Мониторинг и диагностика GOOSE-потоков на базе Ethernet-коммутатора МЭК61850

GOOSE CHECK

Лопухов Иван
Moxa.Inc
2019 Июль

MOXA®
Reliable Networks ▲ Sincere Service

Содержание

Коммуникации

GOOSE Details

GOOSE Communication

GOOSE CHECK
- GOOSE Tampering
- GOOSE Time-Out

SMART ALARMING

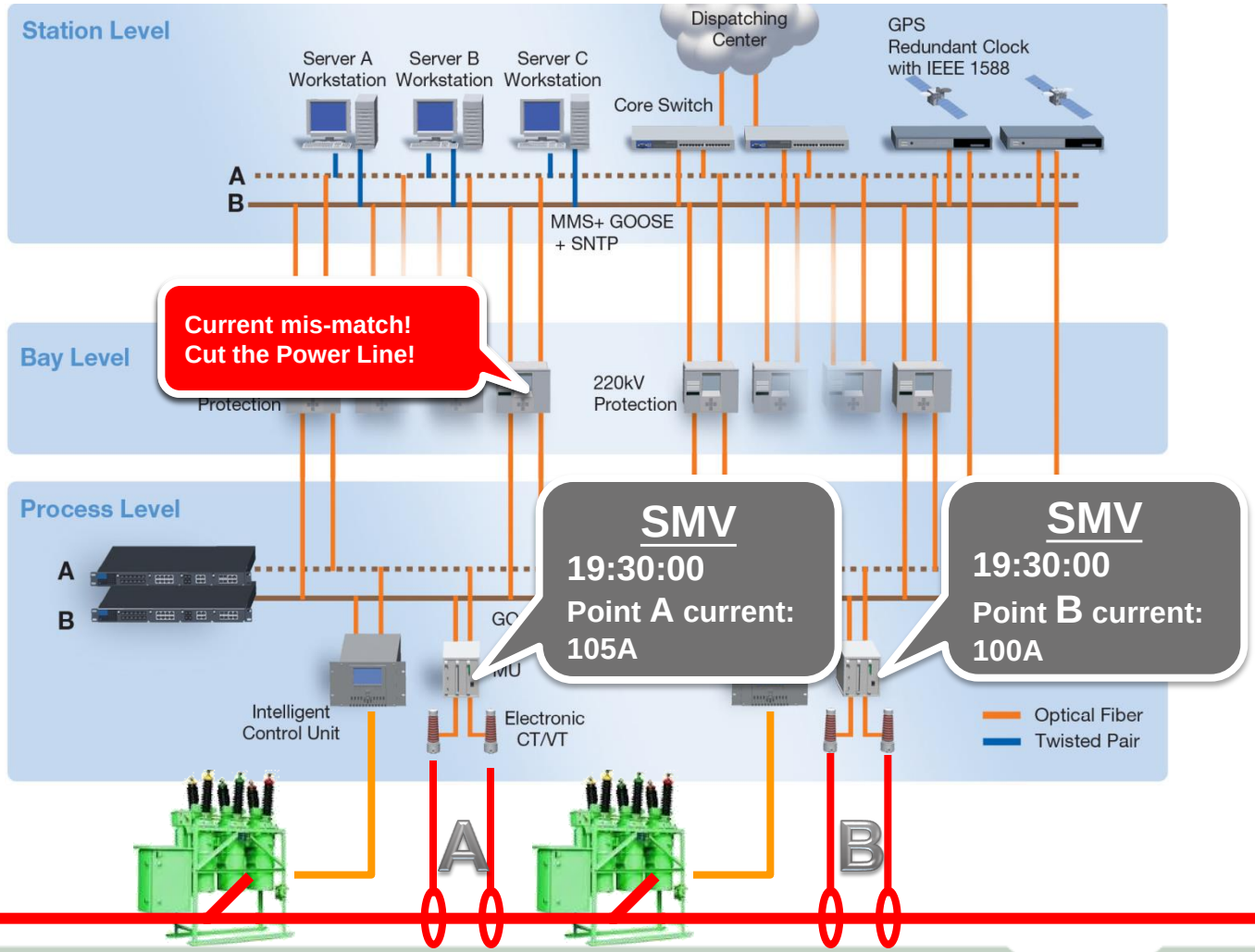
COMMUNICATION WITH SCADA

МЭК-61850 архитектура и протоколы

Power SCADA Monitoring

Logic & Control

