Can Cyber Attacks Cause a Blackout?

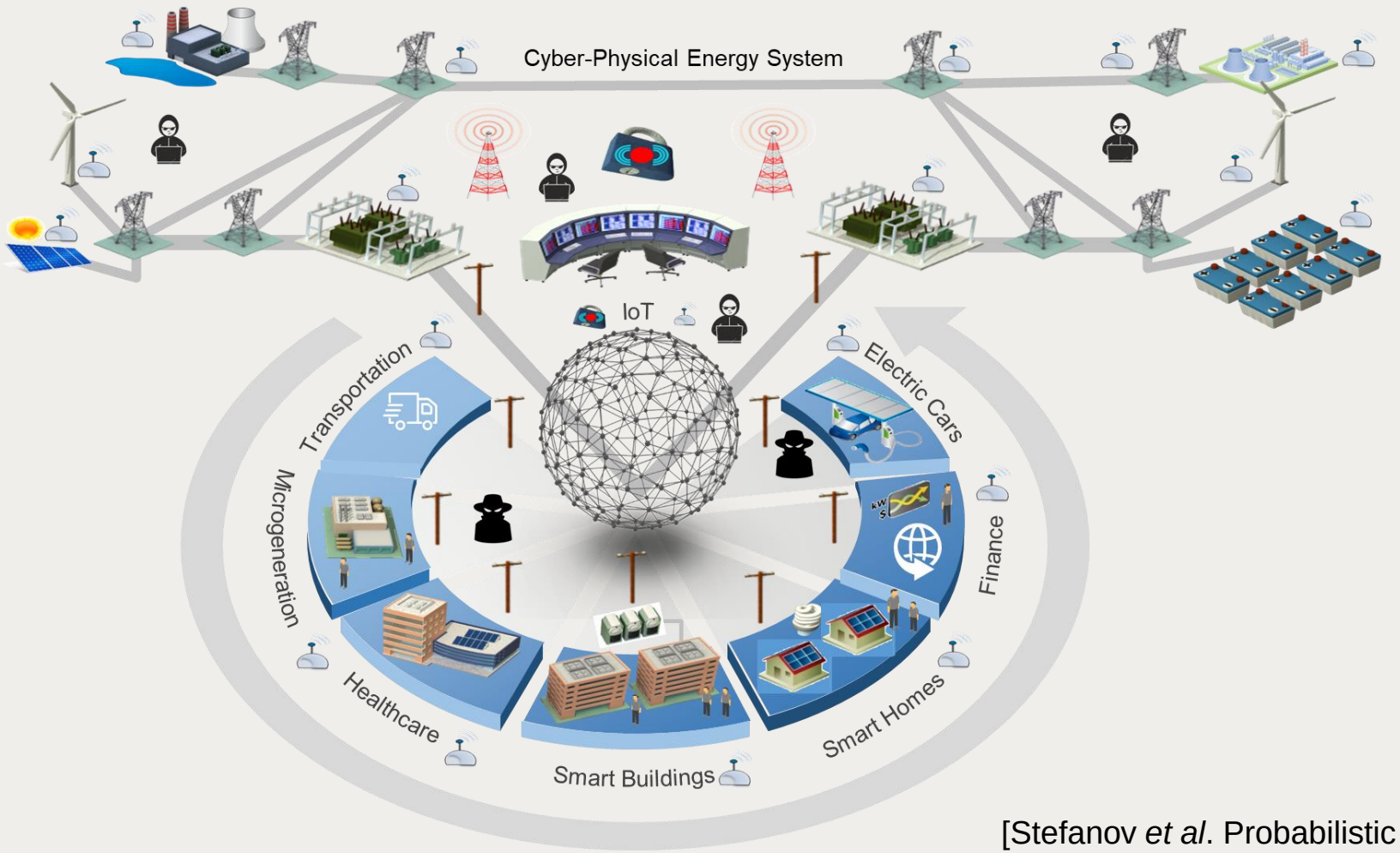
CEng. Dr. Alex Stefanov

Assistant Professor, TU Delft

cigre

For power system expertise

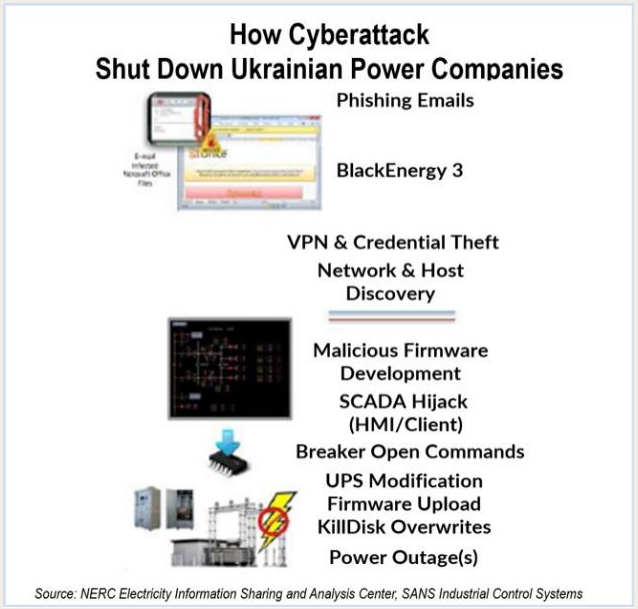
Cyber Security for Power Grids



[Stefanov *et al*. Probabilistic Reliability Analysis of Power Systems, Springer, 2020]

Are Cyber Attacks a Real Threat?

- Cyber attack on the power grid in Ukraine (December 23, 2015)
  - Attackers intruded into IT and SCADA of three DSOs
  - Seven 110 kV and twenty three 35 kV substations disconnected from power grid for 3 hours
  - Cyber attack resulted in power outages that affected 225,000 customers



[Lee *et al*. Analysis of the Cyber Attack on the Ukrainian Power Grid, E-ISAC ICS SANS, 2016]

Are Cyber Attacks a Real Threat?

