSE

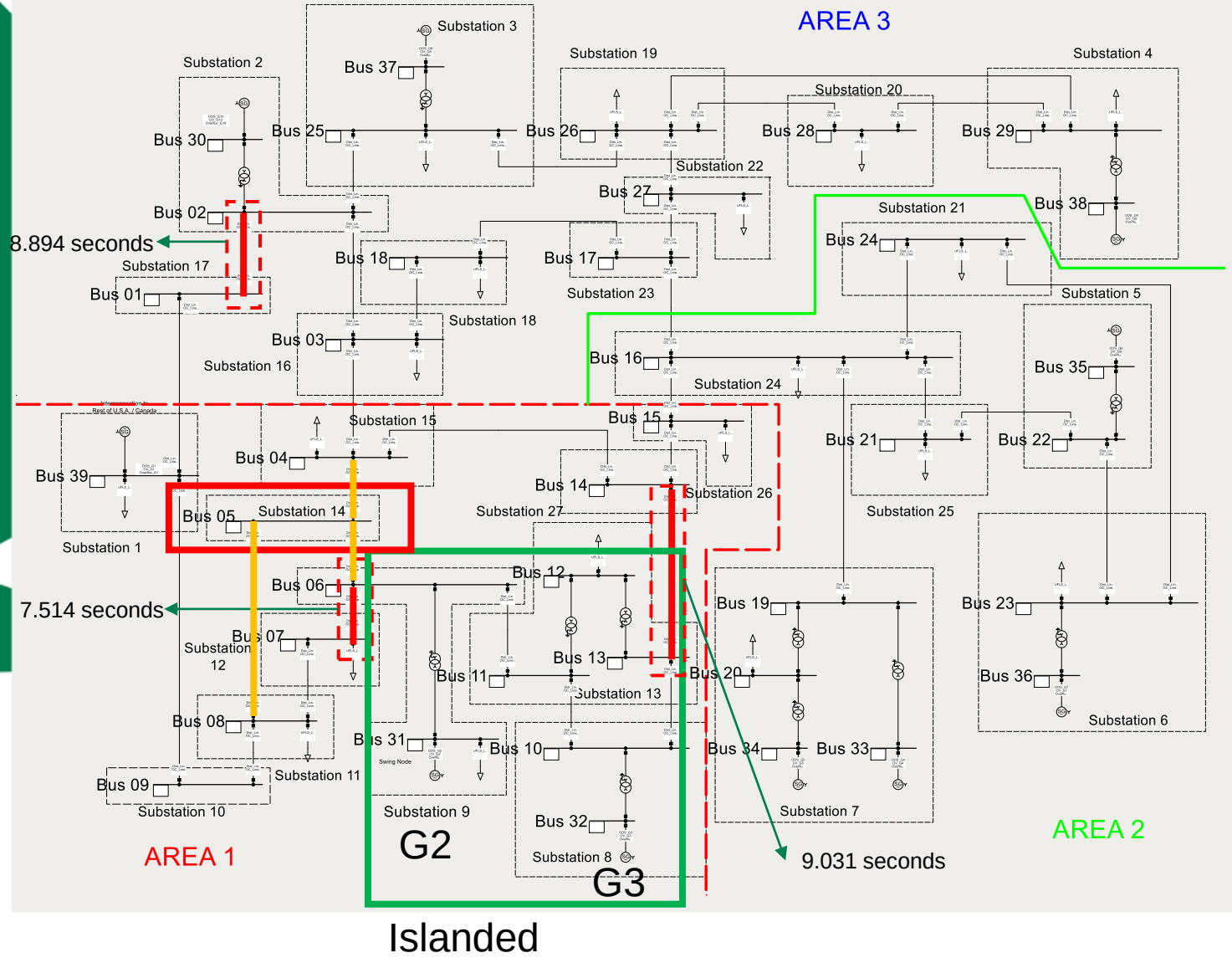


Normal operation GOOSE frame	Cyber attack: False GOOSE frame
gocbRef: P446_SVSystem/LLN0GOgcb01	gocbRef: P446_SVSystem/LLN0GOgcb01
timeAllowedtoLive: 2001	timeAllowedtoLive: 5
t: Mar 28, 1994 03:42:25.531999945 UTC	t: Mar 20, 1994 22:04:09.076999962 UTC
stNum: 95	stNum: 99
sqNum: 80850	sqNum: 0
numDatSetEntries: 10	numDatSetEntries: 10
allData: 10 items	allData: 10 items
Data: boolean (3)	Data: boolean (3)
boolean: False	**boolean: True**