Data Acquisition & Circuit Breaking

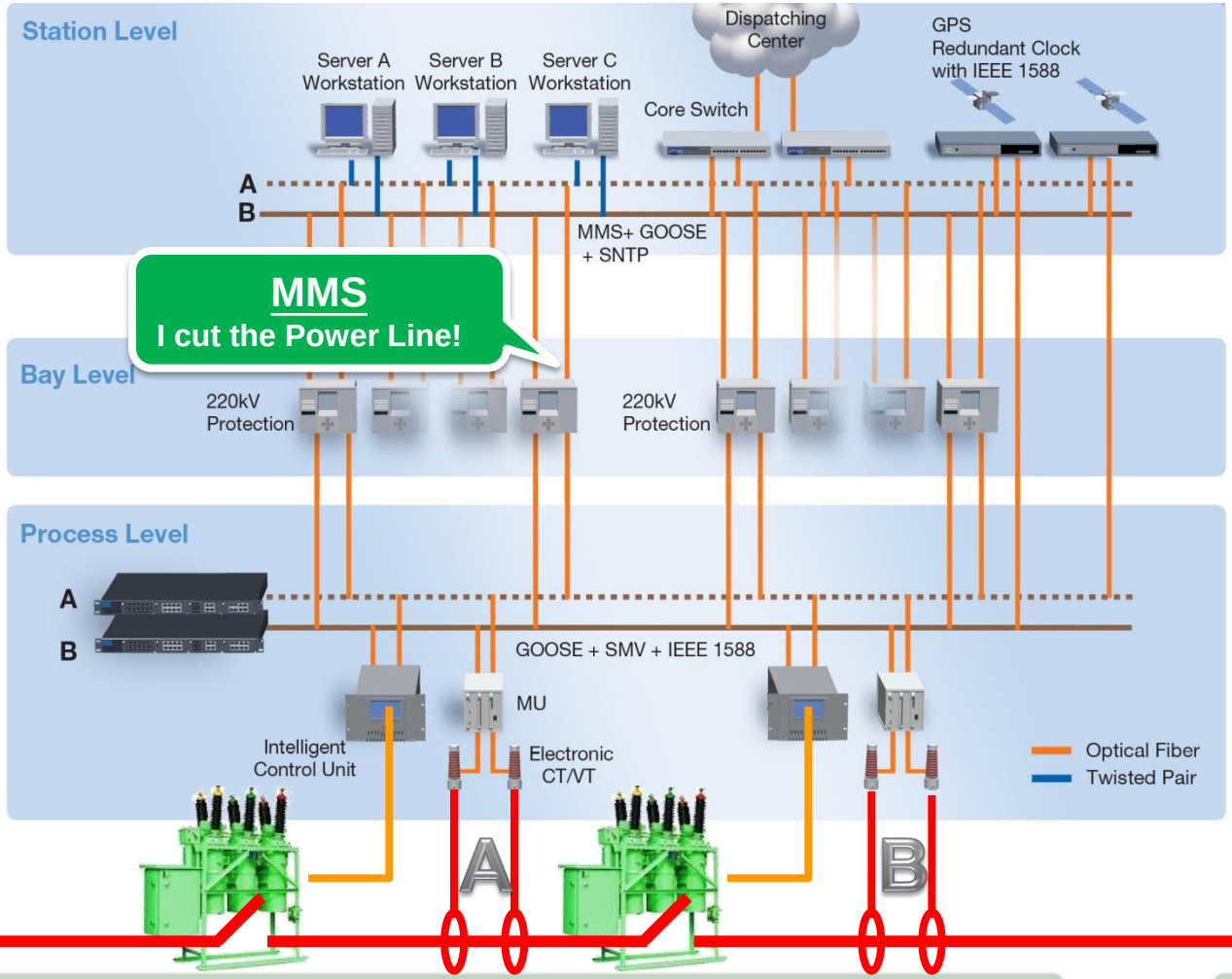


МЭК-61850 архитектура и протоколы

Power SCADA Monitoring

Logic & Control

Data Acquisition & Circuit Breaking

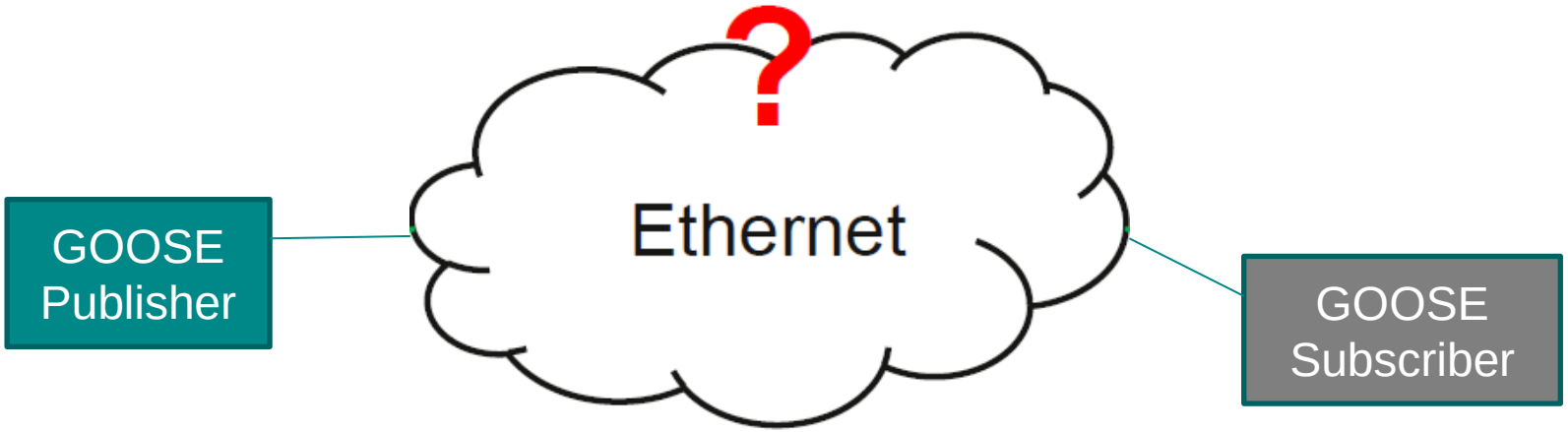


MOXA

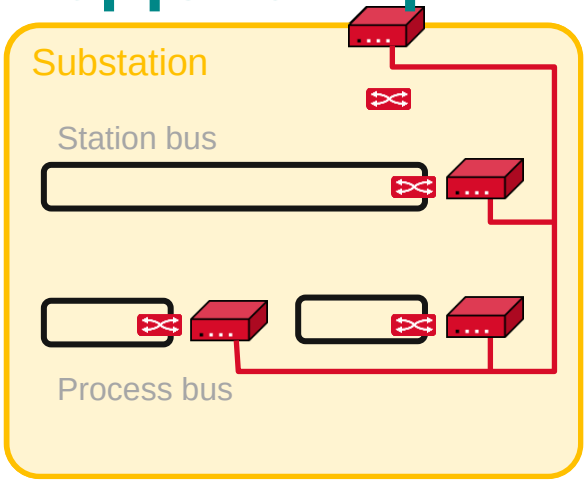
GOOSE проблемы коммуникации

Bad / No GOOSE reception

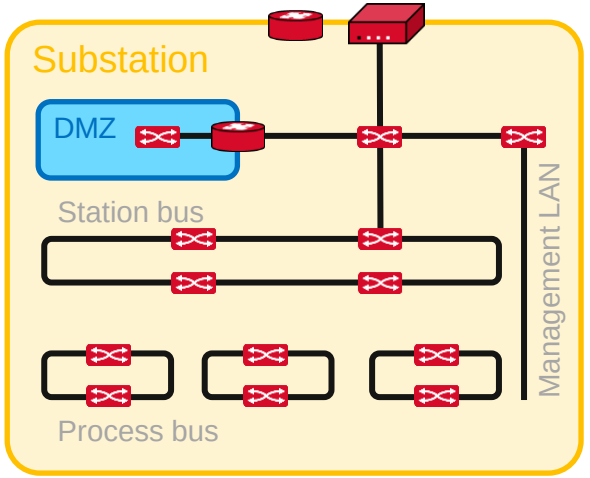
- Network setting issue?
- ID settings issue?
- Other?