- Video of cyber attack on power grid in Ukraine (December 23, 2015)
- Source: WIRED
- Link: https://www.wired.com/story/video-hackers-take-over-power-grid-computer-mouse/

Are Cyber Attacks a Real Threat?

The New York Times

U.S. Escalates Online Attacks on Russia's Power Grid

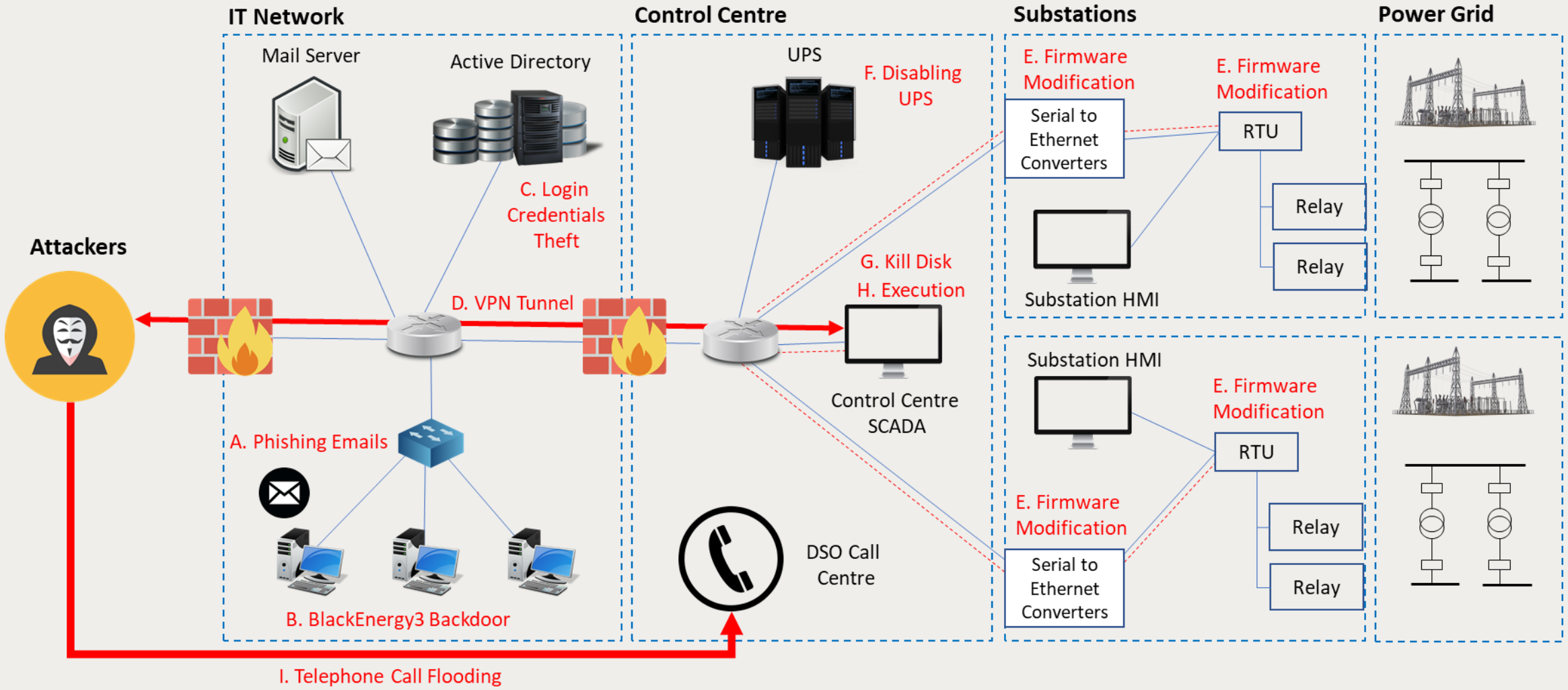
"Advocates of the more aggressive strategy said it was long overdue, after years of public warnings from the Department of Homeland Security and the F.B.I. that Russia has inserted malware that could sabotage American power plants, oil and gas pipelines, or water supplies in any future conflict with the United States." (Source: The New York Times, June 15, 2019)

"But now the American strategy has shifted more toward offense, officials say, with the placement of potentially crippling malware inside the Russian system at a depth and with an aggressiveness that had never been tried before. It is intended partly as a warning, and partly to be poised to conduct cyberstrikes if a major conflict broke out between Washington and Moscow."
(Source: The New York Times)

