

# Modelling and Analysing Security Threats Targeting Protective Relay Operations in Digital Substations

## Submission ID: 135

**Presenter:** Mohamed Faisal Elrawy

PhD candidate at KIOS Research and Innovation Centre of Excellence and Electrical and Computer Department, University of Cyprus

**Authors:** Mohamed Elrawy, Lenos Hadjidemetriou, Christos Laoudias and Maria K. Michael

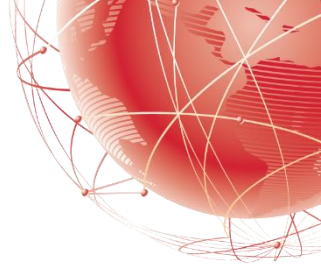
**Date:** 29/6/2023

**ACKNOWLEDGMENT:** This work was supported in part by the European Union's Horizon 2020 Research and Innovation Programme under grant agreement No 101021936 (ELECTRON) and No 101016912 (Smart5Grid); in part by the European Union's Horizon 2020 grant agreement No 739551 (KIOS CoE - TEAMING) and from the Republic of Cyprus through the Deputy Ministry of Research, Innovation and Digital Policy.

**funded by:**



# Contributions



- An integrated threat model for protective relay operations in substations is proposed by presenting a comprehensive analysis of cyber-attack techniques and strategies that target security vulnerabilities of GOOSE protocol.
- The impacts of cyber-attacks on protective relay operations are studied using six different cases. In these cases, cyber-attacks are injected at different times based on the state and operation mode of the relay.
- The criticality of cyber-attacks is studied based on the impact and the warnings caused by these attacks. In the proposed cyber-attacks assessment framework, the effect of the attacks on the physical operations (e.g., open or close Circuit Breaker (CB)) and communication operations (e.g., connection loss) of relays are considered.

# Outline

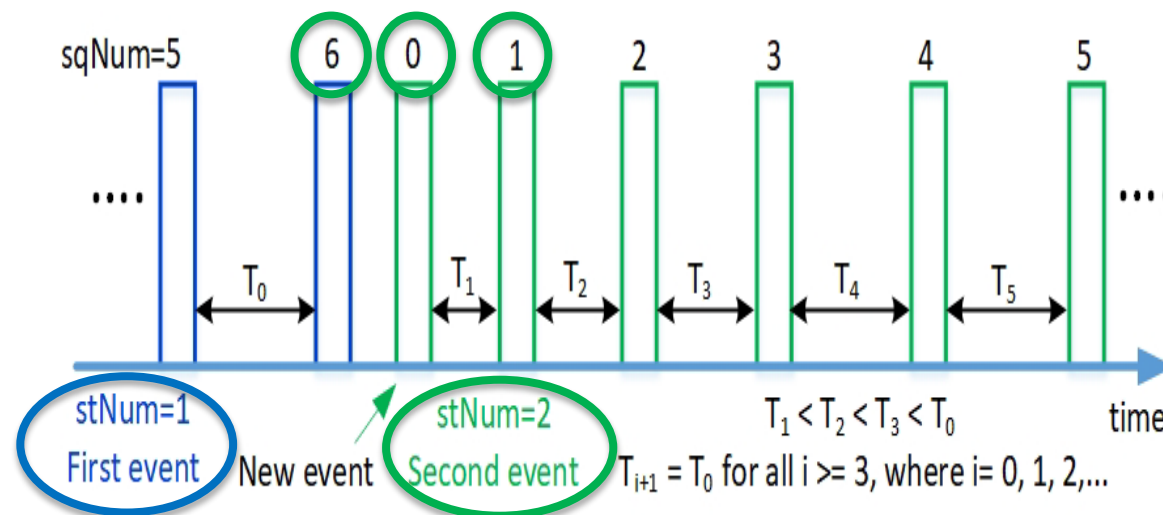
- Introduction
- Threat Model
  - ✓ Potential Attack Vectors
  - ✓ Cyber-attacks Techniques and Strategies
  - ✓ Cyber-attacks Assessment
- Simulation Model Description
- Results
- Conclusions and Future Work



# Substation Area – Introduction

## GOOSE protocol:

- Exchange critical events between Intelligent Electronic Devices (IEDs) in real-time and address the interactivity issue within smart grid digital substations.
- Protocol vulnerabilities, such as using multi cast mechanism and plaintext format, can be exploited by potential attackers to threaten the protection and automation functionalities of the substation.
- The GOOSE protocol uses two transmission mechanisms: (1) Steady-state retransmission (2) Fast-retransmission.





