Study Committee B5

PROTECTION & AUTOMATION

10150

Analysis of Network Monitoring in the Context of IEC 61850

Paulo Sérgio Pereira Junior, Rodolfo Cabral Bernardino, Gustavo Silva Salge, Cristiano Moreira Martins, Paulo Sergio Pereira, Gustavo Espinha Lourenço

CONPROVE

Objectives

- **Importance** of **monitoring** the **IEC 61850 network**;
- **Network requirements** necessary for **monitoring**;
- Implementation of **monitoring techniques**.

Introduction

- Fully **digital substations** based on **IEC 61850**:
  - **Process Bus** highlights **Ethernet communication network performance**.
- **C/S**, **SV** and **GOOSE**:
  - **Network aspects** -> **reliability**, **speed**, **availability and security** of the information .
- Item **8.4.2** of **IEC 61850-5 Ed.2**:
  - Different **application functions distributed** through allocations of LNs in different PDs: **exchange information** through a communication network.

- **Performance of the function** to be executed **depends** on the **network communication performance**:
  - Communication network and its **availability** are part of this function: **monitoring** is **vital**.
- **Vulnerabilities of SAS** based on IEC 61850:
  - As the **complexity** of the system **increases**, more **vulnerable to cyber attacks** it becomes;
  - **External and Internal threats**.
- **COVID-19** pandemic scenario:
  - Power utility **staff** have been working from **home** and accessing the substation's internal network through **remote access**: one of the reasons for opening **security holes for threats**.

Considerations about IEC 62351

- Elaborated by **WG 15** of IEC **TC 57**;
- **Security aspects** related to series of standards covered by TC 57, including **IEC 61850 series**;
- **IEC 62351-6** "Security for IEC 61850":
  - **Security** matters of **IEC 61850 communication protocols**;
  - Contributions to **GOOSE and SV security**: addition of **"Authentication Value"** and optional **encryption methods**;
  - **Performance** issues in case of **time-critical** requirements of **GOOSE and SV**;
  - **Encryption** methods are **recommended** whenever it **does not cause problems**.
- **IEC 62351-7**:
  - **Network and System Management (NSM)**;
  - **NSM Data Objects (NSM Dos)**;
  - **Management Information Base (MIBs)**.
- **IEC 62351-14**:
  - Implementation of **security logs** - **Syslog**;
  - Importance of security logs for the **cybersecurity operation centers**.
- **Detection mechanism** on the IEC 62351:
  - **SNMP** – defined on **part 7: operational monitoring**;
  - **Syslog** – defined on **part 14: security operation center**.

Network monitoring system and cybersecurity for PACS

- **PACS network** must incorporate **monitoring functions** able to:
  - Detect and point out **anomalies** or **lacking** of messages;
  - Detect **lacking of synchronism** signal;
  - Verify and point out **abnormal propagation time**;
  - **Independent system**;
  - **Storing event records**.

Study Committee B5

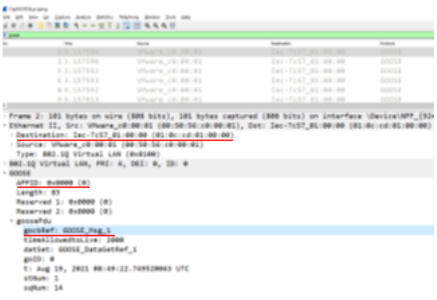
PROTECTION & AUTOMATION

10150

Analysis of Network Monitoring in the Context of IEC 61850 continued

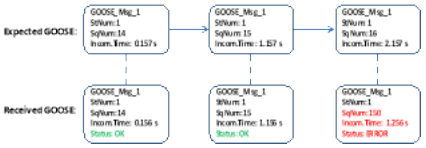
- **PACS network** must incorporate **mechanisms** that offer **cybersecurity** to ensure:
    - **Confidentiality**;
    - **Integrity**;
    - **Availability**;
    - **Authenticity**.
- Some **requirements may not be foreseen in the monitoring system** – **blind spot**;
- Monitoring deal with: **Test/Simulation configuration** -> **two SV streams: simulated and the real one**;
- Monitoring system -> **event logs** to be **stored and consulted**;
- **Trunk Port** on the network Switch or through **Port Mirroring**;
- **GOOSE** frames carrying as data a **Trip** command:
    - **Not delivered** to the **SCU** -> the **protection system is compromised**,

  Monitoring system must **detect** this anomaly:
    - **Is the GOOSE there?**
    - **Analyzing** all IEDs instances through **SCL file (SCD or ICD)**;
    - **Filters** like **Destination MAC Address**, **GOOSE Control Block Reference** and



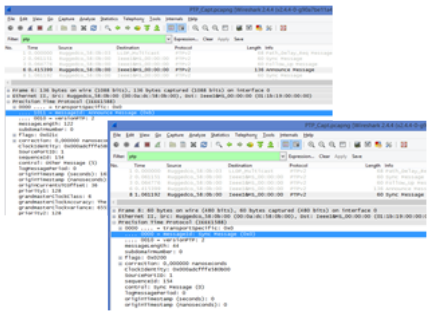
- An invader could publish **malicious GOOSE** frames:
    - To **open** or to **close** a **circuit breaker**;
    - Causing a **network overload**.