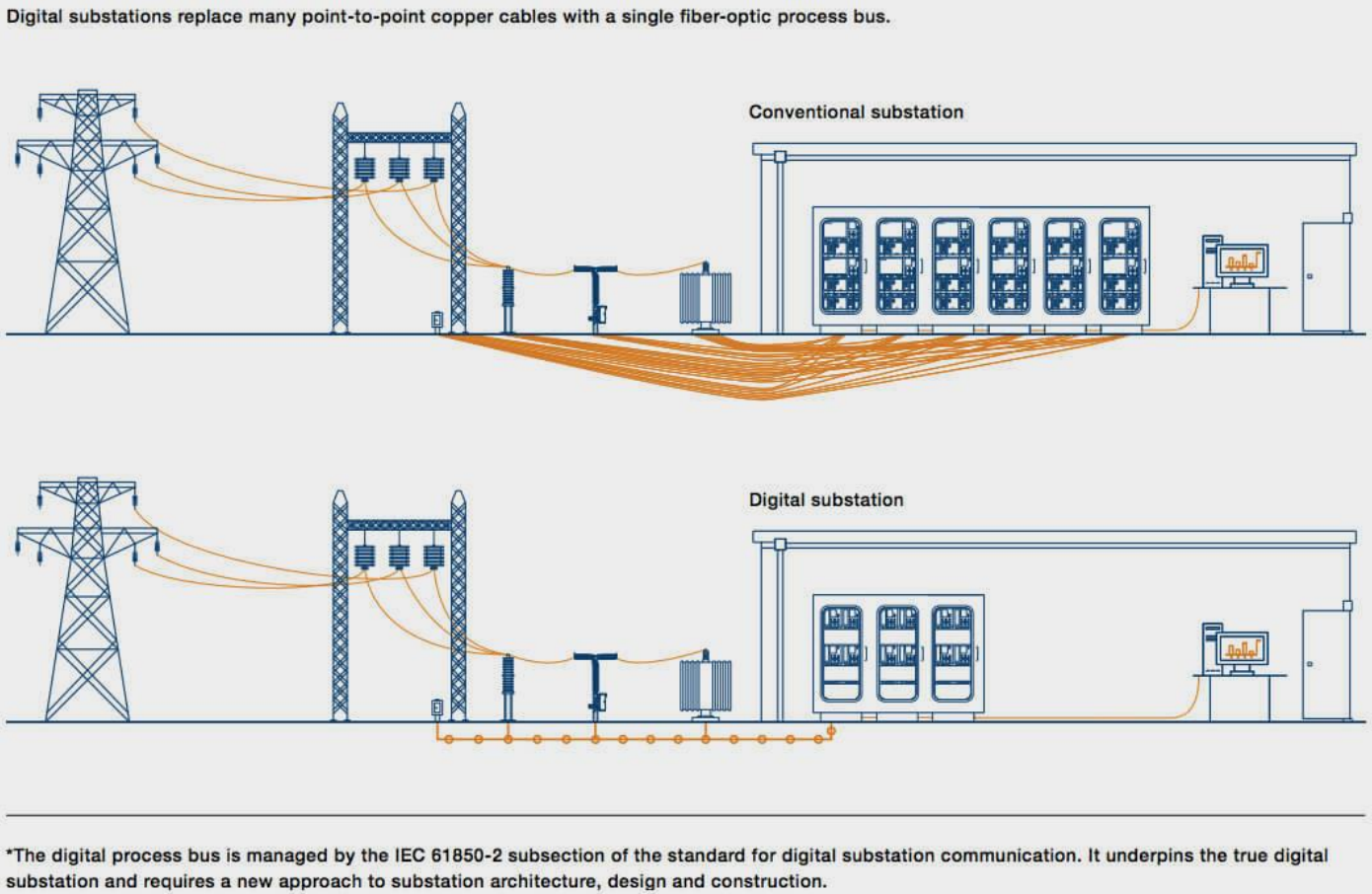
"*A heating power plant in Moscow. Officials described the move into Russia's grid and other targets as a classified companion to more publicly discussed action directed at Moscow's disinformation and hacking units around the 2018 midterm elections*." (Source: The New York Times)

Can Cyber Attacks Cause a European Blackout?

Cyber Attacks on DSO Control Centres in Ukraine 2015



Digital Substations & IEC 61850 Standard



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

IEC 61850 protocols

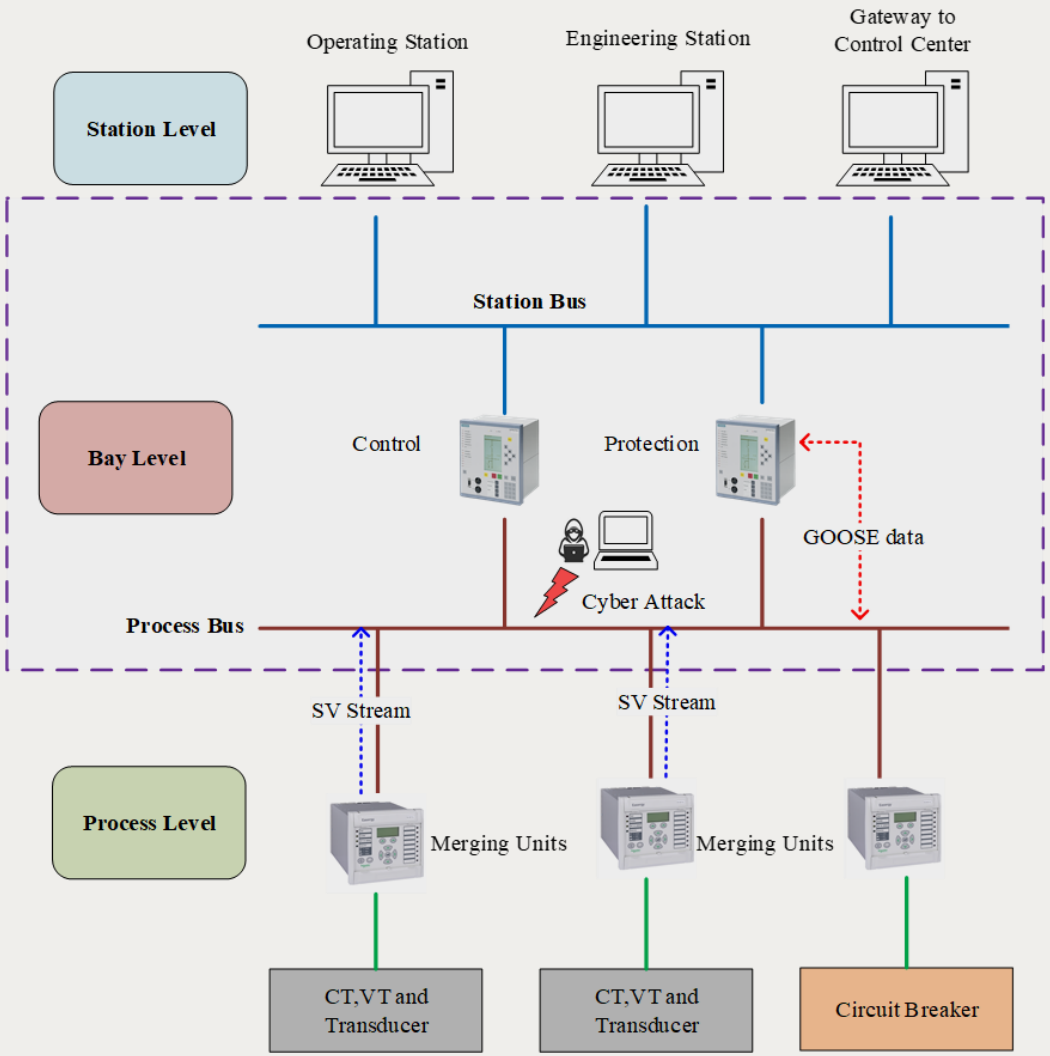
- Generic Object-Oriented Substation Event (GOOSE)
- Sampled Values (SV)
- Manufacturing Messaging Service (MMS)