Result of spoofing cyber attacks on IEC 61850 protocols

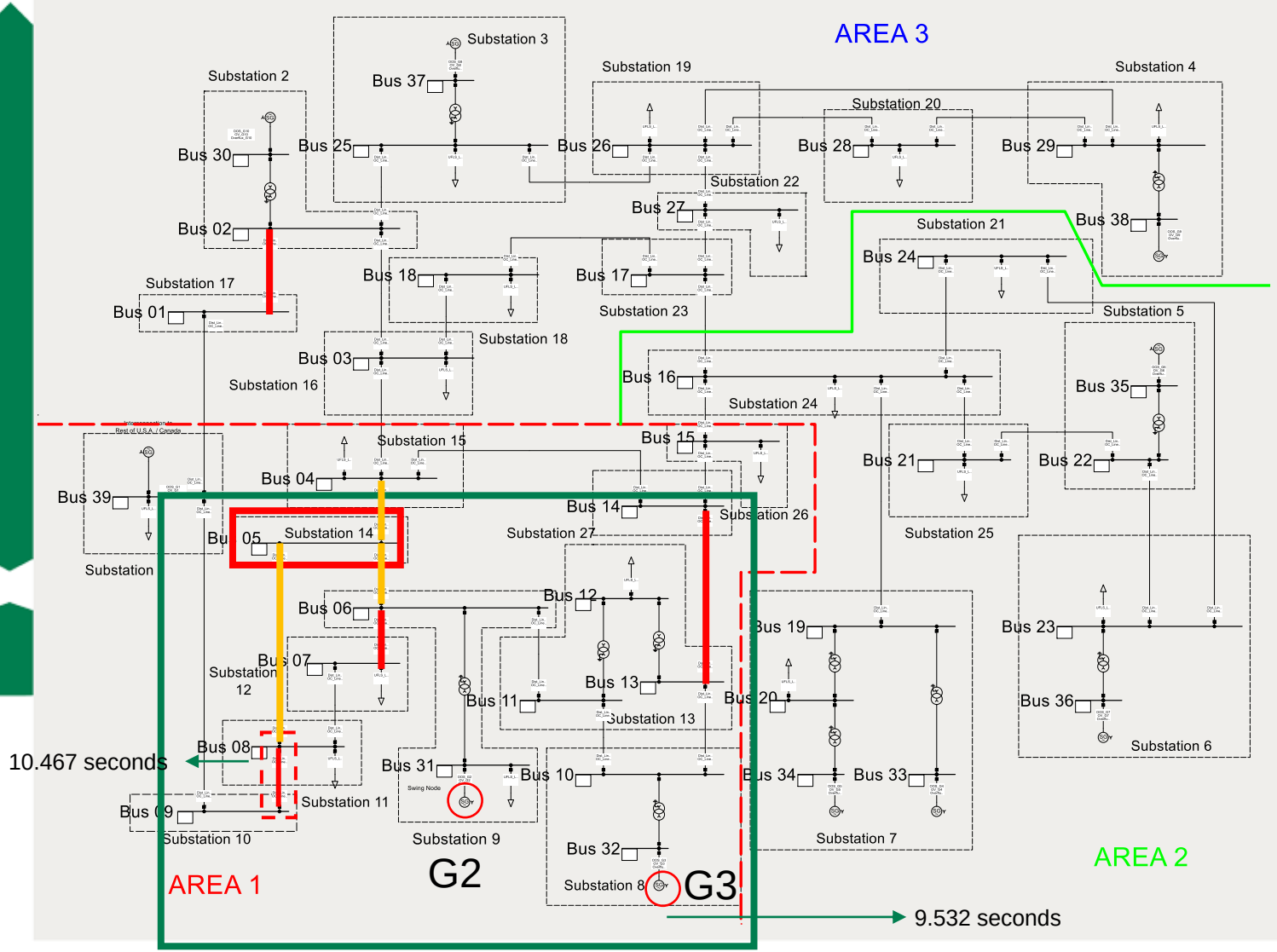
- GOOSE: opens circuit breakers
- GOOSE: disables interlocking and opens disconnectors on load, leading to a fault
- SV: fabricates abnormal conditions for voltage, frequency and ROCOF, leading to protection tripping
- SV: blocks protection relays

