IEC 61850: New Needs and Solutions

New GOOSEs…

Mark Adamiak
GE Grid Automation

imagination at work

Simplified GOOSE Exchange

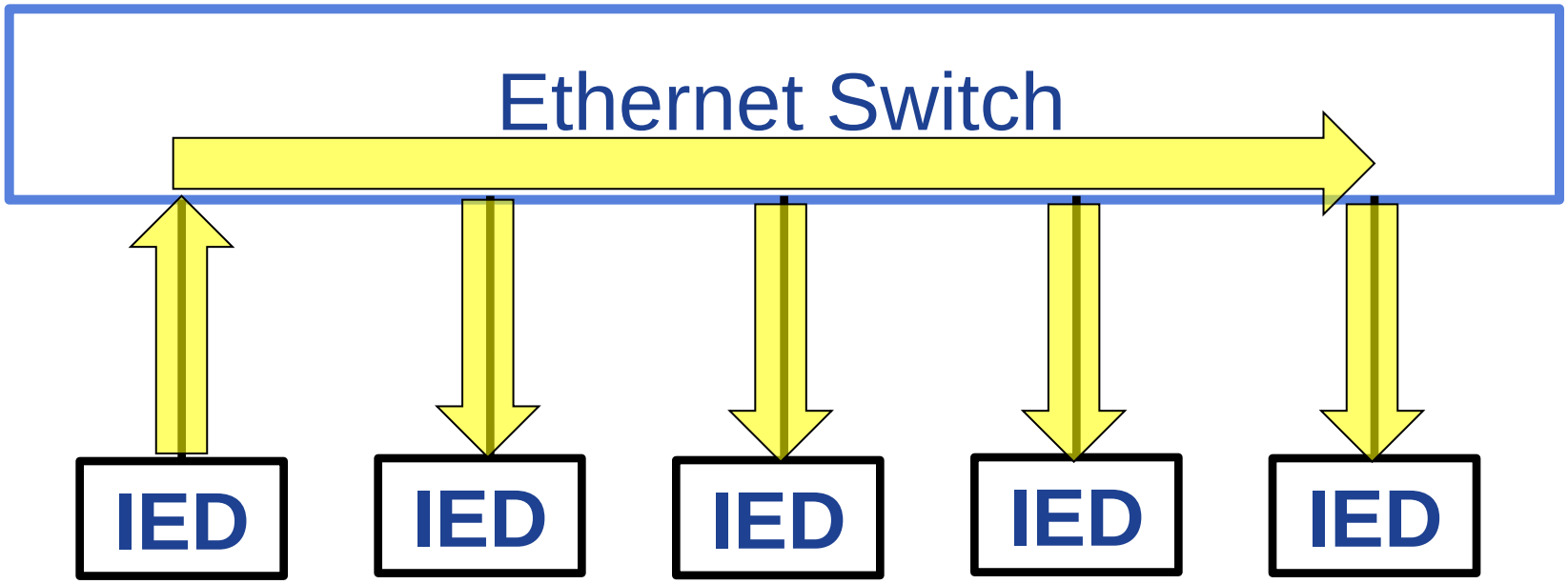
GOOSE Launched

- Change of Data
- Integrity period time-out

- GOOSE received by one or more subscribers

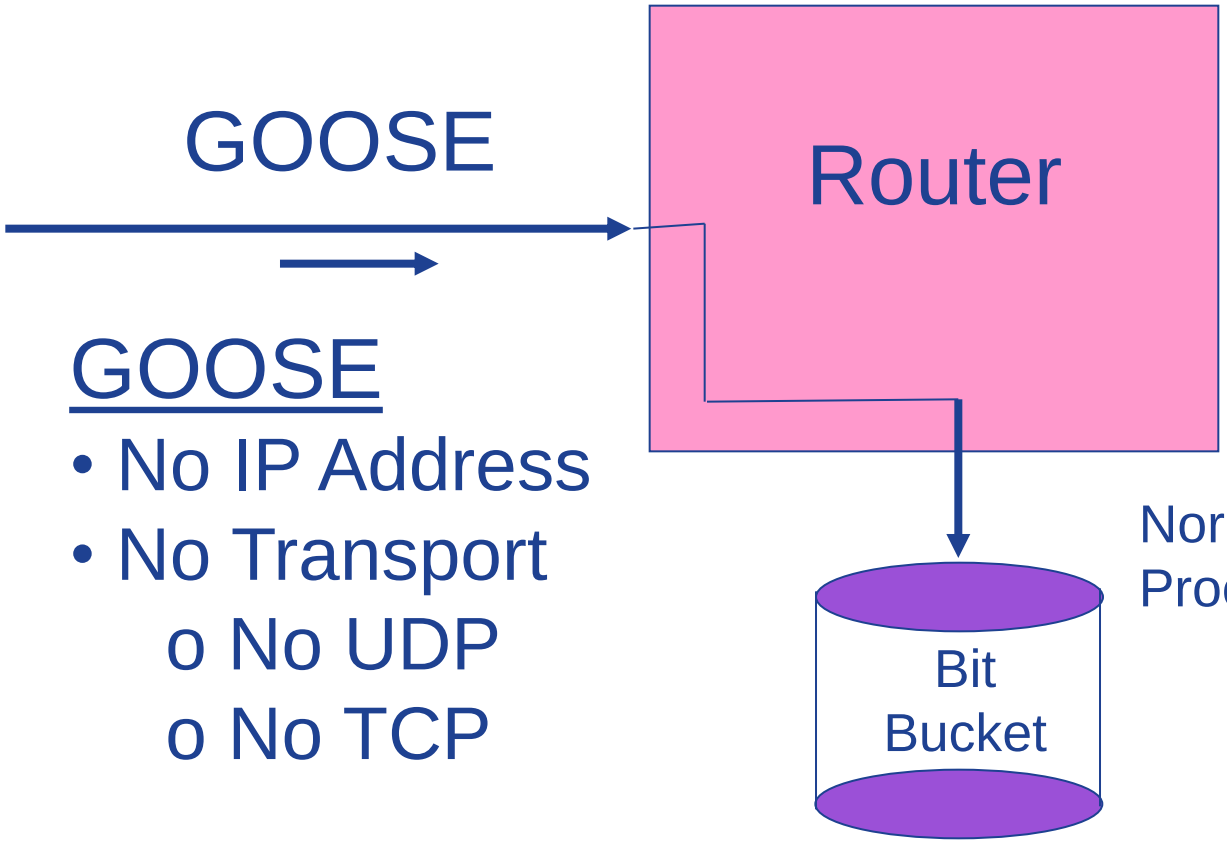
No animals were *permanently* harmed in this GOOSE exchange