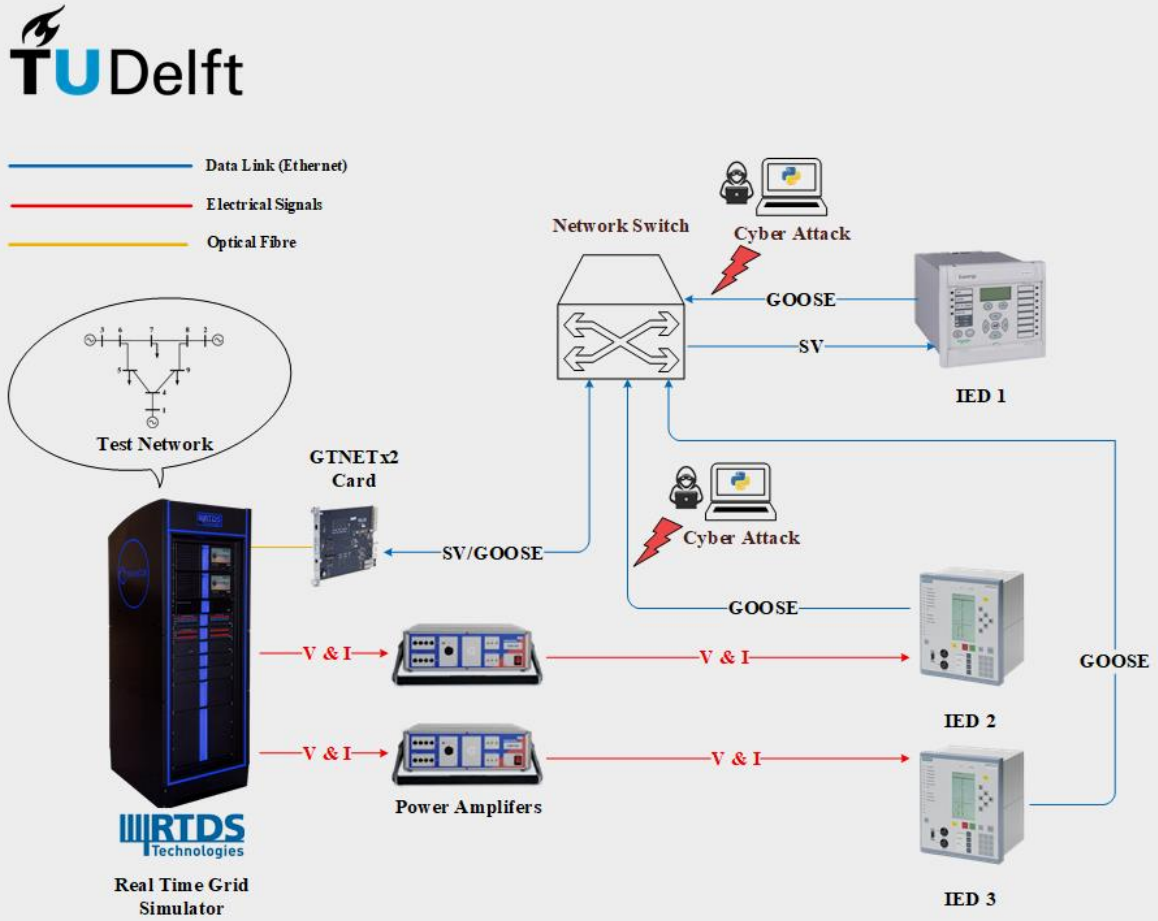
IEC 61850 cyber threats

- 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



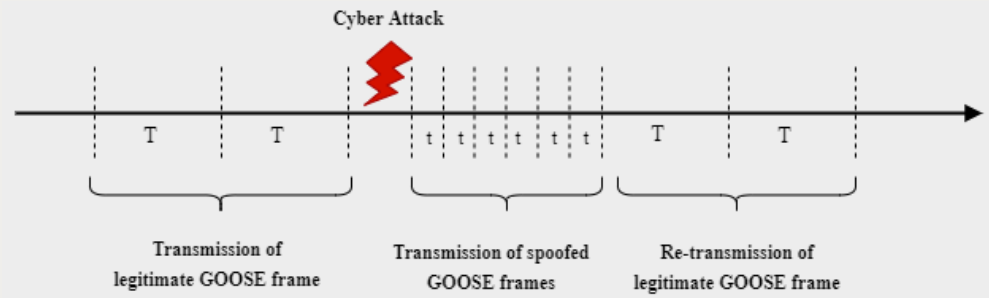


Cyber Attacks on IEC 61850 in Digital Substations

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

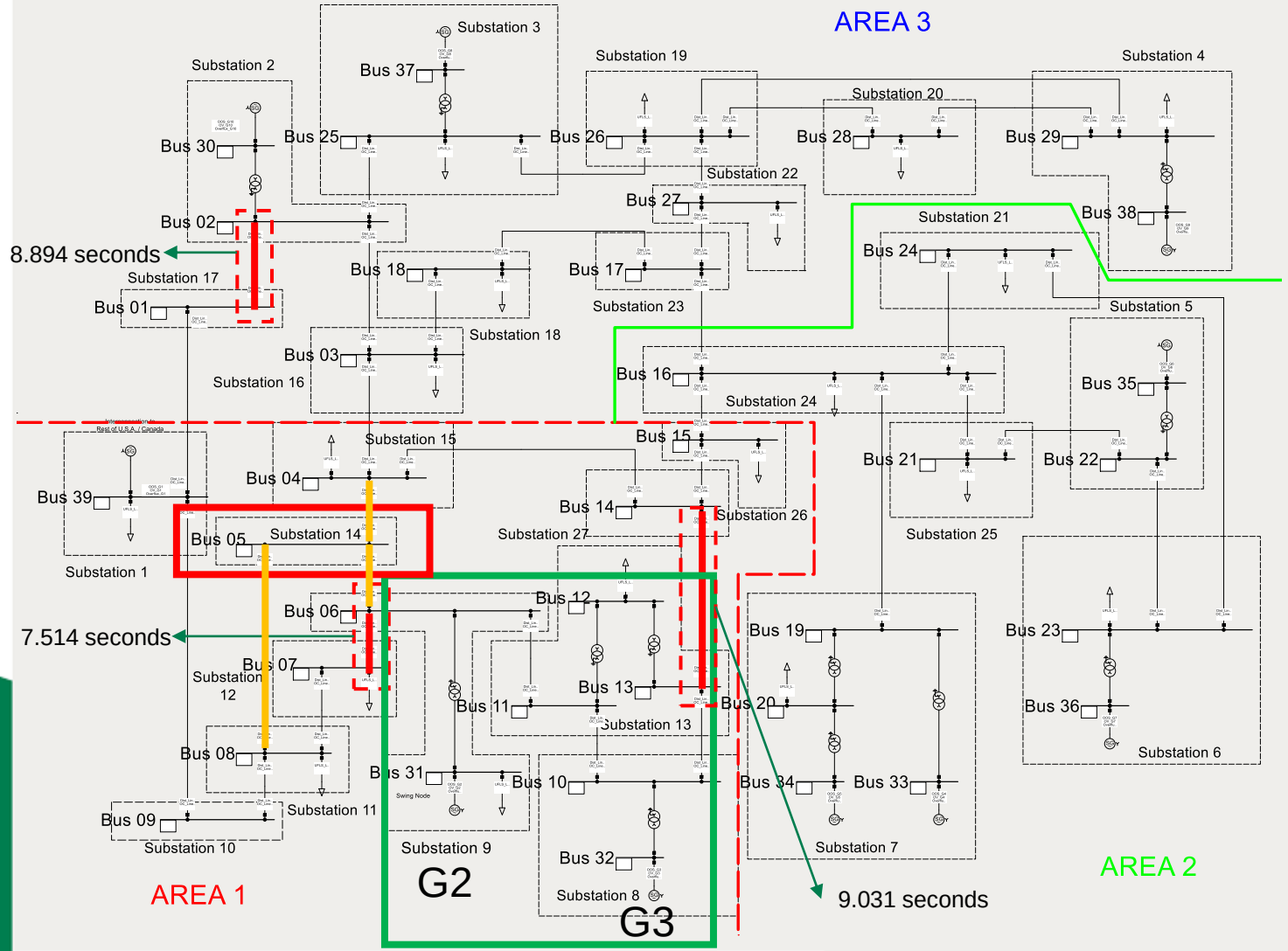


Normal operation GOOSE frame	Cyber attack: False GOOSE frame
gocbRef: P446_SVSystem/LLN0GOgcb01	gocbRef: P446_SVSystem/LLN0GOgcb01
timeAllowedtoLive: 2001	timeAllowedtoLive: 5