IEEE 39-Bus System: Coordinated GOOSE Attack on 2 Substations



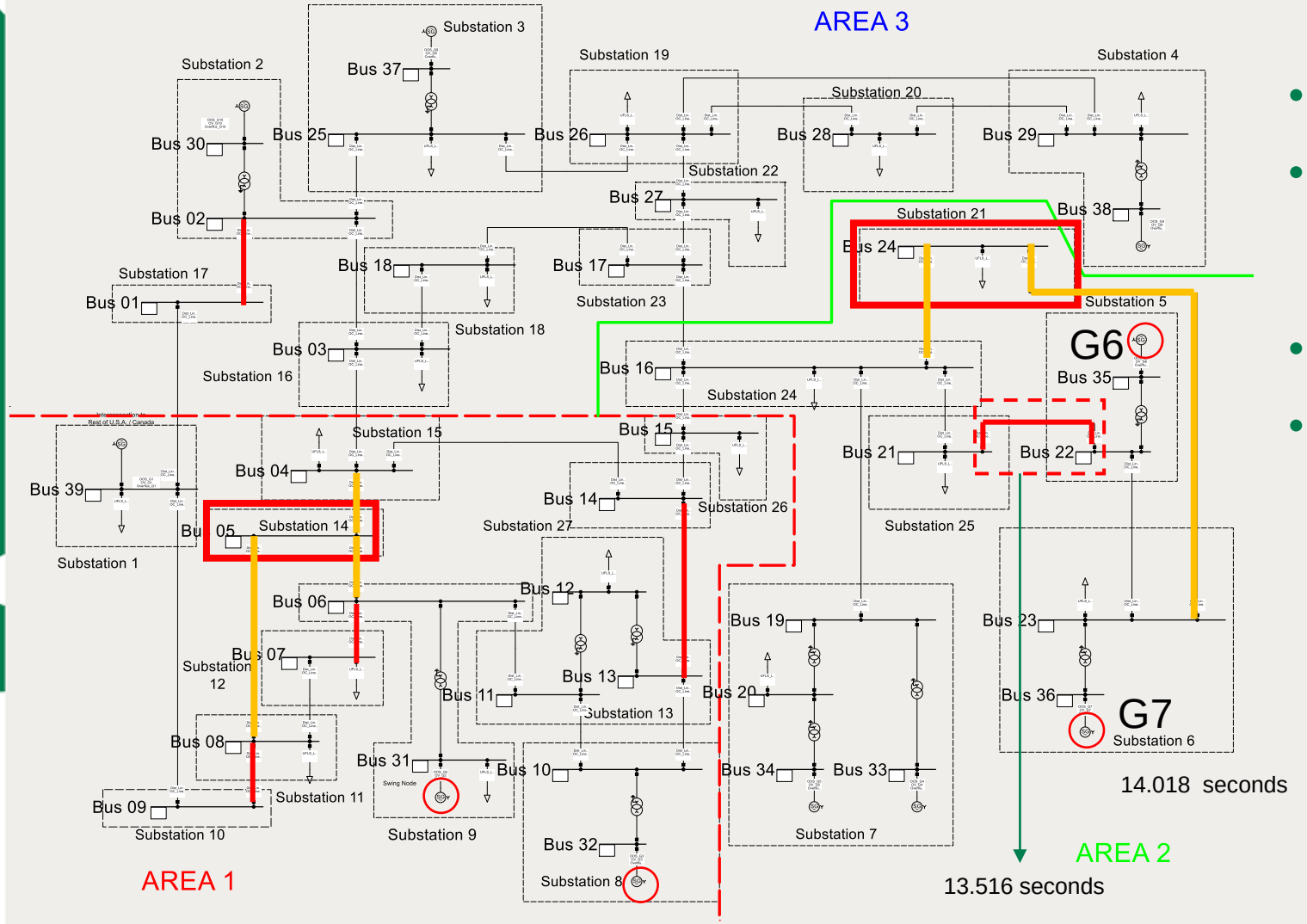
- Cyber attack on substation 14
- Lines 05-06, 05-08 and 04-05 maliciously disconnected by spoofed IEC 61850 GOOSE
- Multiple lines tripped due to distance protection
  - Distance relay confuses heavy loading, coupled with low system voltages for uncleared zone 3 fault as the impedance enters the third zone of protection
  - Observed in real-world cascading failures and blackouts: USA-Canada 2003, Turkey 2015
- Generators G2 and G3 form an island