IDS, Firewall и коммутатор на подстанции



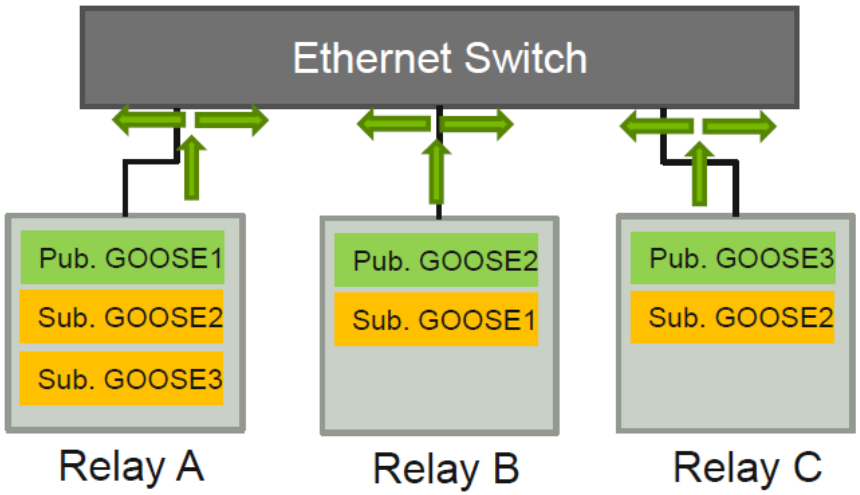
- Cybersecurity provided via **powerful traffic content analysis.**
- **Inspection of mirrored traffic by central hosts.**
- Analysis realized by computers (hosts) with scanning software.
- Deep-packet and traffic pattern analysis.
- Learning capabilities via artificial intelligence.



- Real world substation IT networks are **dominated** by switches
- Switches have **limited** CPU power and memory resources
- Switches are in **immediate vincinity of end devices** (IED, station computers, gateways) from Station to Process level

GOOSE специфика

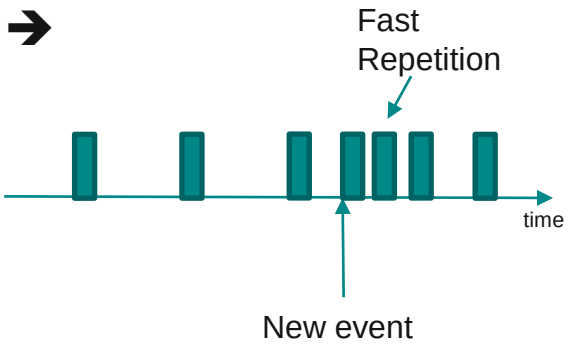
GOOSE
Publish /
Subscribe



Publish

- Multicast Message (Layer 2)
- No confirmation of message reception

➔ repetition strategy ➔

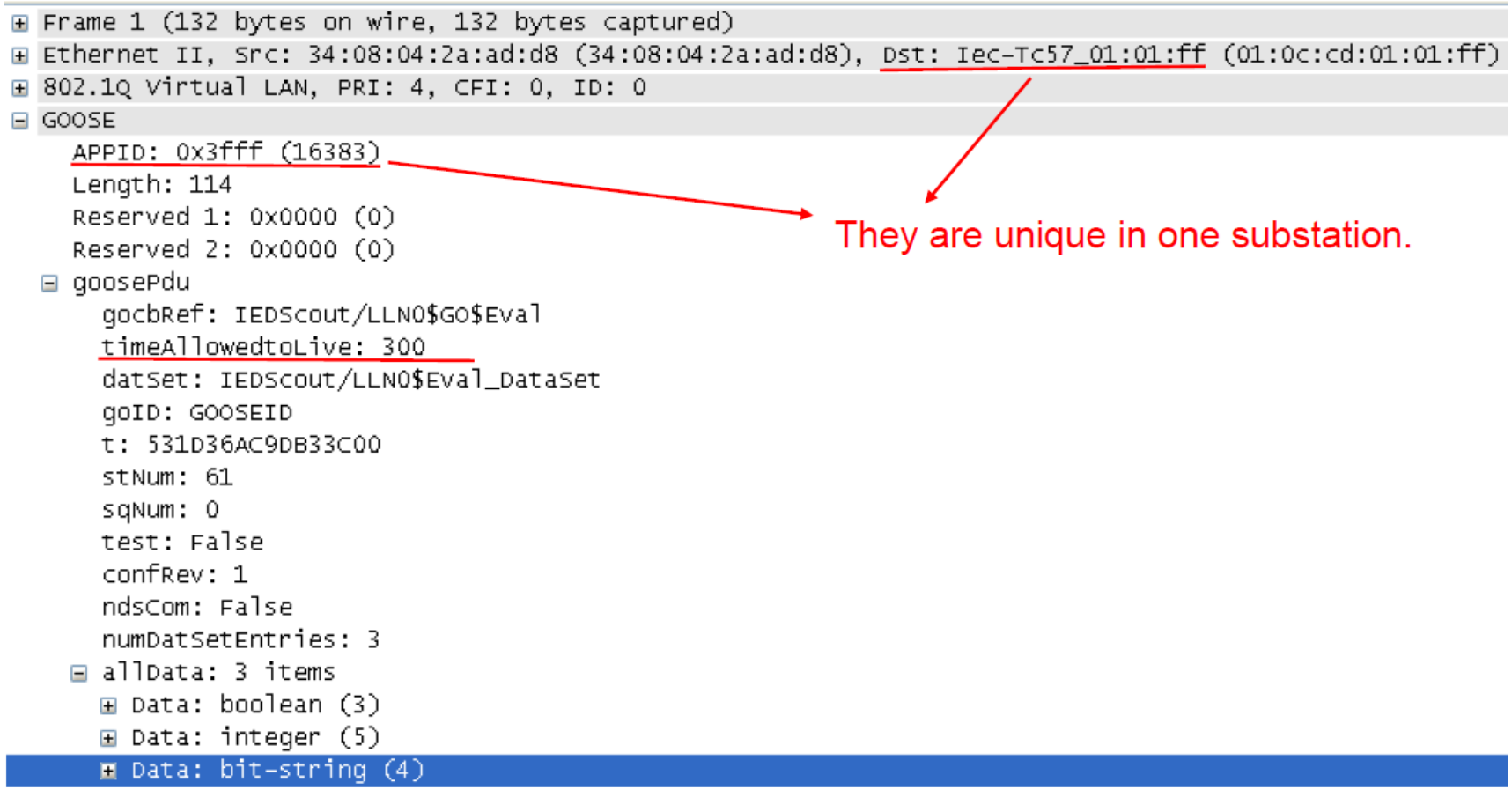


Subscribe

Typical parameters used for subscription (depends on implementation):