t: Mar 28, 1994 03:42:25.531999945 UTC	t: Mar 20, 1994 22:04:09.076999962 UTC
stNum: 95	stNum: 99
sqNum: 80850	sqNum: 0
numDatSetEntries: 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

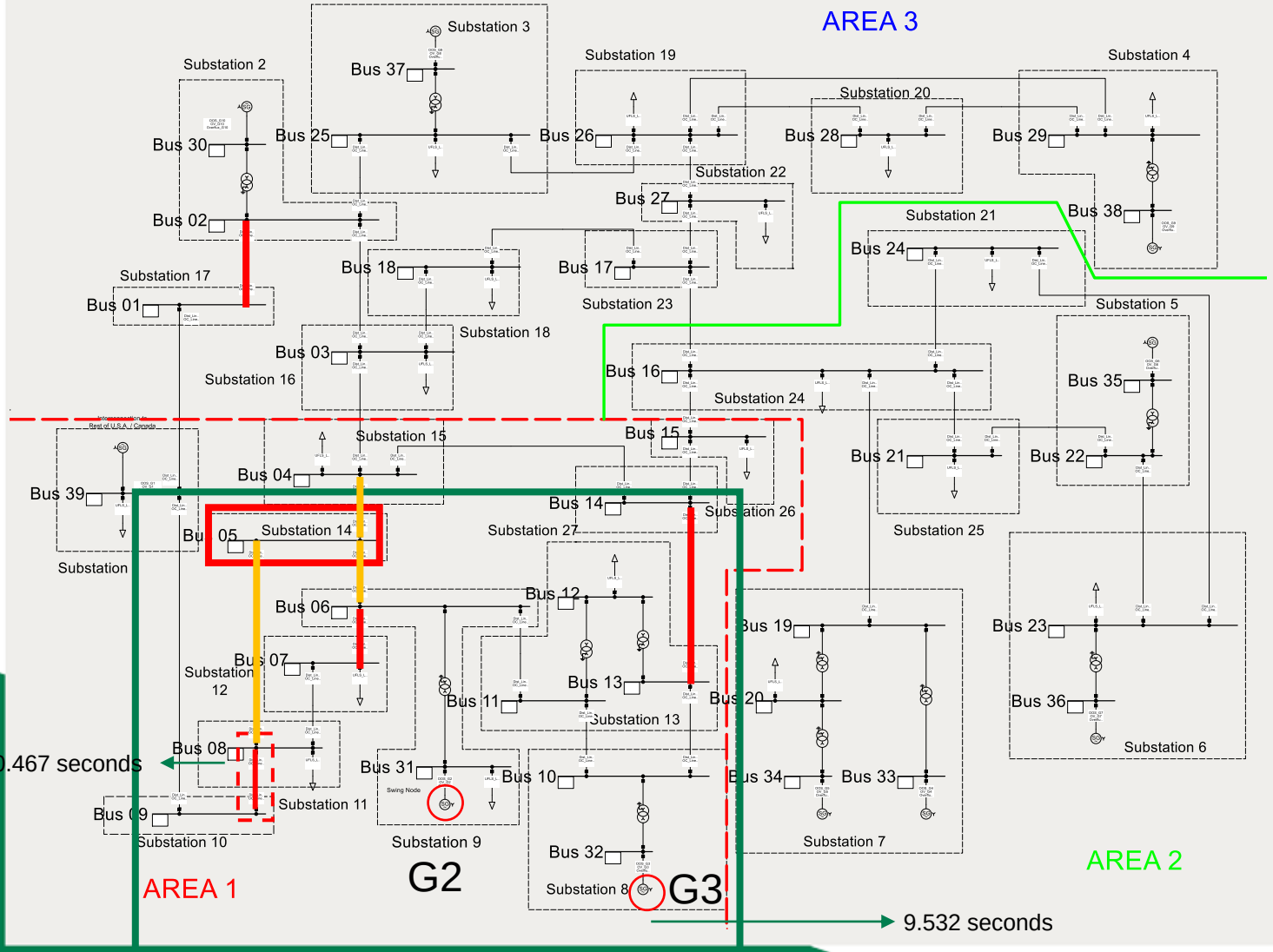
- GOOSE: opens circuit breakers
- GOOSE: disables interlocking and opens disconnectors on load, leading to a fault
- SV: fabricates abnormal conditions for voltage, frequency and ROCOF, leading to protection tripping
- SV: blocks protection relays