IEEE 39-Bus System: Coordinated GOOSE Attack on 2 Substations



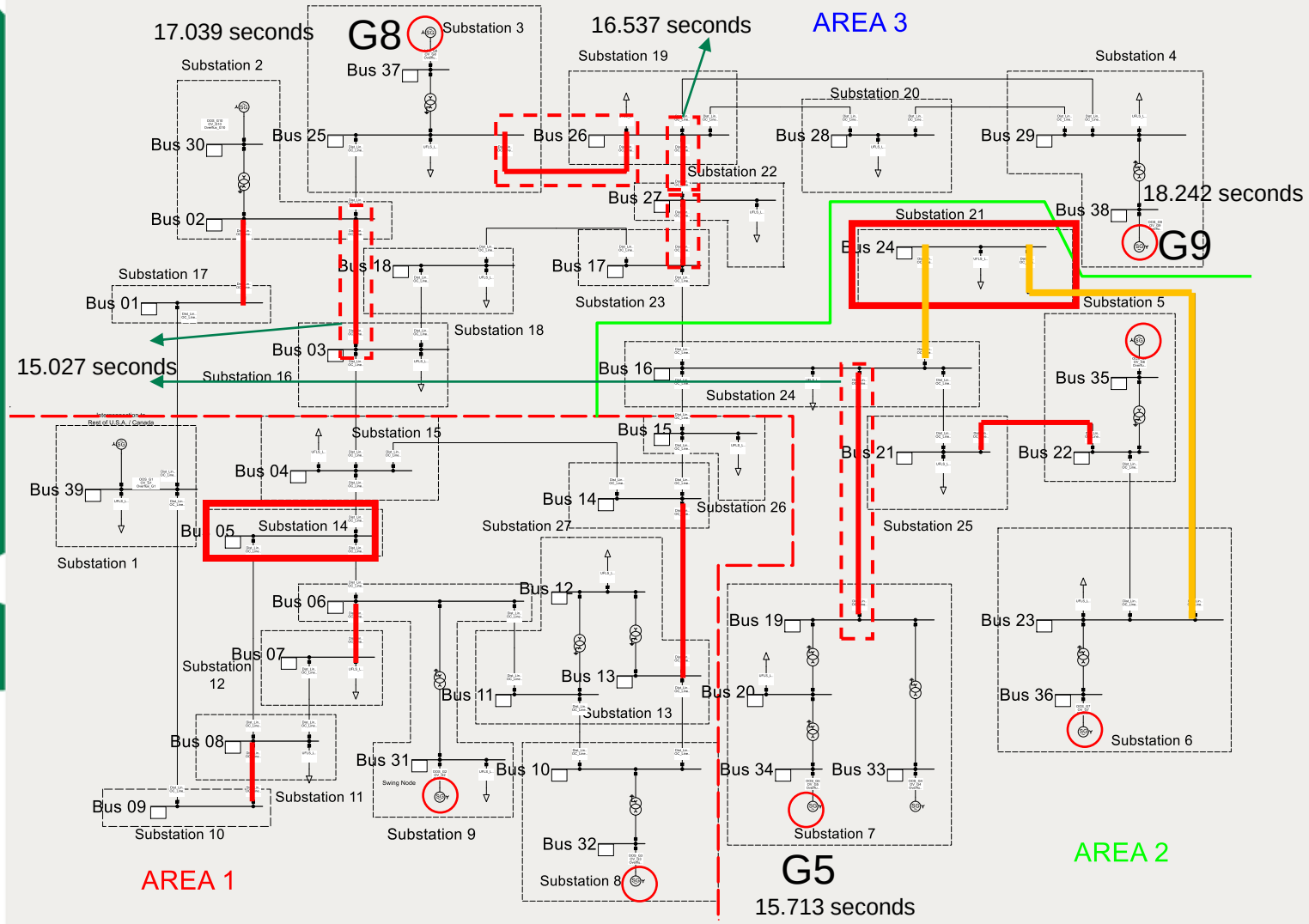
- Generators G2 and G3 trip due to ROCOF protection
- Line 08-09 trips on distance protection
- Area 1 is unsupplied