- Application ID
- Destination MAC Address
- GOOSE ID

GOOSE формат сообщения



GOOSE мониторинг

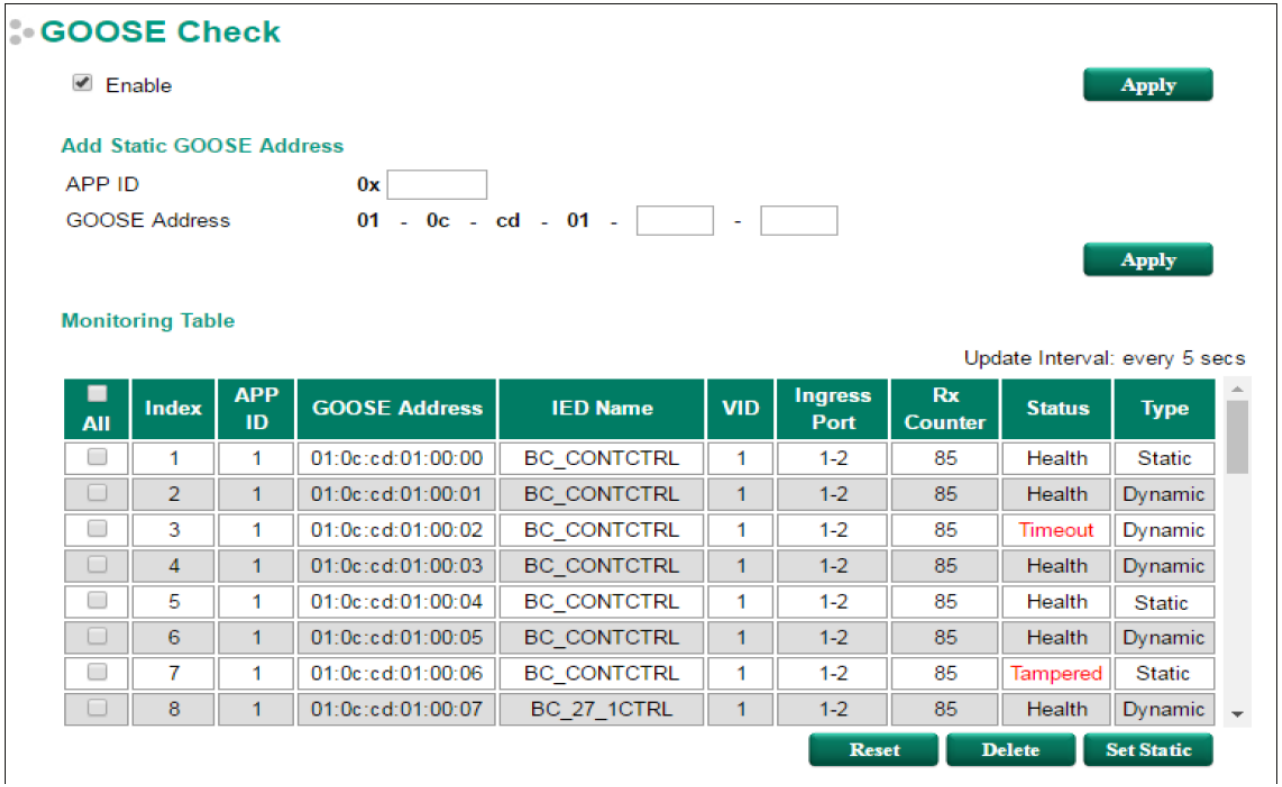
GOOSE мониторинг - интерфейс

GOOSE monitoring

- APPID
- Destination Address (DA)
- IED Name
- VLAN ID
- Ingress Port
- Rx Counter

GOOSE Status

- Health
- Tampered
- Time-out



GOOSE смена порта

GOOSE Packet

Monitoring Table

Update Interval: every 5 secs

All	APP ID	GOOSE Address	IED Name	VID	Ingress Port	Rx Counter	Status	Type
☐	a	01:0c:cd:01:01:ff	IEDScout	1	1-2	64	Health	Dynamic

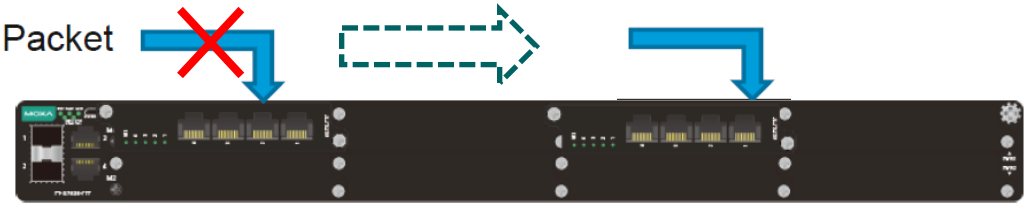
Reset Delete Set Static

GOOSE Ingress port* is automatically learned by the switch

** Trunk port is also supported*

Behavior if we change the cabling?

GOOSE Packet



Monitoring Table

Update Interval: every 5 secs

All	APP ID	GOOSE Address	IED Name	VID	Ingress Port	Rx Counter	Status	Type
☐	a	01:0c:cd:01:01:ff	IEDScout	1	4-1	64	Health	Dynamic

Reset Delete Set Static

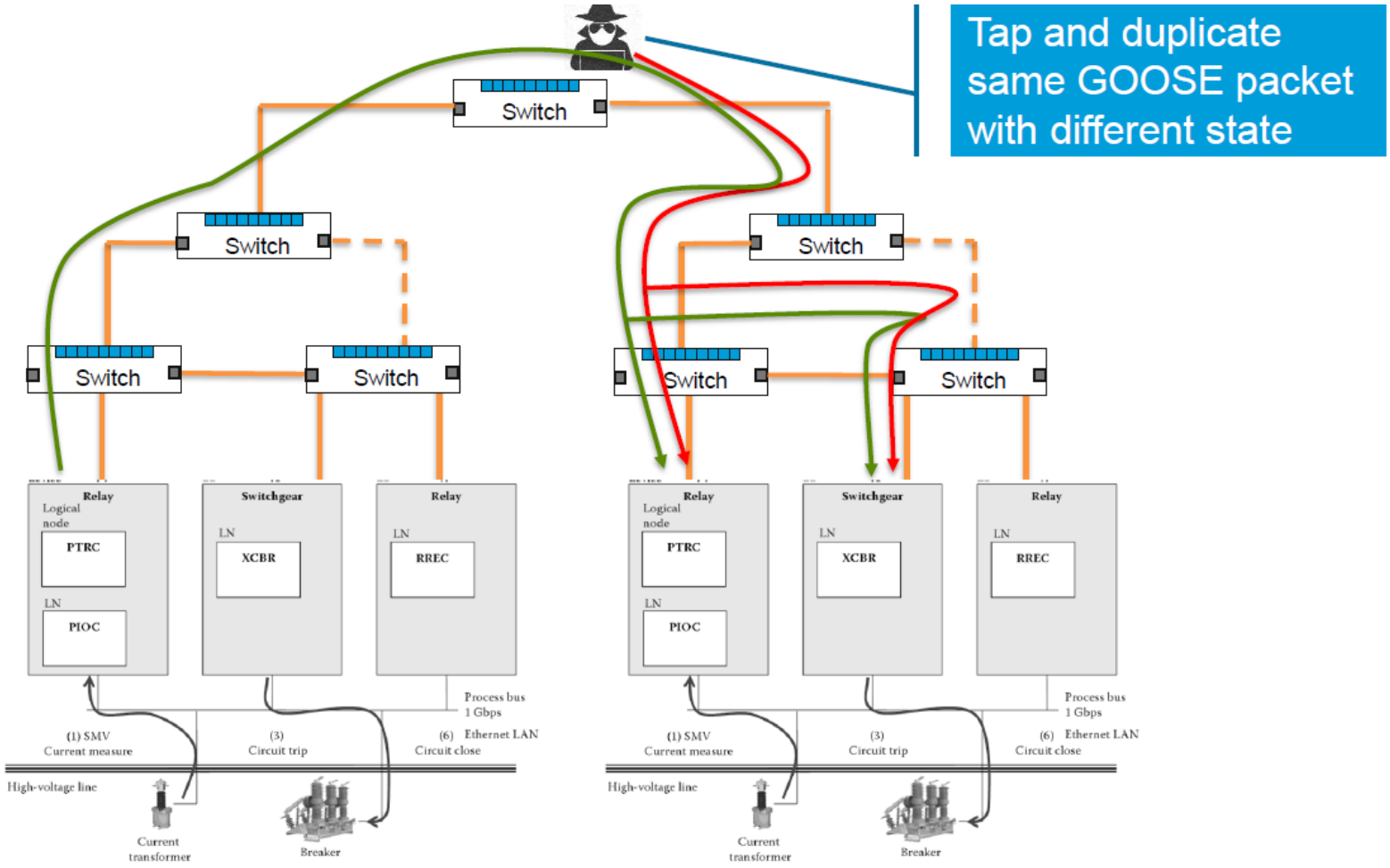
Ingress port is updated accordingly (no Alarm)