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



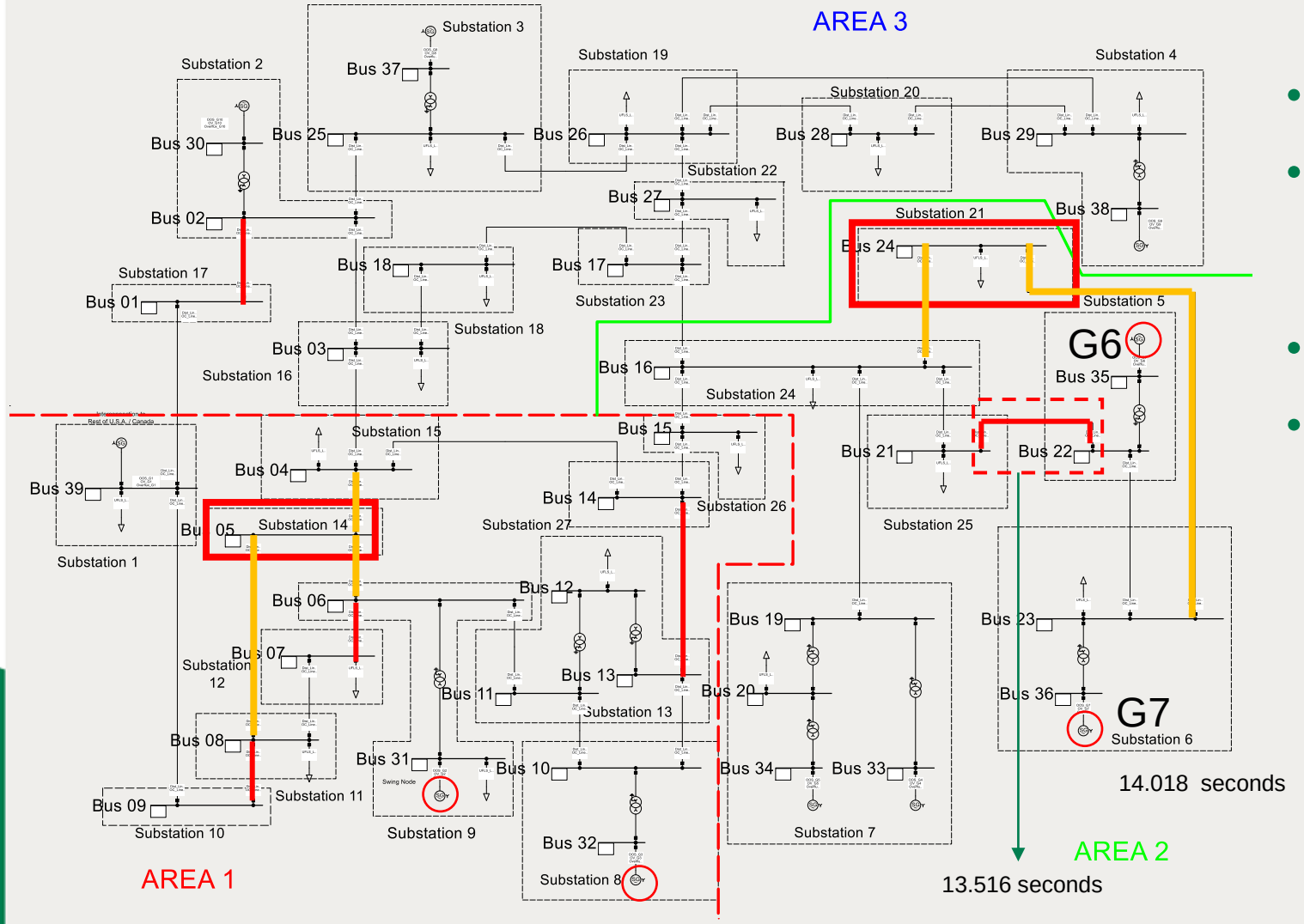
- Cyber attack on substation 14
- Lines 05-06, 05-08 and 04-05 maliciously disconnected by spoofed IEC 61850 GOOSE
- Multiple lines tripped due to distance protection
  - Distance relay confuses heavy loading, coupled with low system voltages for uncleared zone 3 fault as the impedance enters the third 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