IEEE 39-Bus System: Coordinated GOOSE Attack on 2 Substations



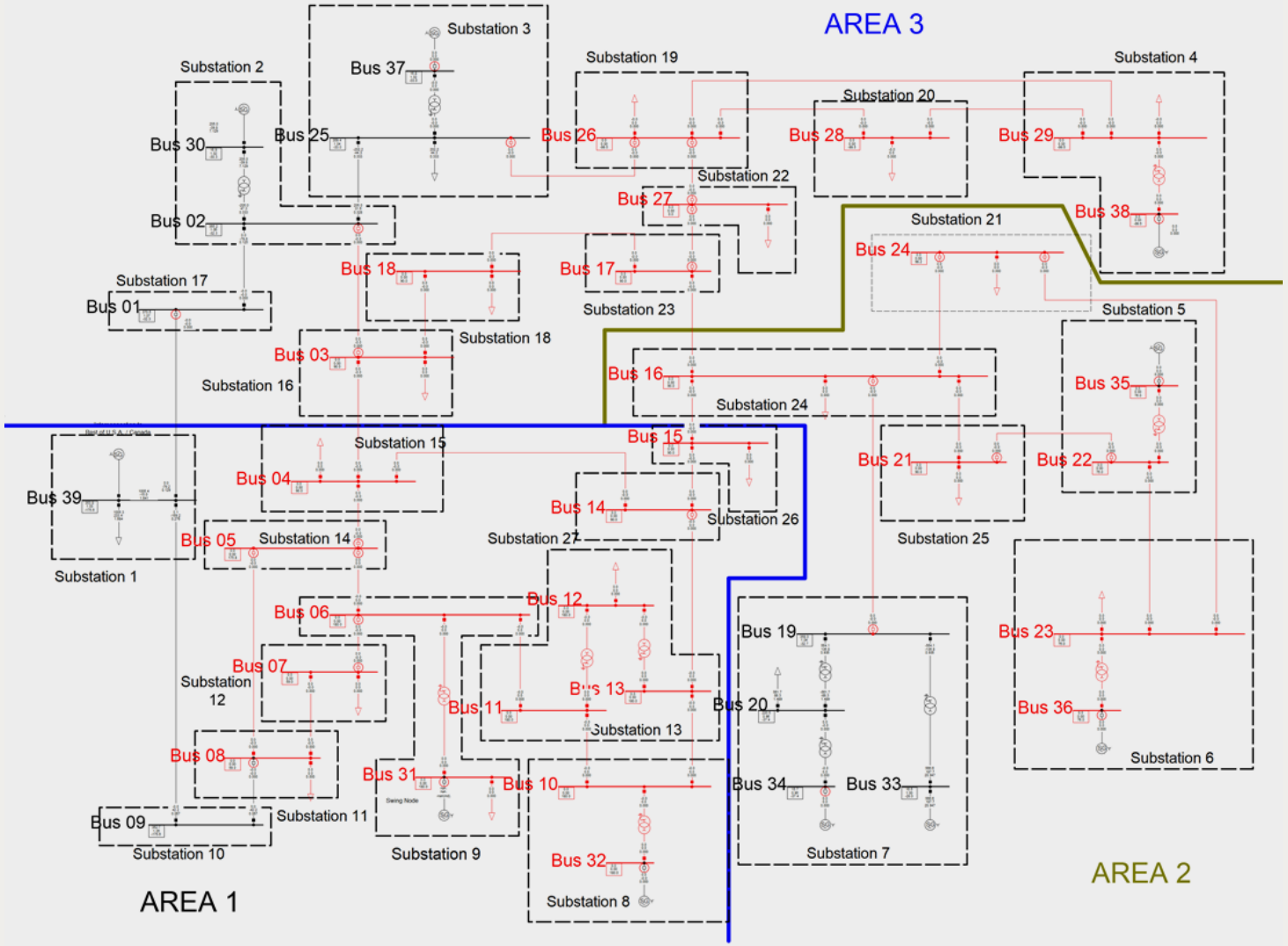
- Cyber attack on substation 21
- Lines 16-24 and 23-24 maliciously disconnected by spoofed IEC 61850 GOOSE
- Distance relay trips line 21-22
- Generators G6 and G7 form an island, and they trip due to ROCOF