Note: *same mechanism when network topology changes*

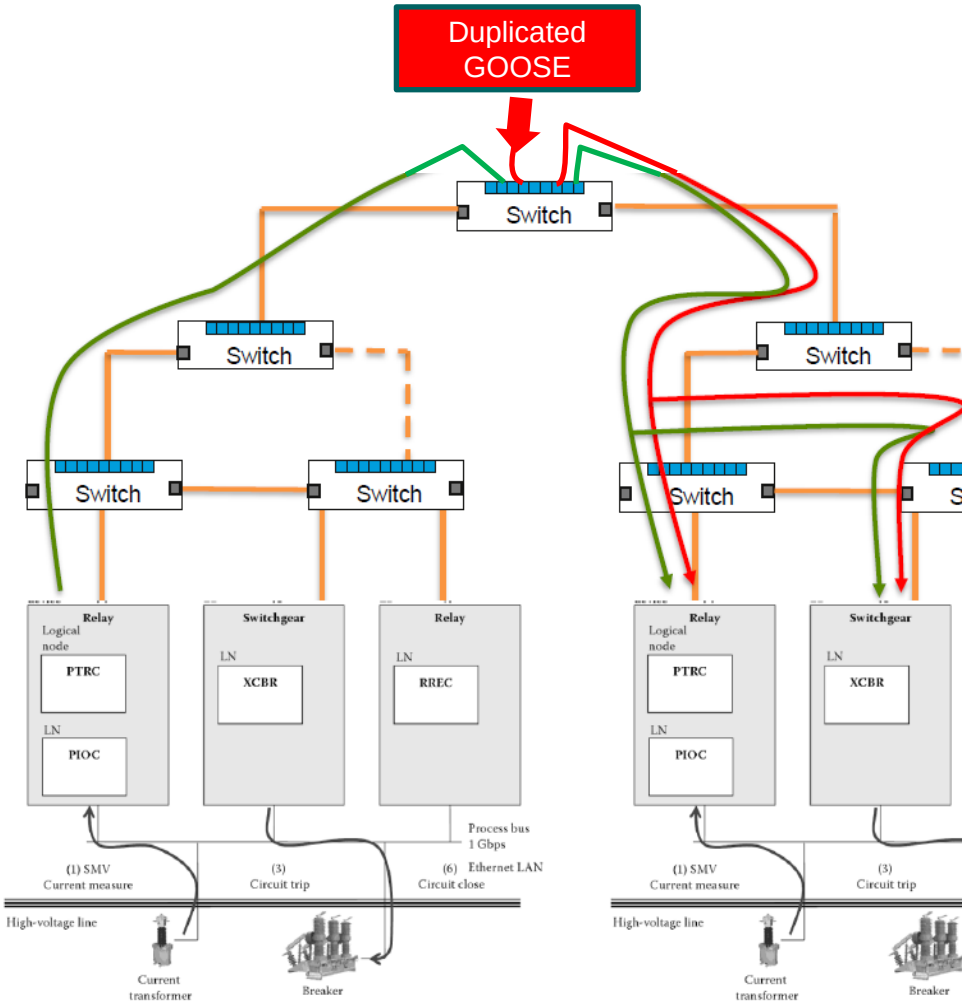
GOOSE подмена пакета

GOOSE подмена

Злонамеренная атака



Обнаружение источника



In case of tampered GOOSE, only the switch where “Duplicated GOOSE” is connected may detect the alarm

The said switch is the one that issues the alarm making easy the diagnosis of the fault location

Тревога по факту обнаружения

GOOSE Packet

Monitoring Table

Update Interval: every 5 secs

All	APP ID	GOOSE Address	IED Name	VID	Ingress Port	Rx Counter	Status	Type
☐	a	01:0c:cd:01:01:ff	IEDScout	1	1-2	64	Health	Dynamic

Reset Delete Set Static

- **Description**
  - The same GOOSE message from different source ports
  - Only Reset action can clear Tampered Event