GOOSE over Local Area Network



Multicast Message….One to Many

Original GOOSE into a Router…

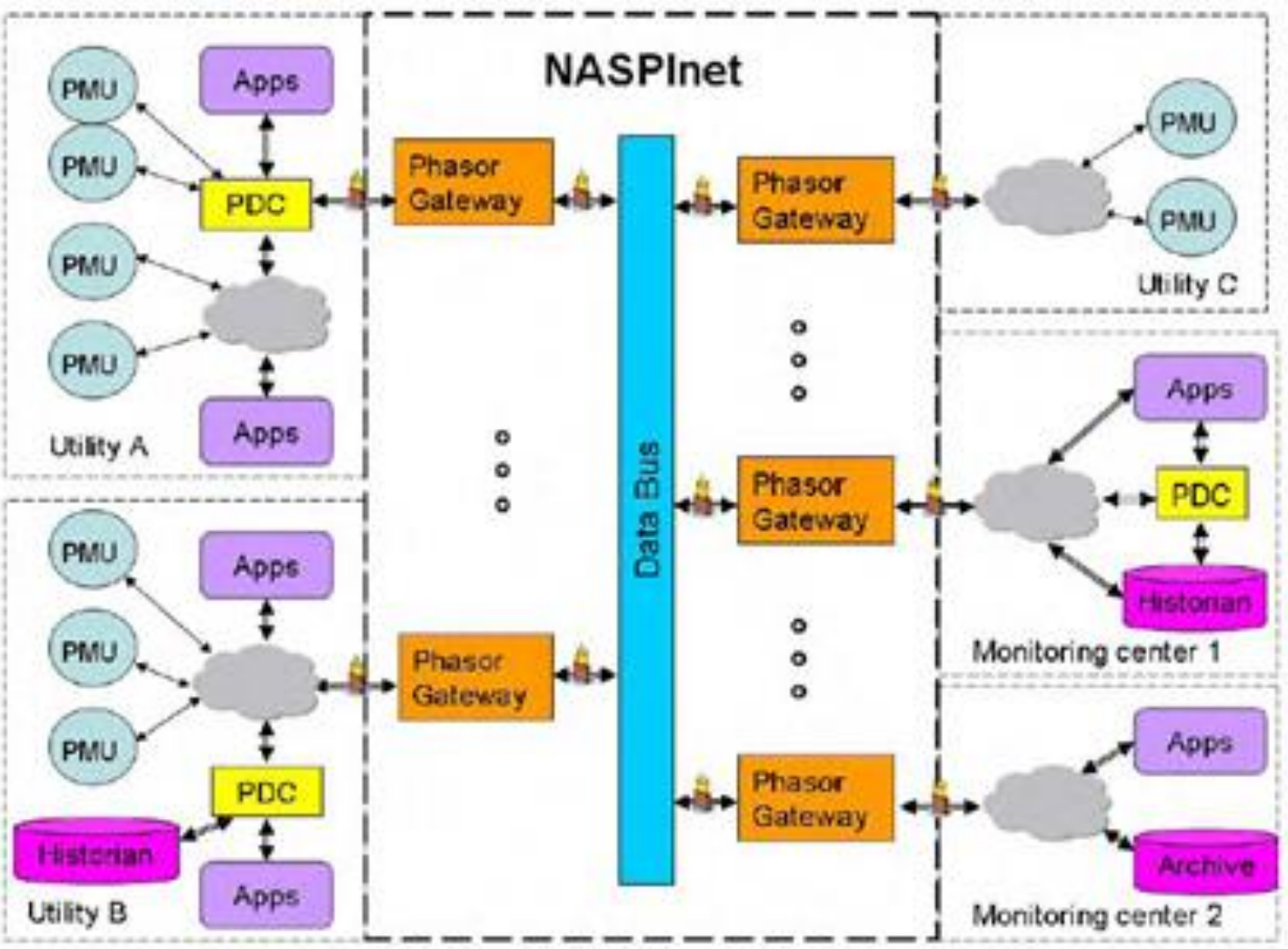