IEEE 39-Bus System: Coordinated GOOSE Attack on 2 Substations



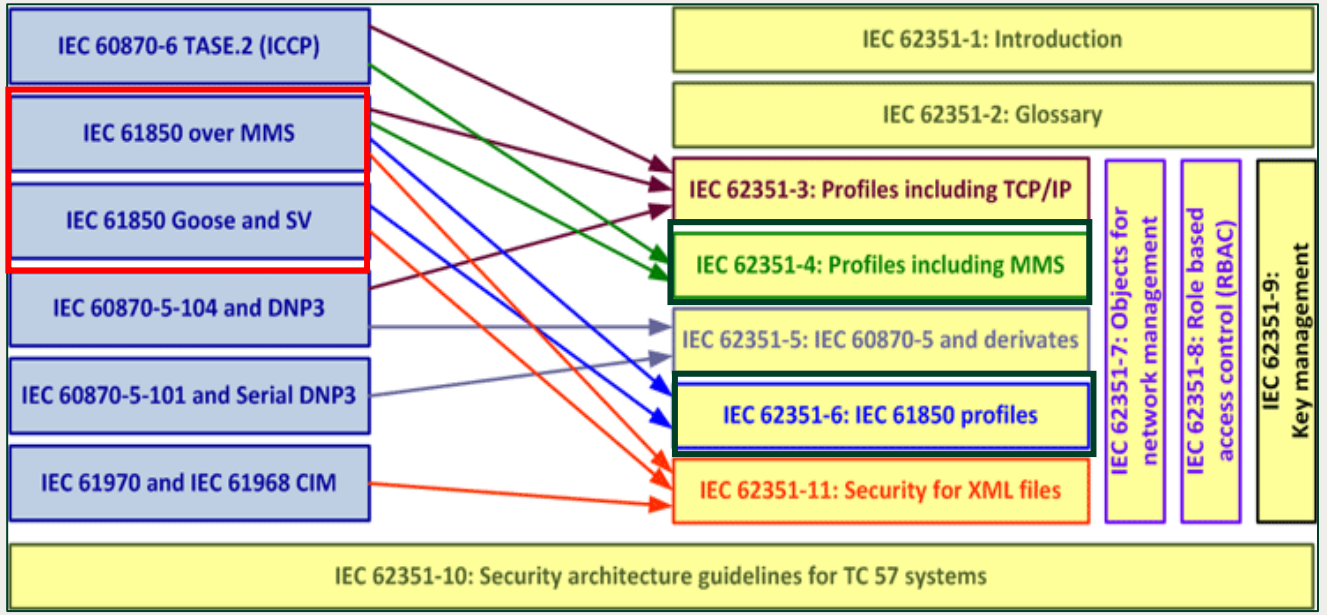
- Lines 02-03 and 16-19 trip due to distance protection
- Generator G5 disconnects due to ROCOF
- Lines 17-27, 25-26, and 26-27 trip due to distance protection
- Generators G8 and G9 disconnect due to ROCOF