# Threat Model

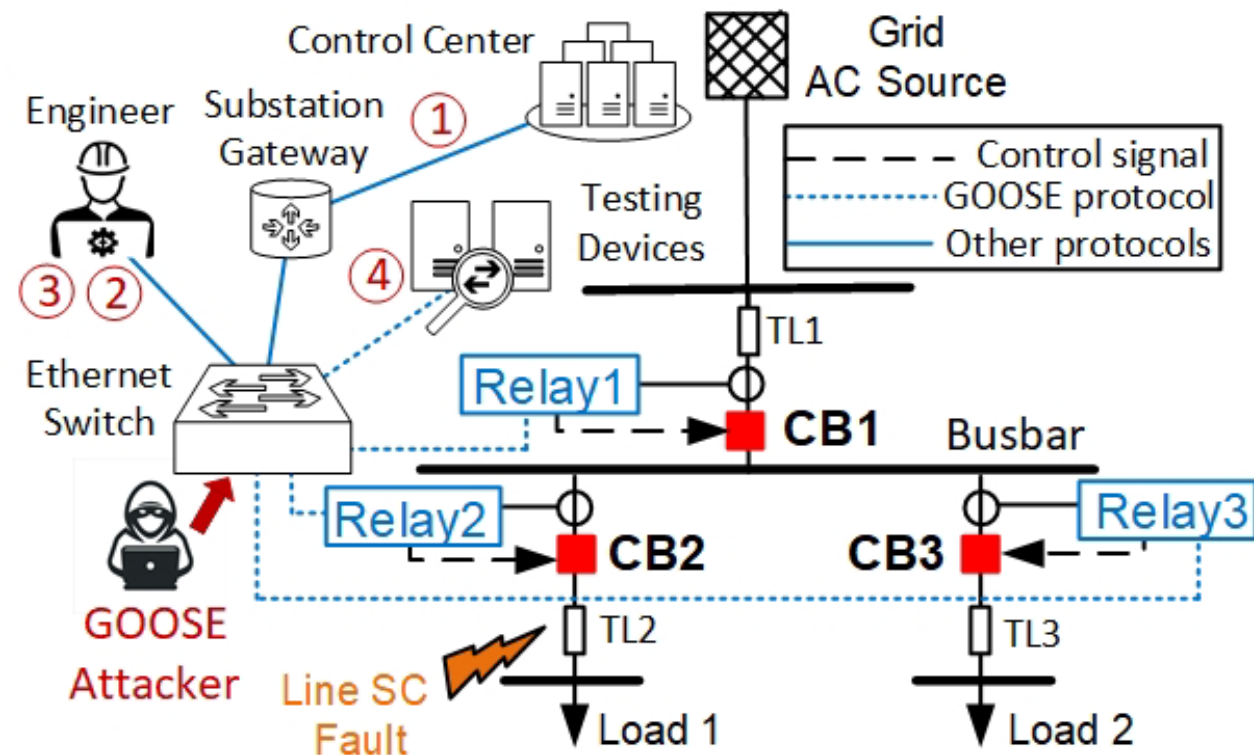
## A) Potential Attack Vectors

(1) The attacker targets the IT domain of the control center to steal credentials of user accounts with remote accessibility rights in substations; and then he/she can gain access to SCADA systems (e.g., cyber-attack on the Ukrainian power grid in 2015).

(2) The attacker enters the substation network through the computer of a power engineer using an infected Universal Serial Bus (USB) device (e.g., Stuxnet cyber-attack in 2010)

(3) The attacker exploits the vulnerabilities of software installed in the engineer's computer (e.g., SolarWinds cyber-attack in 2020).

(4) The attacker accesses the substation network through an infected testing device, such as GOOSEMeter.