GOOSE

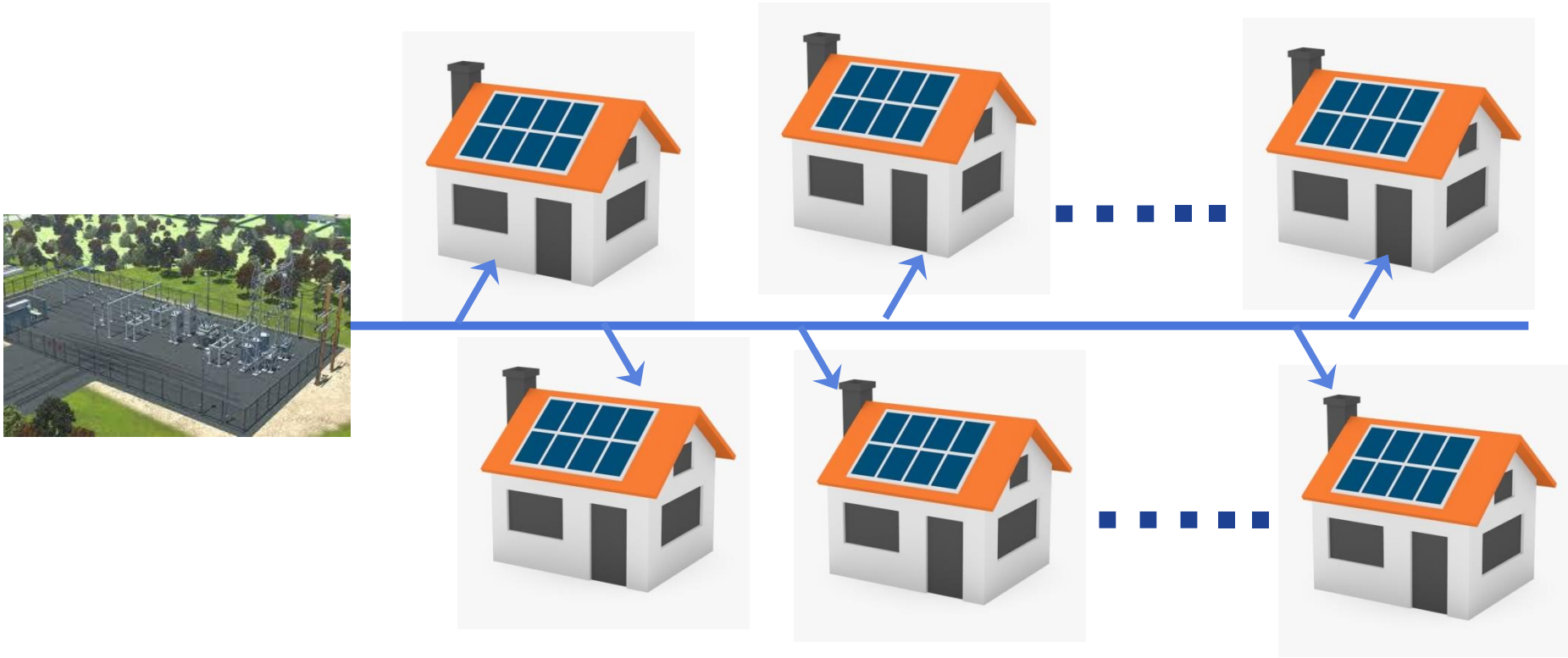
- No IP Address
- No Transport
  - o No UDP
  - o No TCP