GOOSE Packet Tampered GOOSE Packet

Monitoring Table

Update Interval: every 5 secs

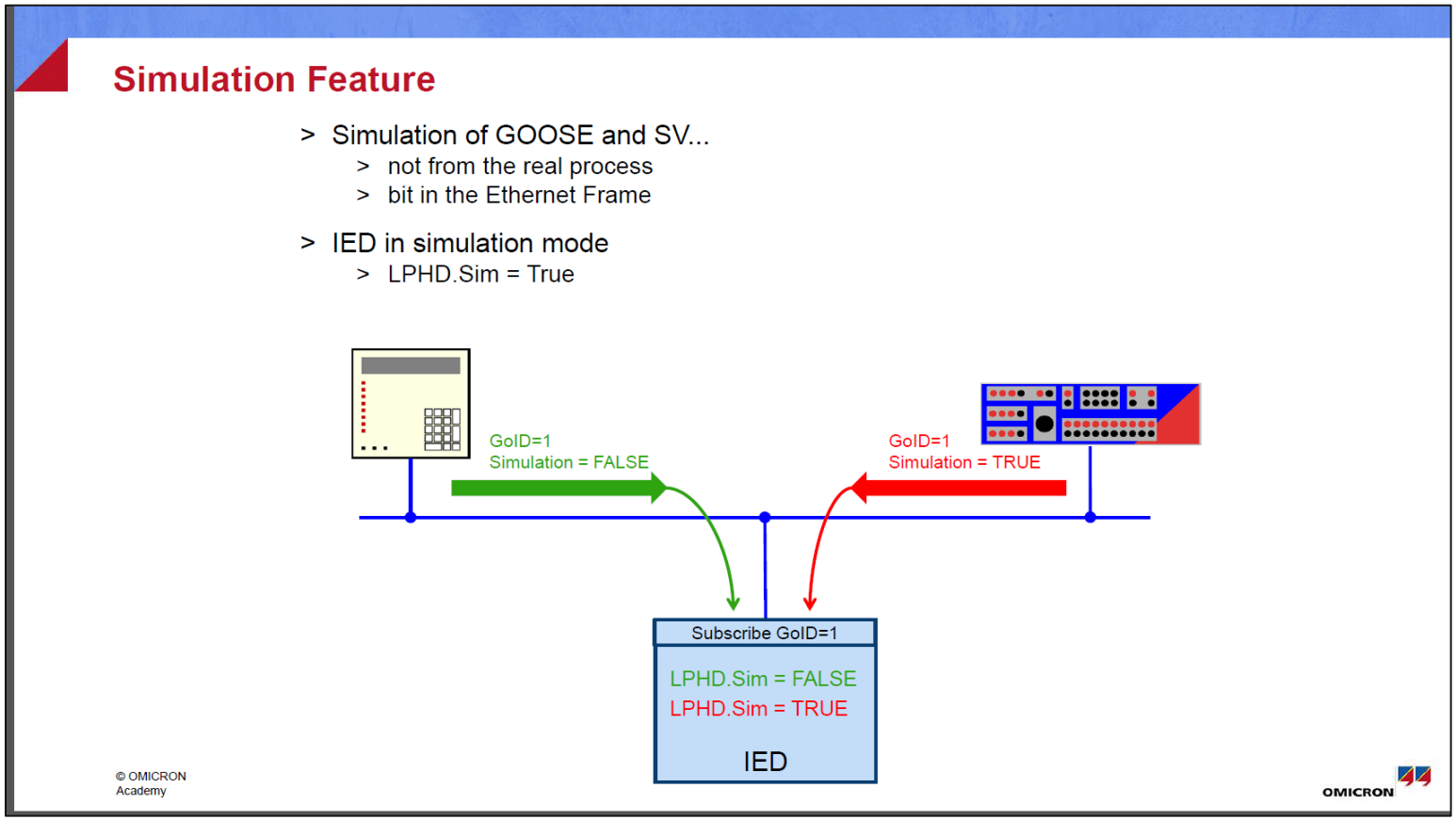
All	APP ID	GOOSE Address	IED Name	VID	Ingress Port	Rx Counter	Status	Type
☐	a	01:0c:cd:01:01:ff	IEDScout	1	1-2	284	Tampered	Dynamic

Reset Delete Set Static

Tampered GOOSE
- Same APPID
- Same DA
- Different Port ID

Не-злонамеренная подмена GOOSE

Simulation feature introduced with IEC61850 Edition 2



Example of IEC61850 Test with Omicron test equipment

GOOSE -задержки

GOOSE причины задержек

The GOOSE messages transmitted in the network can be influenced by noise, traffic, or human error, resulting in the packets not being received within a certain time frame.

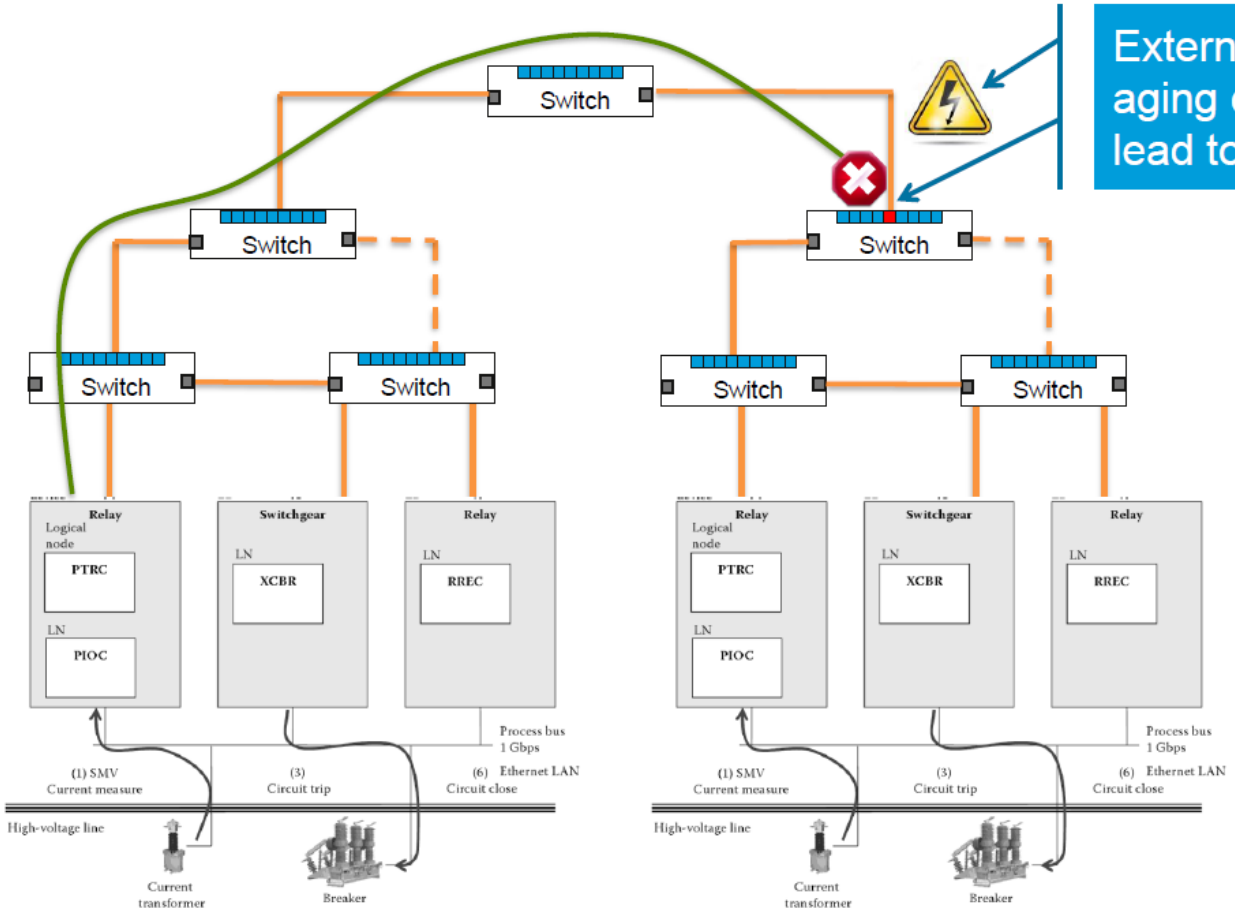
When it happens, switches will issue a Time-Out Alarm