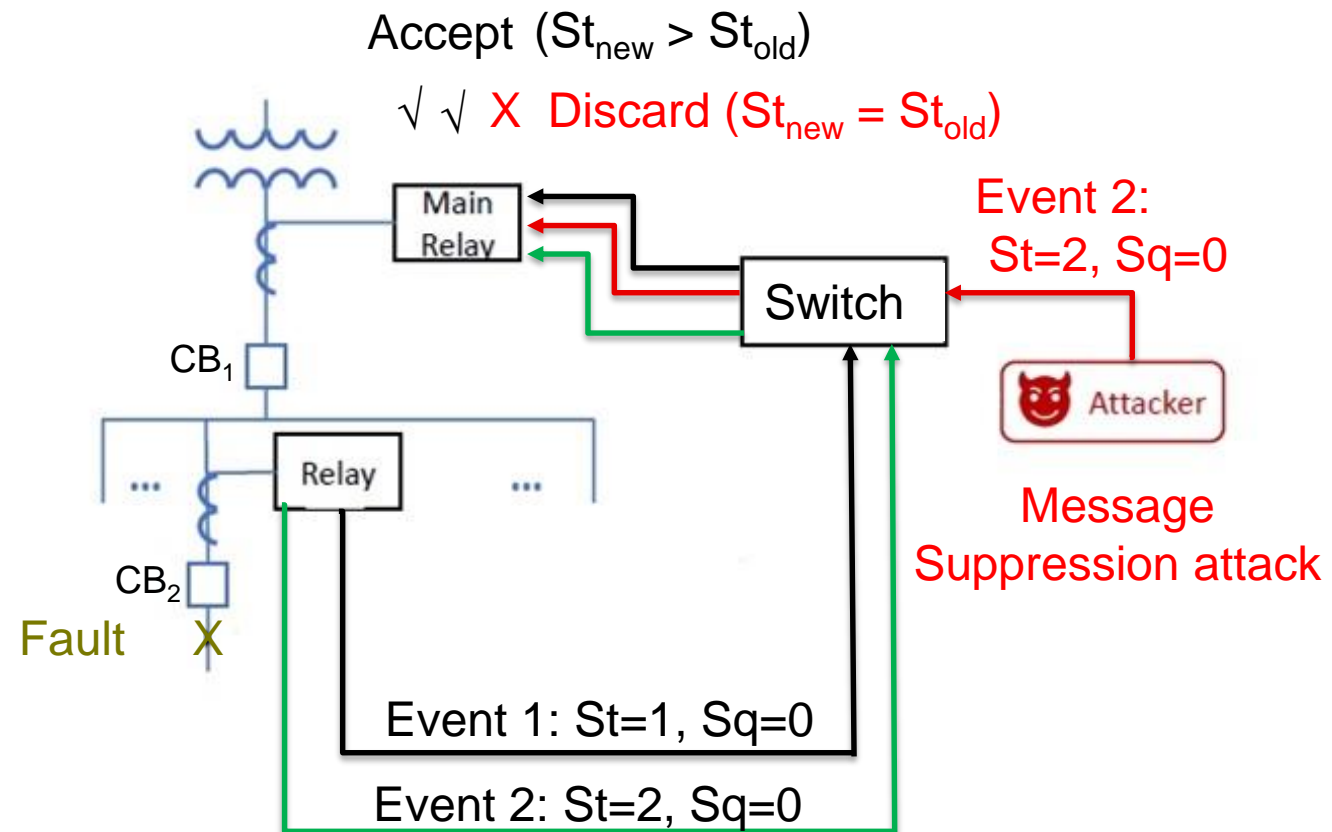


# Threat Model

## B) Cyber-attacks Techniques and Strategies

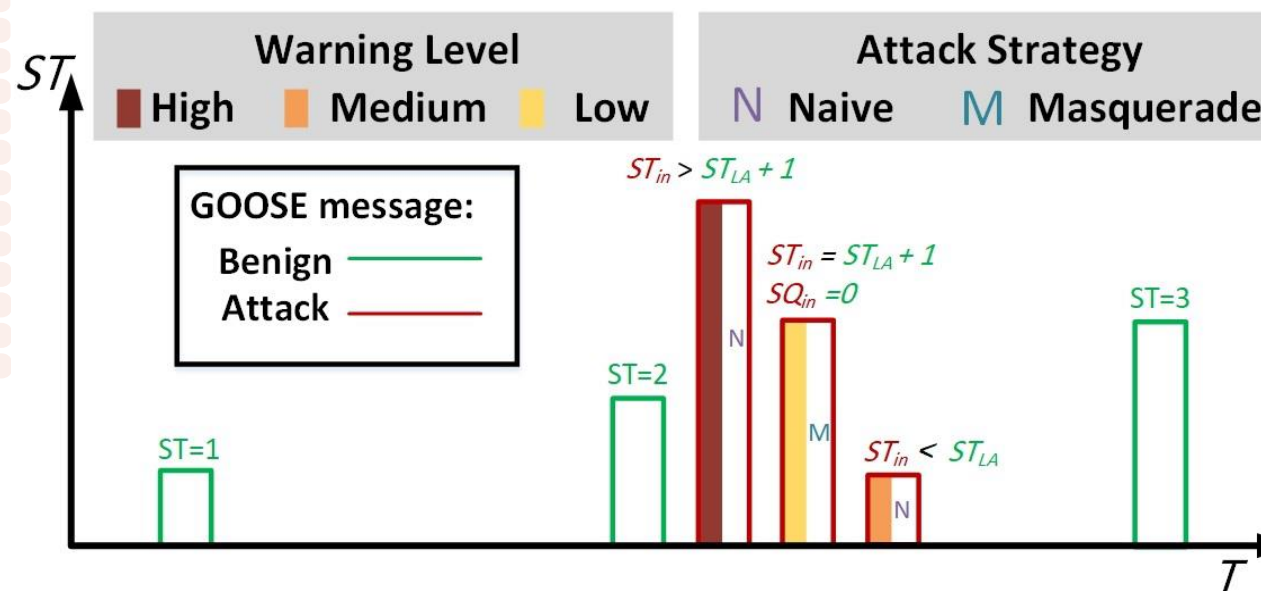
### 1) Cyber-attacks Techniques:

- Message Suppression (MS) attack
- False Data Injection (FDI) attack



# Threat Model

## 2) Cyber-attacks Strategies :



### Algorithm 2: Warning algorithm for GOOSE protocol

**Input:**  $ST_{in}$ ,  $SQ_{in}$ ,  $ST_{LA}$ ,  $SQ_{LA}$ ,  $TTL$ ,  $W_h$ ,  $W_m$ ,  $W_l$

**Output:**  $X(j)$ ,  $WS$

**Initialization**  $WS = 0$ ,  $i = 0$ ,  $j = 0$  ;

**foreach** *New incoming GOOSE message* **do**

$j = j + 1$ ;  $W = 0$ ;

**if**  $ST_{in} \neq ST_{LA}$  **then**

**if**  $ST_{in} > ST_{LA} + 1$  **then**

$X(j) = \text{Trigger high-level warning}$ ;

$W = W_h$ ;  $i = i + 1$ ;

**end**

**if**  $ST_{in} = ST_{LA} + 1$  **then**

**if**  $SQ_{in} == 0$  **then**

$X(j) = \text{No warnings}$ ;

**else**

$X(j) = \text{Trigger high-level warning}$ ;

$W = W_m$ ;  $i = i + 1$ ;

**end**

**end**

**if**  $ST_{in} < ST_{LA}$  **then**

**if**  $ST_{in}$  roll-over Or  $TTL$  time-out **then**

$Age = \text{current timestamp} - \text{message timestamp}$  ;

**if**  $Age < 2 \text{ minute skew}$  **then**

$X(j) = \text{No warnings}$ ;

**else**

$X(j) = \text{Trigger medium-level warning}$ ;

$W = W_m$ ;  $i = i + 1$ ;

**end**

**else**

$X(j) = \text{Trigger medium-level warning}$ ;

$W = W_m$ ;  $i = i + 1$ ;

**end**

**end**

**else**

**if**  $SQ_{in} == SQ_{LA}$  **then**

$X(j) = \text{Trigger low-level warning}$ ;

$W = W_l$ ;  $i = i + 1$ ;

**else**

$X(j) = \text{No warnings}$ ;