GOOSE Cyber Attacks on Two Substations Cause a Blackout



IEC 62351: Overview

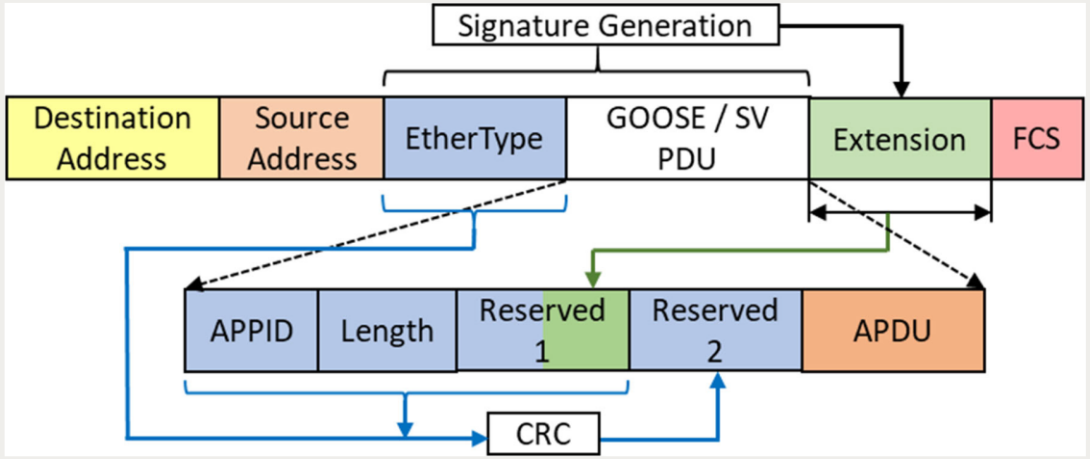
- Provides end-to-end cybersecurity measures for power grids
- Addresses cybersecurity issues of different standards
  - IEC 61850, IEC 60870-5, IEC 61970, etc.
- Part 4: profiles including MMS and derivatives
- Part 6: cyber security for IEC 61850



Source: Int Electrotech Commission, Data and Communications Security—Part 6: Security for IEC 61850, IEC 62351-6, 2.0, 2020

IEC 62351-6: Digital Signatures

- IEC 62351-6:2007 proposes use of Digital Signature (DS) scheme
- DS generated by SHA256 and signed by RSA algorithms
- Appended as extension to GOOSE/SV frame
- Provides security against unauthorised data access, tampering, replay attacks
- Unable to meet latency requirements ~3-4 ms