It may happen:

- When CRC is wrong
- When next GOOSE is received after “maximum delay”

GOOSE задержка (time out)

Из-за плохой среды

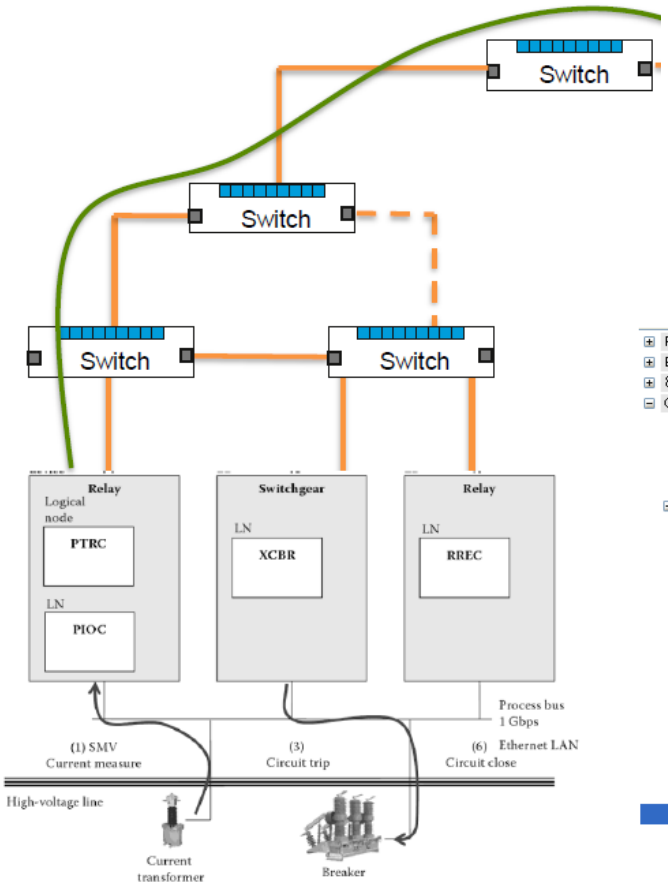


Packet with wrong CRC is discarded and so it is not forwarded to next switch

Switch discovering wrong CRC issues Time-Out alarm (no need waiting for next switch to flag the time-out)

GOOSE задержка (time out)

Перегрузка трафиком



IEC 61850-8-1 defines timeAllowedtoLive (TATL) for each GOOSE message, which is the maximum validity period for a GOOSE message

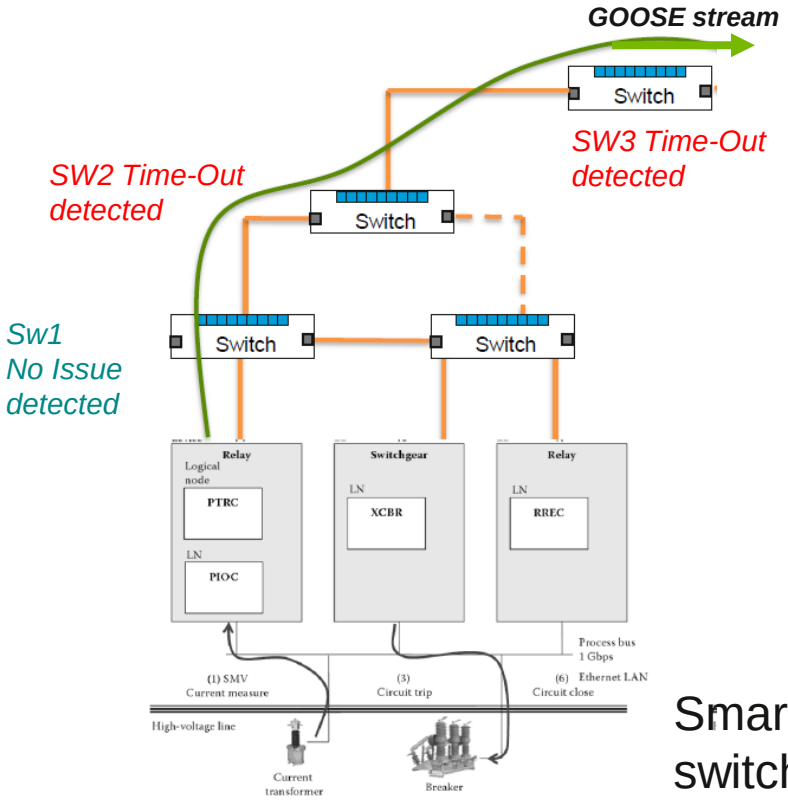
```
⊞ Frame 1 (132 bytes on wire, 132 bytes captured)
⊞ Ethernet II, Src: 34:08:04:2a:ad:d8 (34:08:04:2a:ad:d8), Dst: Iec-Tc57_01:01:ff (01:0c:cd:01:01:ff)
⊞ 802.1Q Virtual LAN, PRI: 4, CFI: 0, ID:
⊟ GOOSE
    APPID: 0x3fff (16383)
    Length: 114
    Reserved 1: 0x0000 (0)
    Reserved 2: 0x0000 (0)
  ⊟ goosePdu
      gocbRef: IEDScout/LLN0$GO$Eval
      timeAllowedtoLive: 300
      datSet: IEDScout/LLN0$Eval_DataSet
      goID: GOOSEID
      t: 531D36AC9DB33C00
      stNum: 61
      sqNum: 0
      test: False
      confRev: 1
      ndsCom: False
      numDatSetEntries: 3
    ⊟ allData: 3 items
      ⊞ Data: boolean (3)
      ⊞ Data: integer (5)
      ⊞ Data: bit-string (4)
```