**end**

**end**

**if**  $W > 0$  **then**

$WS = ((1/i) * W) + ((i - 1)/i) * WS$ ;

**end**

**end**

**return**  $X(j)$ ,  $WS$

# Threat Model

## C) Cyber-attacks Assessment

$$WS_i = (1/i) * W_i + ((i-1)/i) * WS_{i-1} \quad (1)$$

$$IS = \alpha * PIS + (1 - \alpha) * CIS \quad (2)$$

- **Physical Impact Score (PIS) =**

- (i) 0.33 (unable to close CB automatically)
- (ii) 0.67 (unnecessary opening of CB)
- (iii) 1 (unable to open CB during a fault)

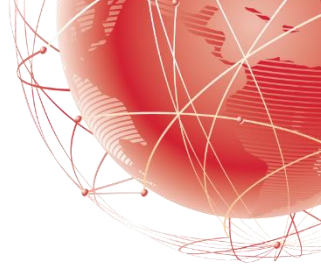
- **Communication Impact Score (CIS) =**

- (i) 1 (If the Connection Loss Duration (CLD) is larger than the duration between detecting and clearing the fault)
- (ii) 0.5 (Otherwise)

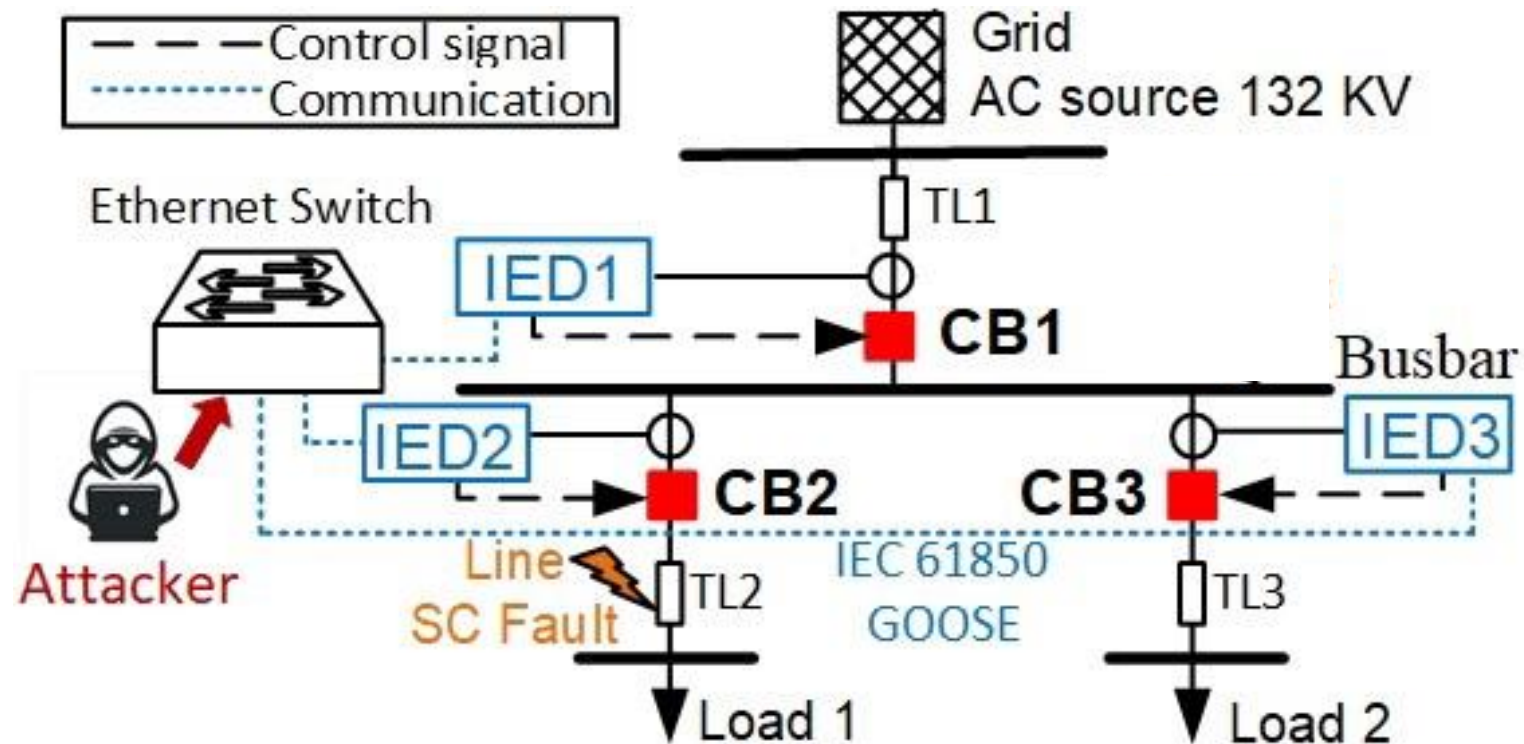
Criticality		Impact	
		$IS \geq 0.5$	$IS < 0.5$
Warning	$WS \leq 0.5$	Level 4	Level 2
	$WS > 0.5$	Level 3	Level 1