Designed for Local Area Operation

Synchrophasor Use Case:

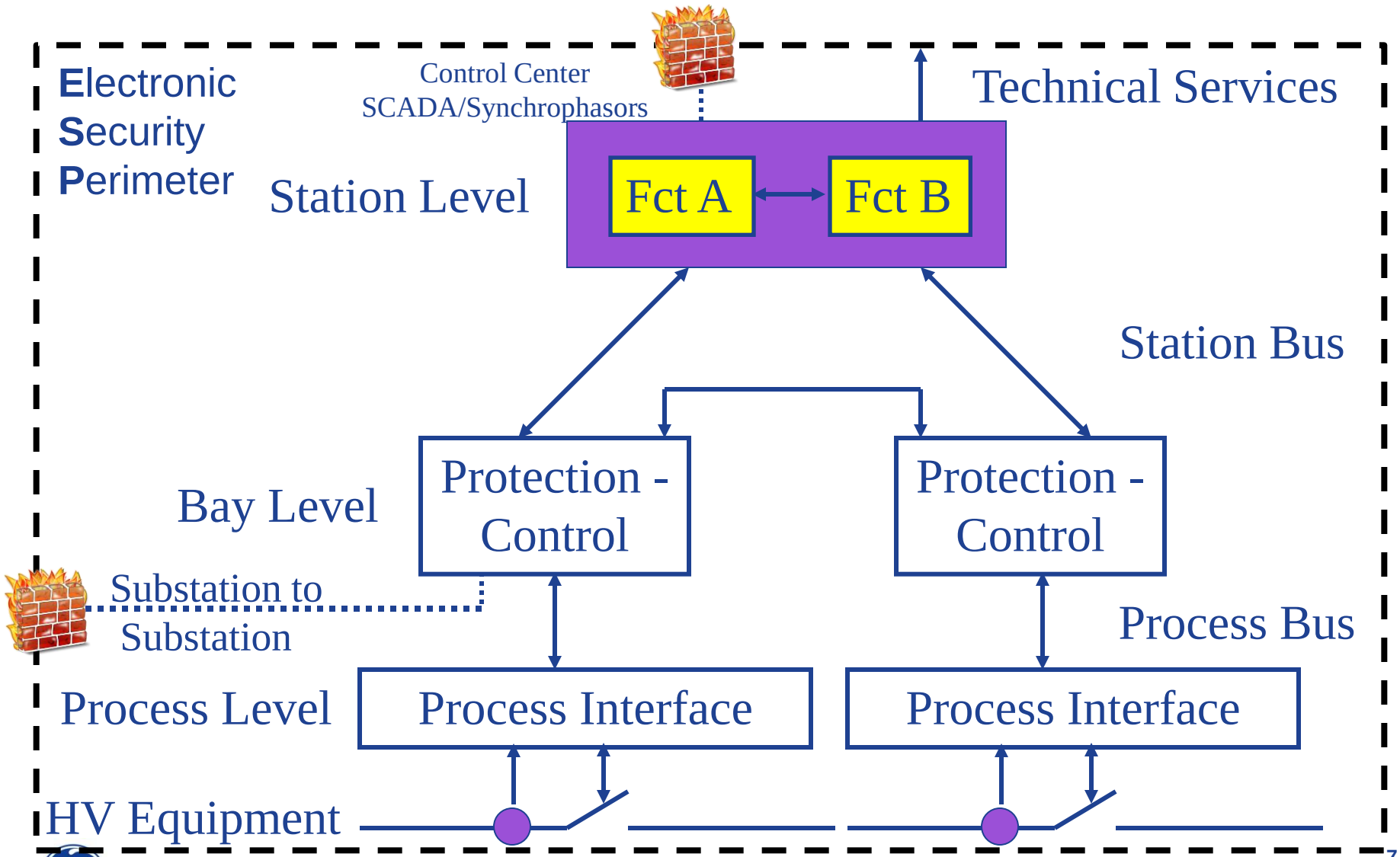


New Use Case: One to Many Communication



Need: Secure Setpoint Communication

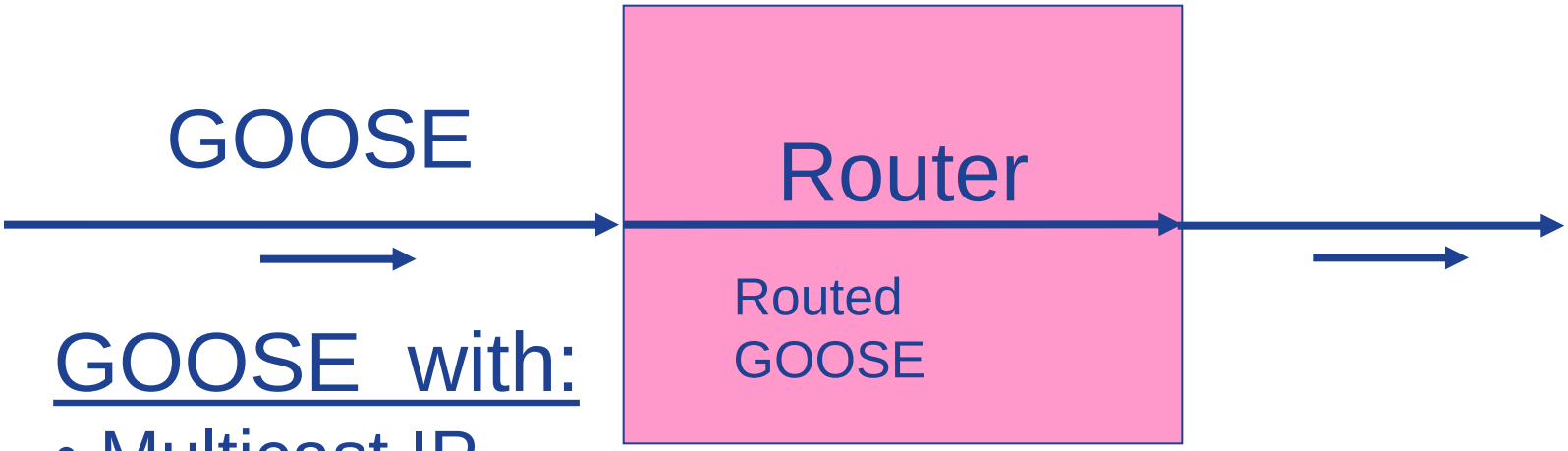
The *Evolving* IEC61850 Interface Model



imagination at work

Crossing the ESP Requires Security

Needed: a SECURE Routable GOOSE



GOOSE with:

- Multicast IP
- UDP Transport (reliability through message repea