  Monitoring system must detect this anomaly:
    - **Retransmission times** too different from what is configured or with **wrong SqNum (out of order)**;
    - **Analyzing reception times** of the frames and verifying the **time difference**, also **SqNum**.



- **Blind spot**: **invader** is able to publish **malicious GOOSE** frames in the **right retransmission time** and **sequence order**.
- **PTP** (Precision Time Protocol):
    - **BMCA**.

  Monitoring system:
    - To verify if **GM** messages;
    - Analyzing **Announce and Sync**.



- **Loss of time synchronism**, -> **threat** in the **Process Level**;

  Monitoring system:
    - Must be a **PTP slave**;
    - **To verify** if the slave **clock jitter** is increasing in relation to **master clock**.
- If **time synch** is **lost** -> two possibilities
    - **Some interference**;
    - **Hardware problem** with **Transparent Clock** or **calibration** of **GM clock**.
- **Invader** pretends to be the **GM** and **break down** the **time synchronism**:
    - With the **same Clock Identity** of the current GM - **blind spot** for **monitoring systems**;
    - With **different Clock Identity** - can be verified by the monitoring system through a **"White List"**.

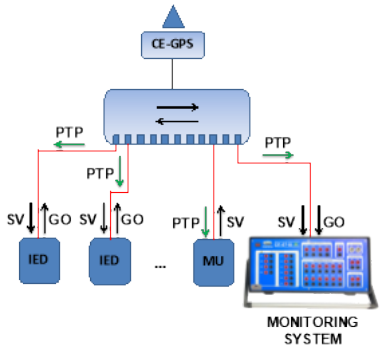
Study Committee B5

PROTECTION & AUTOMATION

10150

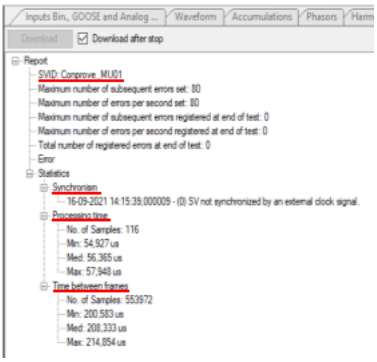
Analysis of Network Monitoring in the Context of IEC 61850 continued

- **Monitoring system -> statistical analysis** of **SV** and **GOOSE** frames;



Sampled Values:

- **Propagation delay**;
- **Processing time**;
- **Time between frames**;
- **Errors in the network**;
- **Synchronism flag**.

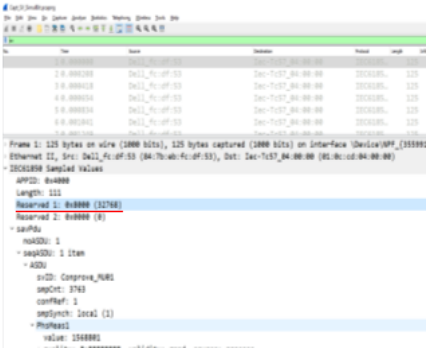


GOOSE:

- **Transfer time**.

- **LN for monitoring** - **IEC 61850-7-4 Ed.2.1** :
  - **LGOS**;
  - **LSVS.**

- **Monitoring system** -> **two SV** frames running: one **simulated** and other **real**:
  - **Test set** -> to **publish SV with simulation bit set** x **MU/SAMU** -> to **publish real SV** frames;
  - If the **monitoring system** has **not** been **notified** that **substation** is **under maintenance**, it must **report data inconsistency** and save this information to a **log**.



Conclusions

- It was possible to evaluate the **requirements** for the **monitoring** of the network and the **failure identification methodologies**;
- Aspects not foreseen by network monitoring were also addressed (**blind spots**);
- The deployment of a **digital substation** can be more **reliable** with the implementation of the **monitoring system**:
- Any failure event will be **alarmed** and **logged** so that will be possible to **trace its causes**.
- It is expected that this work contributes to enable **proper operation of communication networks**, as this is the only way to ensure safe and **reliable traffic of information**.