# Simulation Results And Discussion



- Simulation Model Description

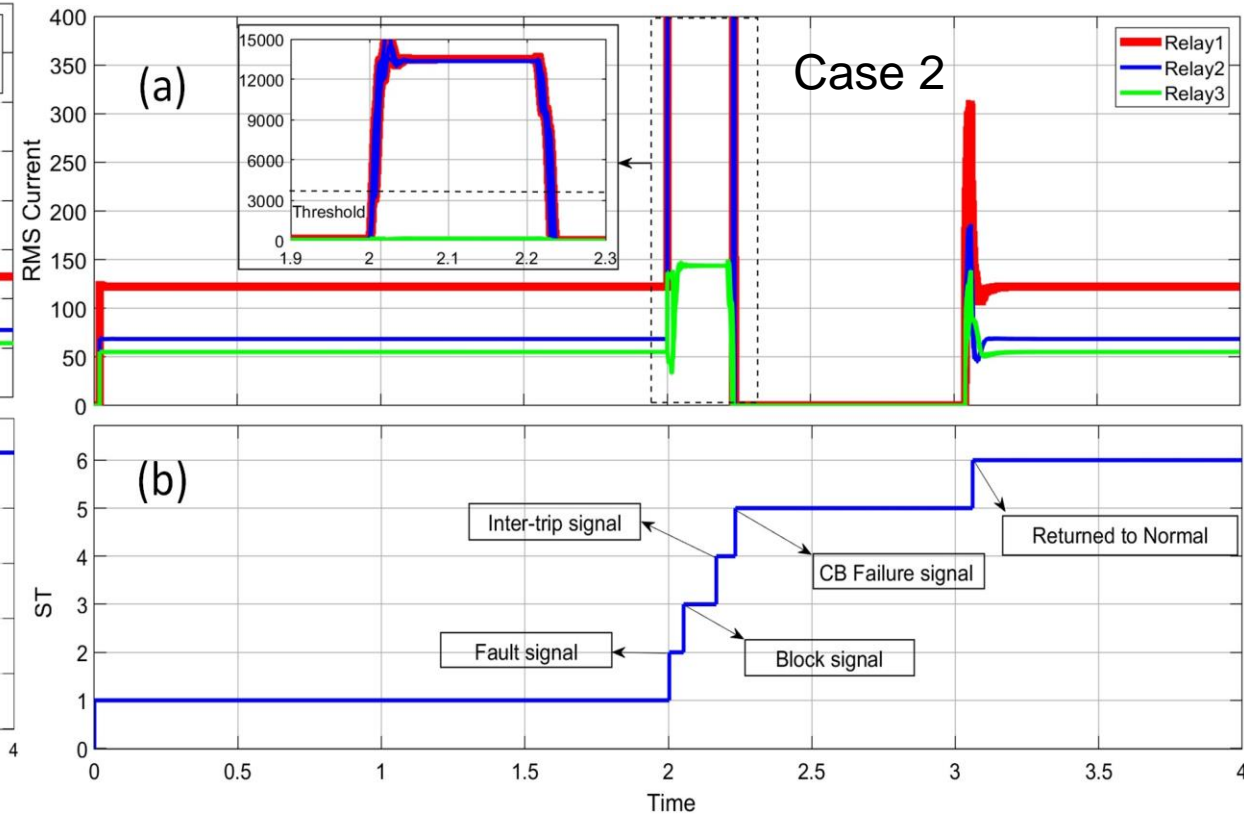
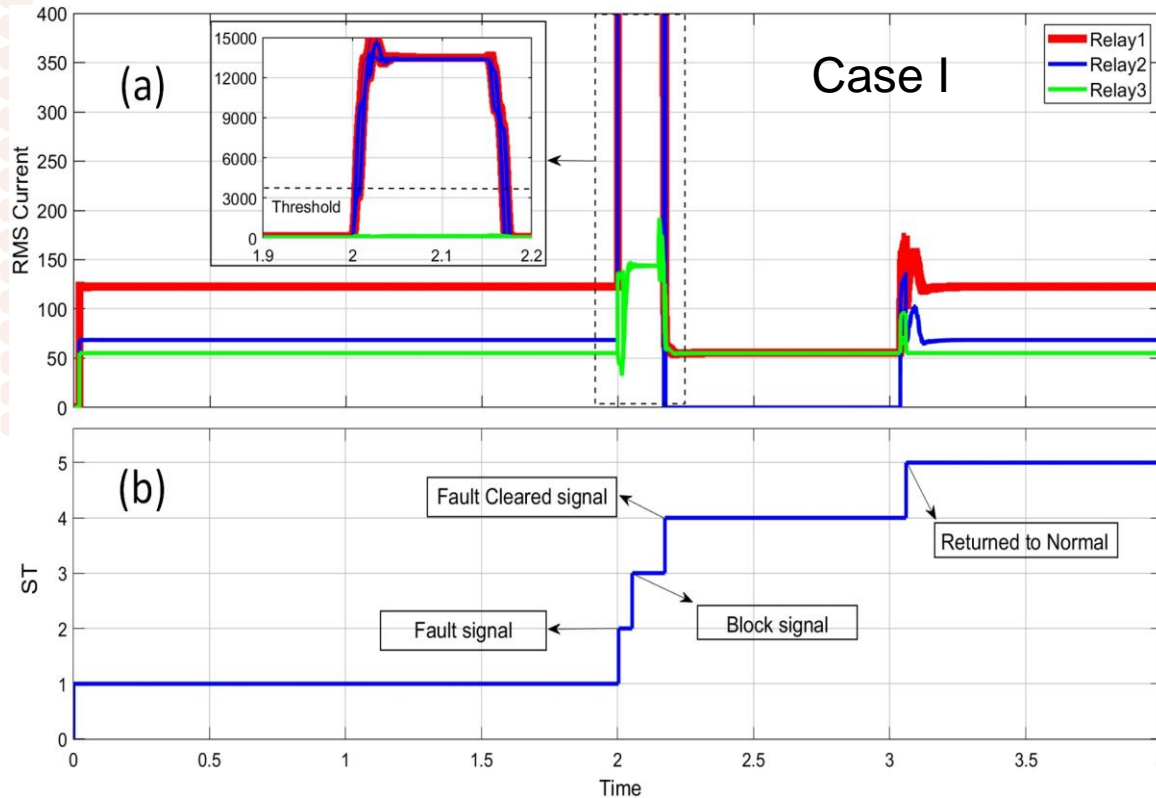


- Schematic diagram of the substation model.