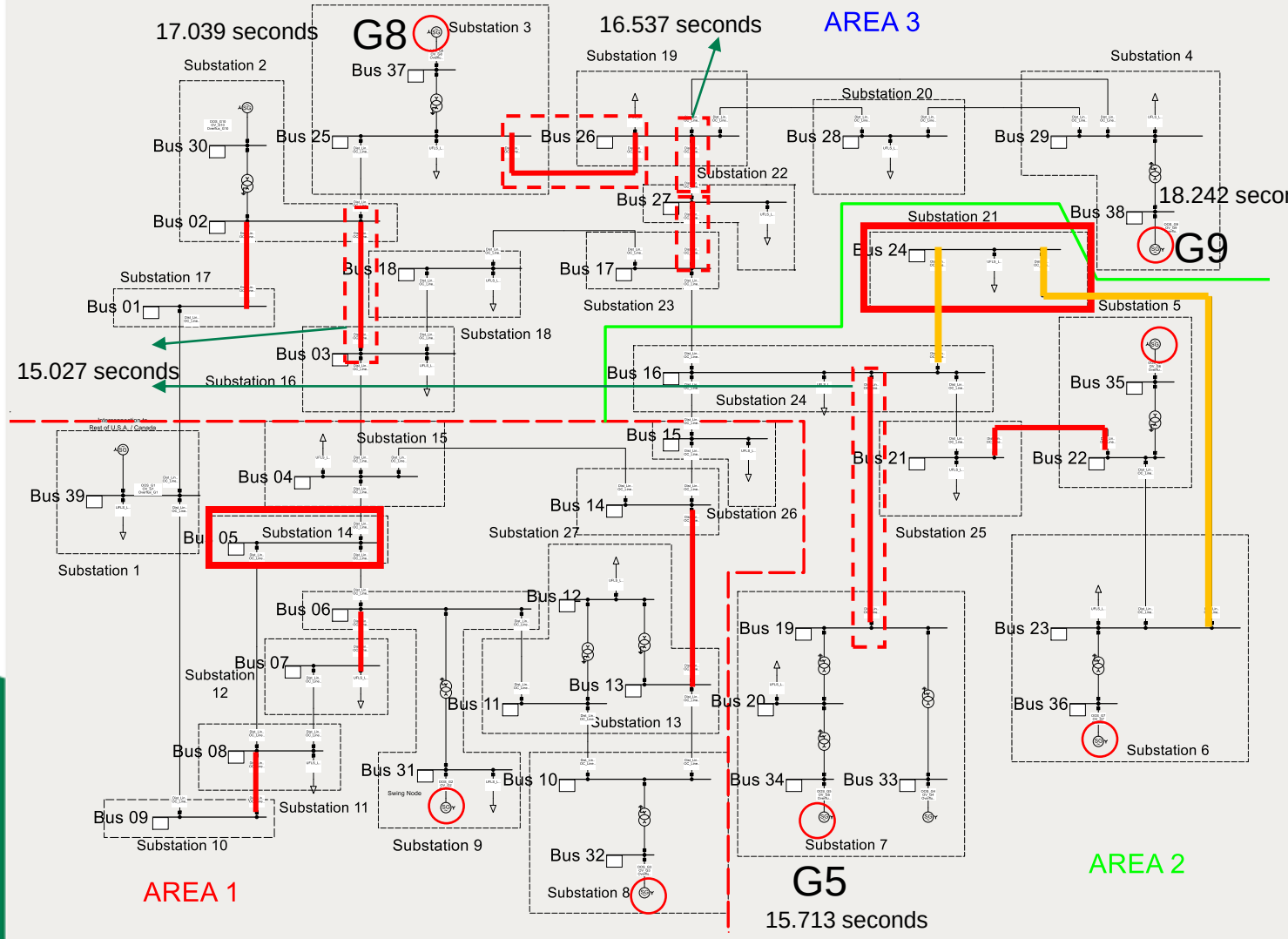
- Generators G2 and G3 trip due to ROCOF protection
- Line 08-09 trips on distance protection
- Area 1 is unsupplied

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



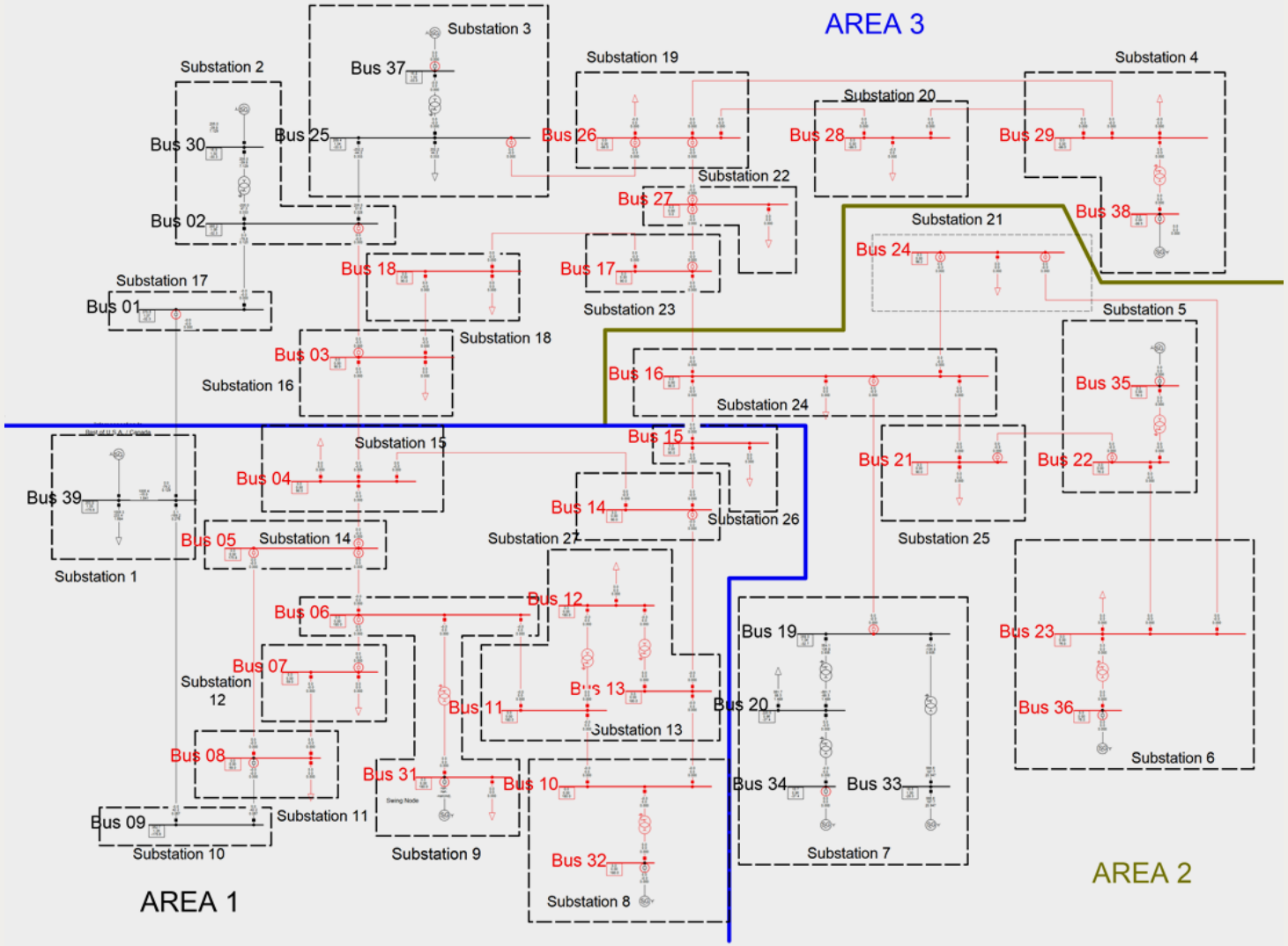
- Cyber attack on substation 21
- Lines 16-24 and 23-24 maliciously disconnected by spoofed IEC 61850 GOOSE
- Distance relay trips line 21-22
- Generators G6 and G7 form an island, and they trip due to ROCOF