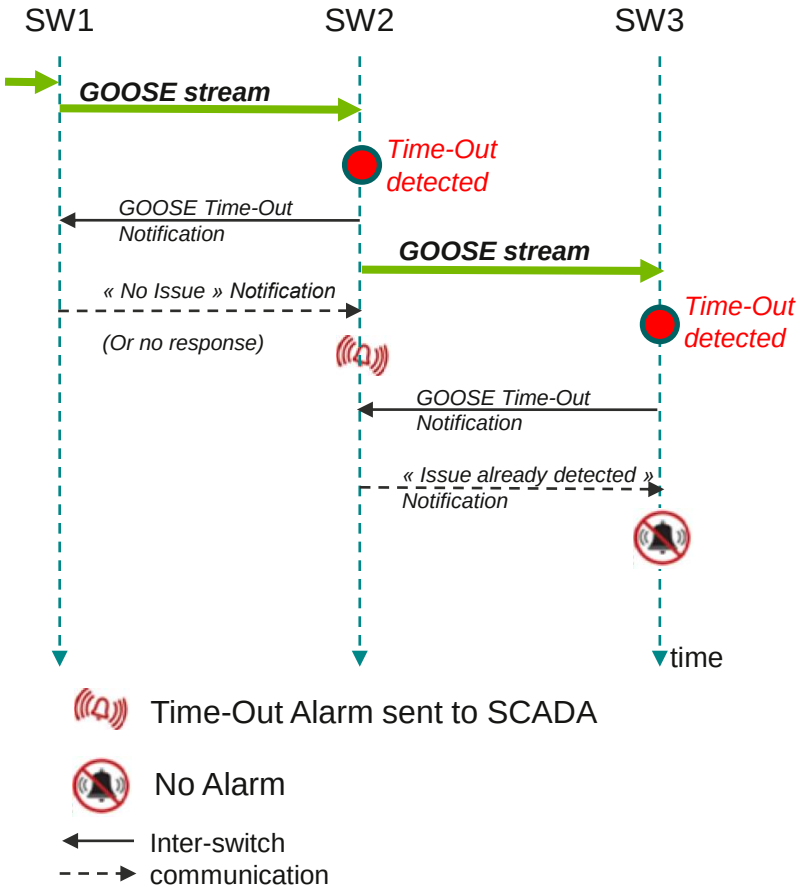
Time Allowed To Live: TATL (ms)

MOXA

Поиск источника задержки

In case of GOOSE Time-out, several switches along GOOSE path may detect the same Time-Out alarm





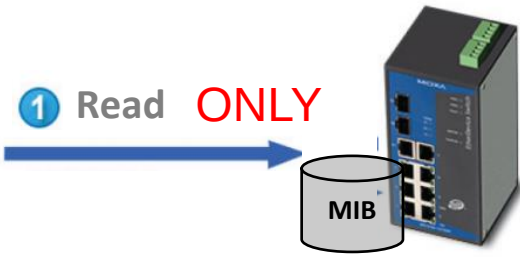
Smart Alarming mechanism ensures that only the first switch that detects the issue, raises the alarm. Time-out root cause is obviously nearby to the said switch

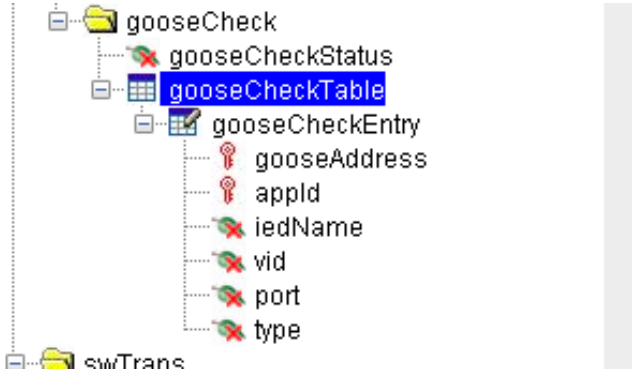
Интеграция в SCADA систему

SNMP

MIB

SNMP Manager





GOOSE state is not available through SNMP

TRAP

SNMP Manager

gooseCheckTrap

"GOOSE Timeout: Port 1-2 0x0001 01:0c:cd:01:00:00"

"GOOSE Tampered by Port1-4: Port1-4 0x0001 01:0c:cd:01:00:00"

Trap examples consider below GOOSE message

APP ID	GOOSE Address	IED Name	VID	Ingress Port	Rx Counter	Status	Type
1	01:0c:cd:01:00:00	BC_CONTCTRL	1	1-2	85	Health	Static

IEC 61850 модель данных

Moxa proprietary logical Node LGOC

Logical Node LGOC				
Data object name	**Common data class**	**Data Attribute**	**Data format**	**Description**
GoApId	INS	stVal	Long	GOOSE APPID
GoAddr	VSS	stVa	Vstring255	Multicast address
IedName	VSS	stVal	Vstring255	IED name
Vid	INS	stVal	Long	VLAN ID
InPort	VSS	stVal	Vstring255	Ingress port
RxGoCnt	BCR	stVal	Int64	Rx GOOSE counter
GoStatus	ENG	stVal	Enum	GOOSE status. 0=health, 1=timeout, 2=tampered

Реализация в коммутаторах Moxa

МЭК 61850-3 Layer 2 and Layer 3 управляемый коммутатор

PT-G7728/G7828

IEC 61850-3
IEEE 1613

- **IEEE 1588 Gigabit PTP – Power / Default Profile and PTP Sync LED индикация**
- **GOOSE Checking– мониторинг потоков GOOSE**
- **Hot Swappable – все модули горячей замены**
- **Dying Gasp – сигнал при потере питания**
- **MMS Server – интеграция со SCADA**

- 2 x 10/100/1000 BaseT(X) and 2 x 100/1000 BaseX SFP port

6 slots, each slot can choose
- 4 x 10/100/1000 BaseT(X), PoE/PoE+
- 4 x 100/1000 BaseX SFP slot

- LV: 24/48 VDC (18 to 72 VDC)
- HV: 110/220 VDC/VAC
- External PoE (720W)

Мониторинг Goose сегодня и завтра

Today

- Enhanced Cybersecurity
- Node-based, distributed detection anomalies in IEC-61850 communication
- GOOSE fingerprinting

Tomorrow

- Integration in host-based systems for
  - GOOSE counter analytics
  - Buffering of anomalous GOOSE packets
  - GOOSE event log
  - GOOSE communication scheme (matrix) verification

Спасибо

Лопухов Иван Владимирович
менеджер по работе с ключевыми клиентами
Представительство Moxa Inc. в России

Tel : +7 (495) 287 09 29 ext. 208

Skype id: ivan_lopukhov

ivan.lopukhov@moxa.com

MOXA®
Reliable Networks ▲ Sincere Service