# Results and Discussion (A- Normal Cases)

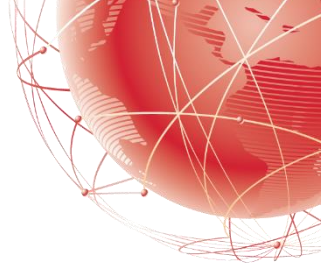
❑ **Case 1:** A Short Circuit (SC) fault on the Transmission Line 2 ( $TL_2$ ), while all the CBs are working properly.

❑ **Case 2:** A SC fault on the  $TL_2$ , while  $CB_2$  has a failure.



(a) RMS currents of the relays, and (b) The ST of messages sent by IED 2 and received at IED 1.

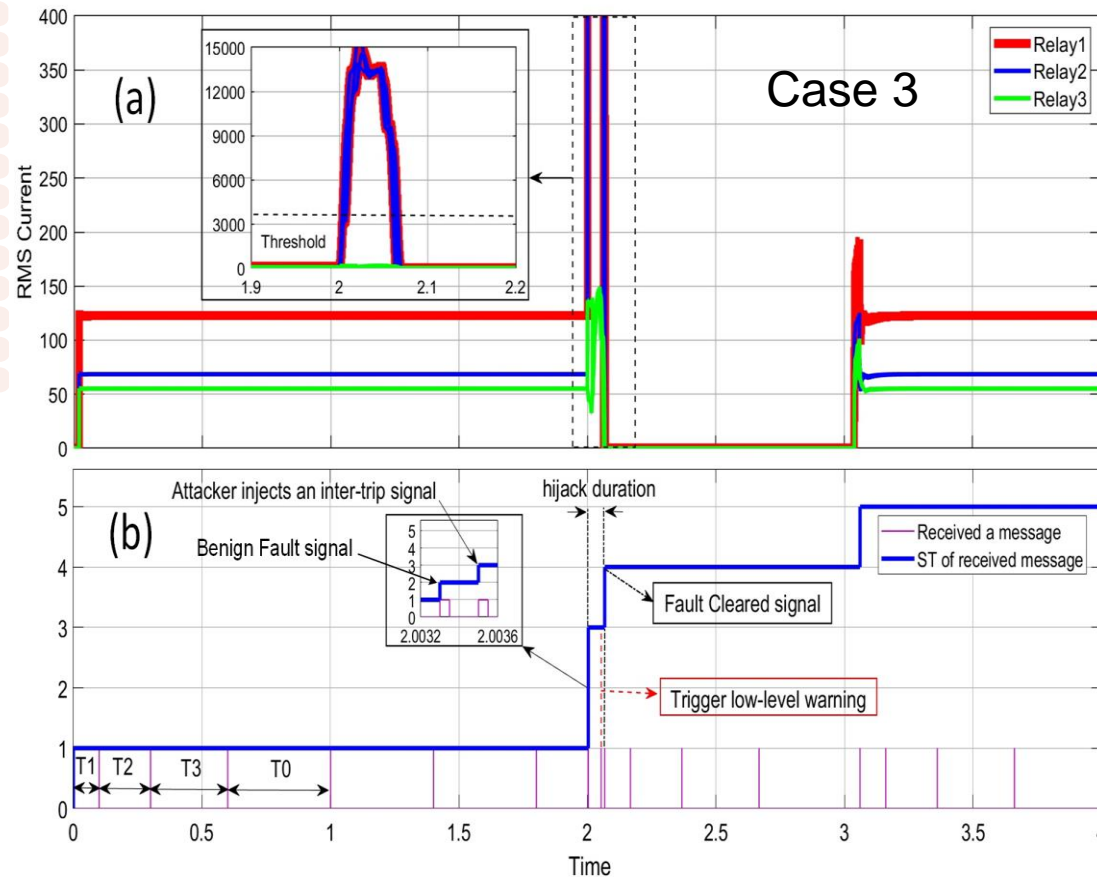
# Results and Discussion (B- Attack Cases)



## ❑ Case 3: FDI Attack

- ✓ Attacker injects a fake inter-trip signal after capturing a fault signal.