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

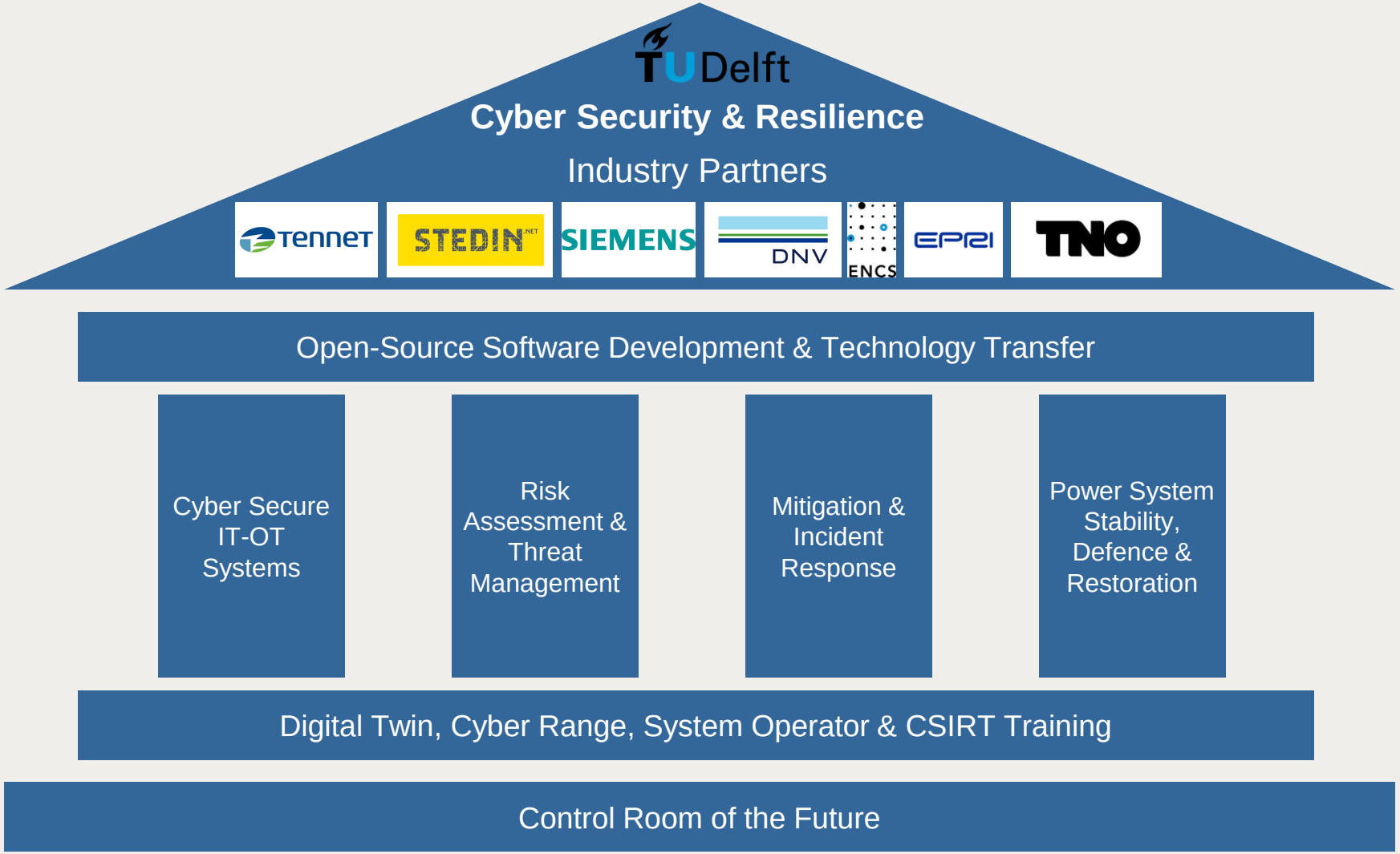


- Lines 02-03 and 16-19 trip due to distance protection
- Generator G5 disconnects due to ROCOF
- Lines 17-27, 25-26, and 26-27 trip due to distance protection
- Generators G8 and G9 disconnect due to ROCOF

GOOSE Cyber Attacks on Two Substations Cause a Blackout



Cyber Security & Resilience Research Programme at TU Delft



Control Room of the Future at TU Delft

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