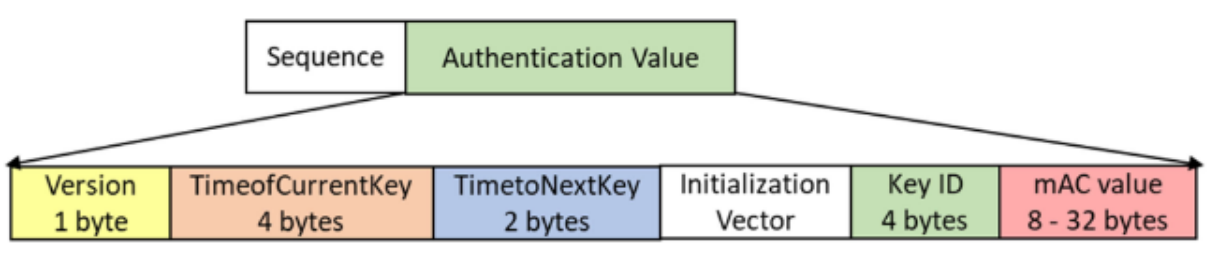


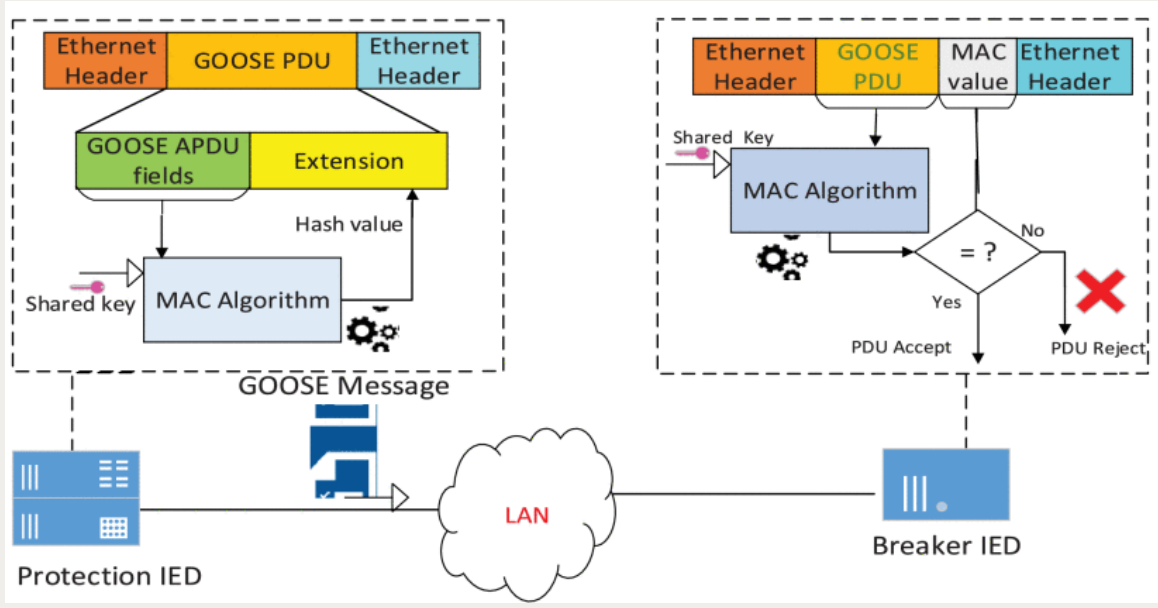
Algorithm	Key Size (bits)	Signing time (ms)	Verification time (ms)
RSA	1024	3.74	0.15
ECDSA	112	3.43	0.22

Source: Hussain et al. Analysis and Implementation of MAC Algorithms for GOOSE Message Security IEEE Access 2019

IEC 62351-6: Message Authentication Codes (MAC)

- DS replaced by MAC value in the extension field of extended GOOSE/SV frame
- SHA256 or AES used as MAC algorithms
- Similar to symmetric encryption: same private key used for generation and verification of MAC values
- Able to meet 3-4ms latency requirements for time critical applications





Source: Hussain et al. Analysis and Implementation of MAC Algorithms for GOOSE Message Security IEEE Access 2019

IEC 62351-6: Message Authentication Codes (MAC)

Algorithm	Computational Time (micro s)	Latency (micro s)	
		Average	Max
HMAC-SHA-256	14.3	75.7	78.0
AES-GMAC-64	6.6	73.0	75.3
AES-GMAC-128	7.0	74.9	77.1

Source: Hussain et al. A Review of IEC 6231 Security Mechanisms for IEC 61850 Message Exchanges, IEEE Trans Indus Info, 2020

Mitigation and Cyber Security

Additional fields for digital signatures

Hash-based message authentication codes for data integrity

IEC 62351-6: Cyber security of IEC 61850

Trade-off between protection requirements and cyber security

Key management infrastructure. Lack of adoption

Thank You

Alex Stefanov

Assistant Professor, Chartered Engineer (CEng MIEI)

Email: A.I.Stefanov@tudelft.nl

Cyber Resilient Power Grids (LinkedIn)

Control Room of the Future (LinkedIn)

Intelligent Electrical Power Grids, EEMCS, **TU Delft**
Mekelweg 4, 2628 CD Delft, The Netherlands