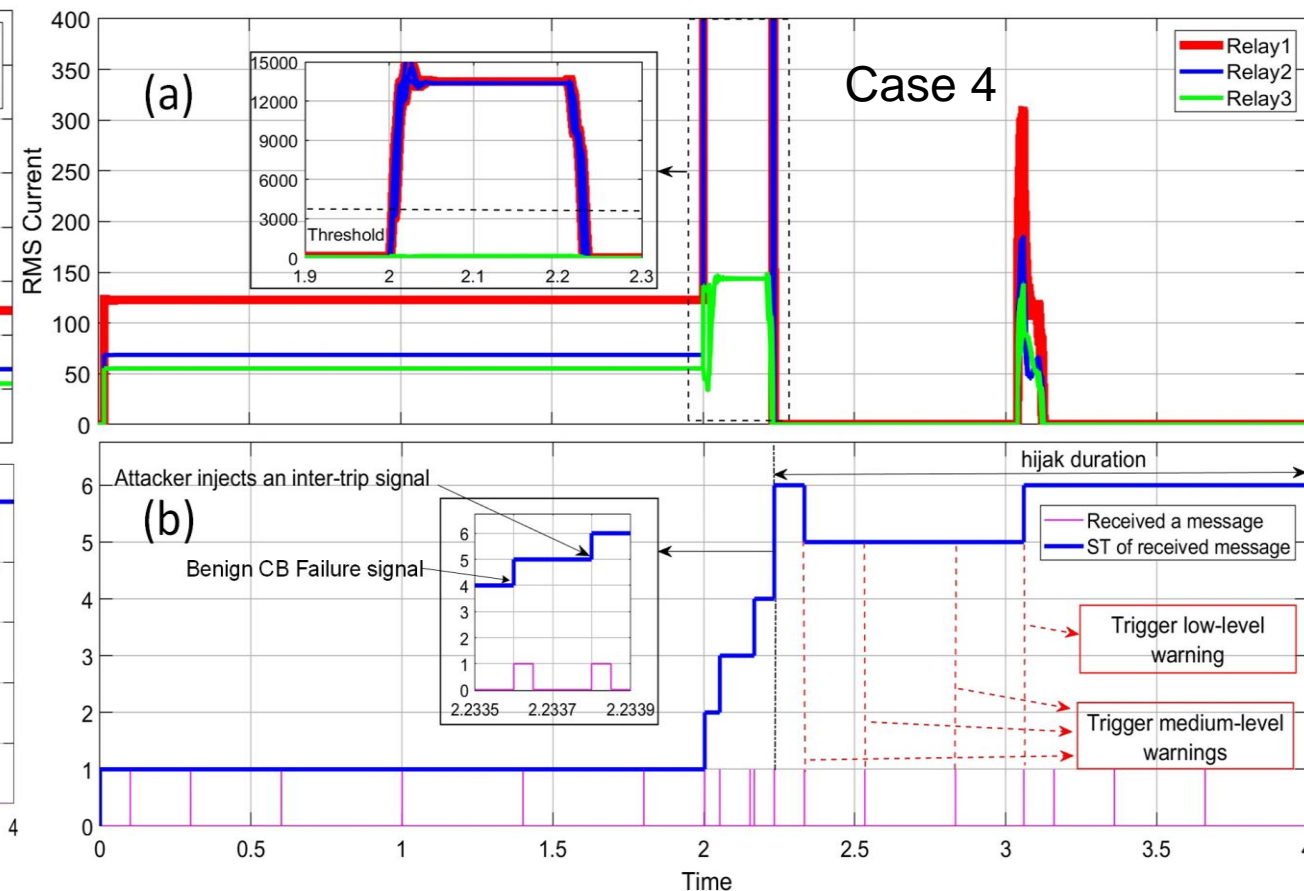
➤ **Impact:** Unnecessary opening of CB1



## ❑ Case 4: FDI Attack

- ✓ Attacker injects a fake inter-trip signal after capturing a CB2 failure signal.

➤ **Impact:** Unable to close CB1 automatically

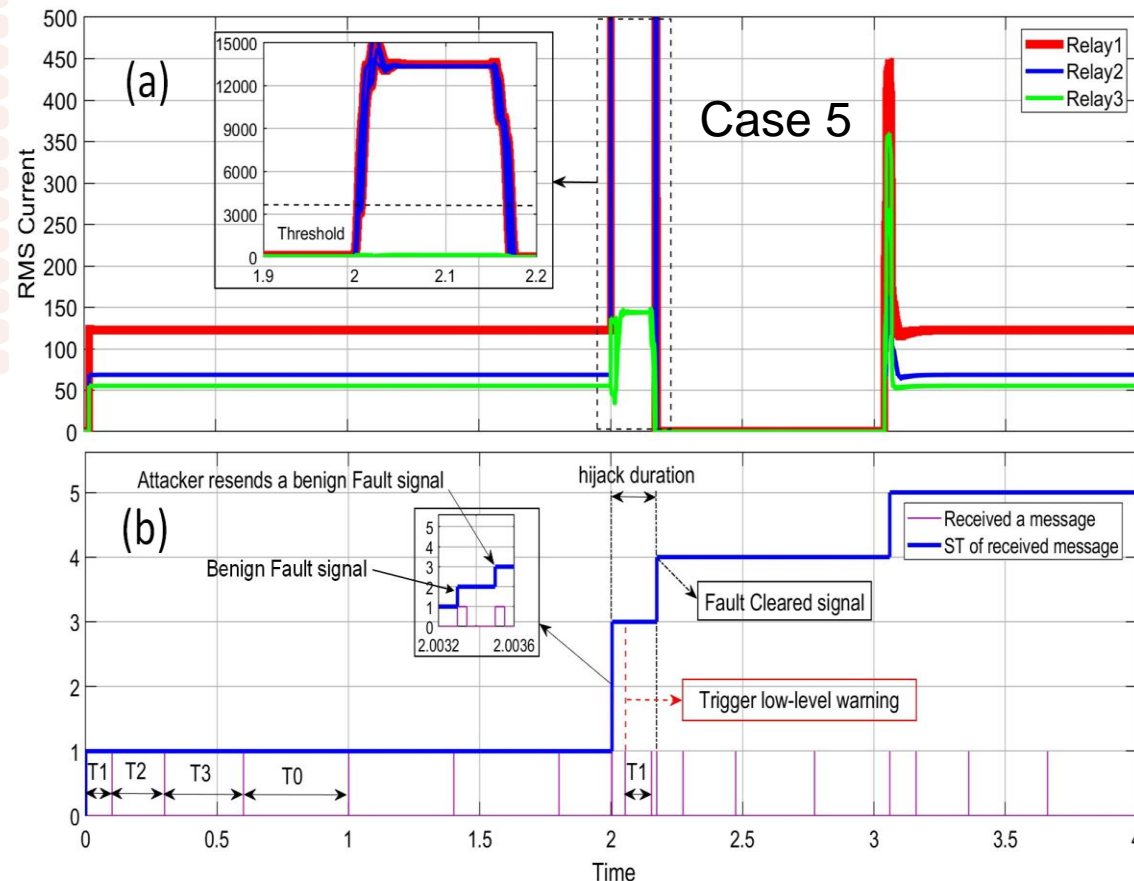


# Results and Discussion (B- Attack Cases)

## ❑ Case 5: MS Attack

- ✓ Attacker re-sends a fault signal after capturing a benign fault signal.

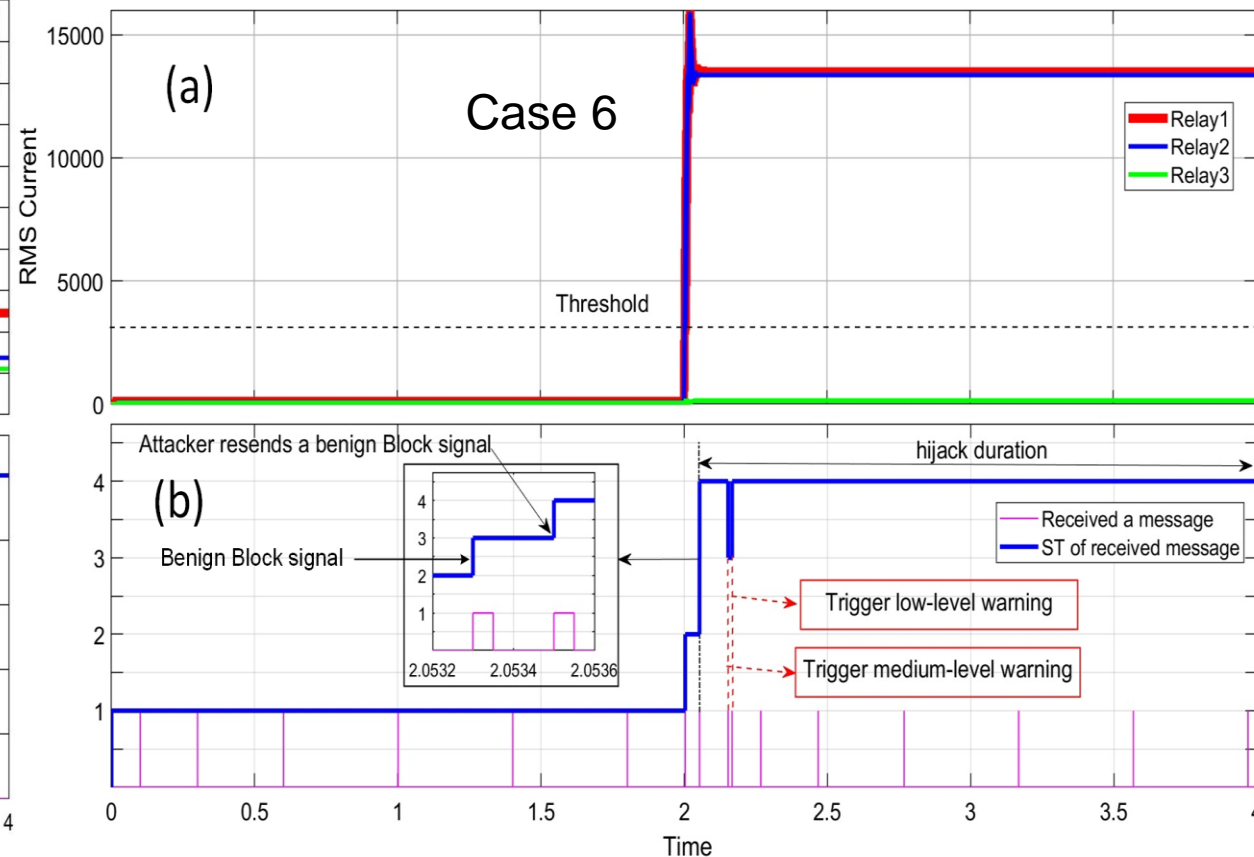
➤ **Impact:** Unnecessary opening of CB1

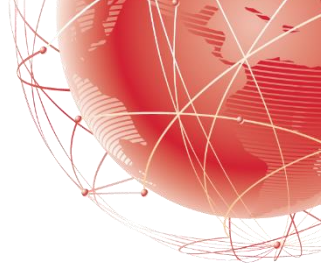


## ❑ Case 6: MS Attack

- ✓ Attacker re-sends a block signal after capturing a benign block signal.

➤ **Impact:** Unable to clear the SC. Fault, which can cause critical damage to the power system





# Conclusions and Future Work

- The cybersecurity of digital substations is a critical issue, as substation protection operations are vulnerable to cyberattacks.
- A deep analysis of cyberattacks can improve the development of new and effective cybersecurity methods and technologies.
- In this paper, we presents a comprehensive study of possible cyber-attacks targeting GOOSE protocol and their impacts on the protection operations of substations.
- We proposed an assessment method for cyberattacks based on the warning level and impact of these attacks.
- For future work, a rule-based IDPS will be designed based on this analysis to protect protective relays operations from different cyberattacks.

# Thank you

## Any Questions