- Supported by Routers
  - No configuration required

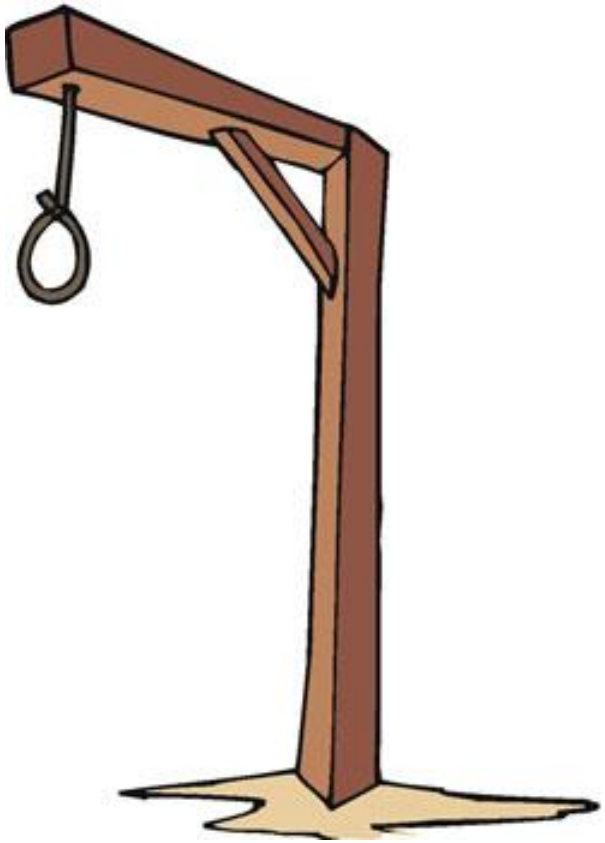
Committee Approved Technical Report:

IEC 61850: COMMUNICATION NETWORKS AND SYSTEMS FOR POWER UTILITY AUTOMATION –

Part 90-5: Use of IEC 61850 to transmit synchrophasor information according to IEEE C37.118

Mark's Proposed name for IEC 90-5: **N**etworked **O**bject **O**riented **S**ubstation **E**vent

The NOOSE !



imagination at work

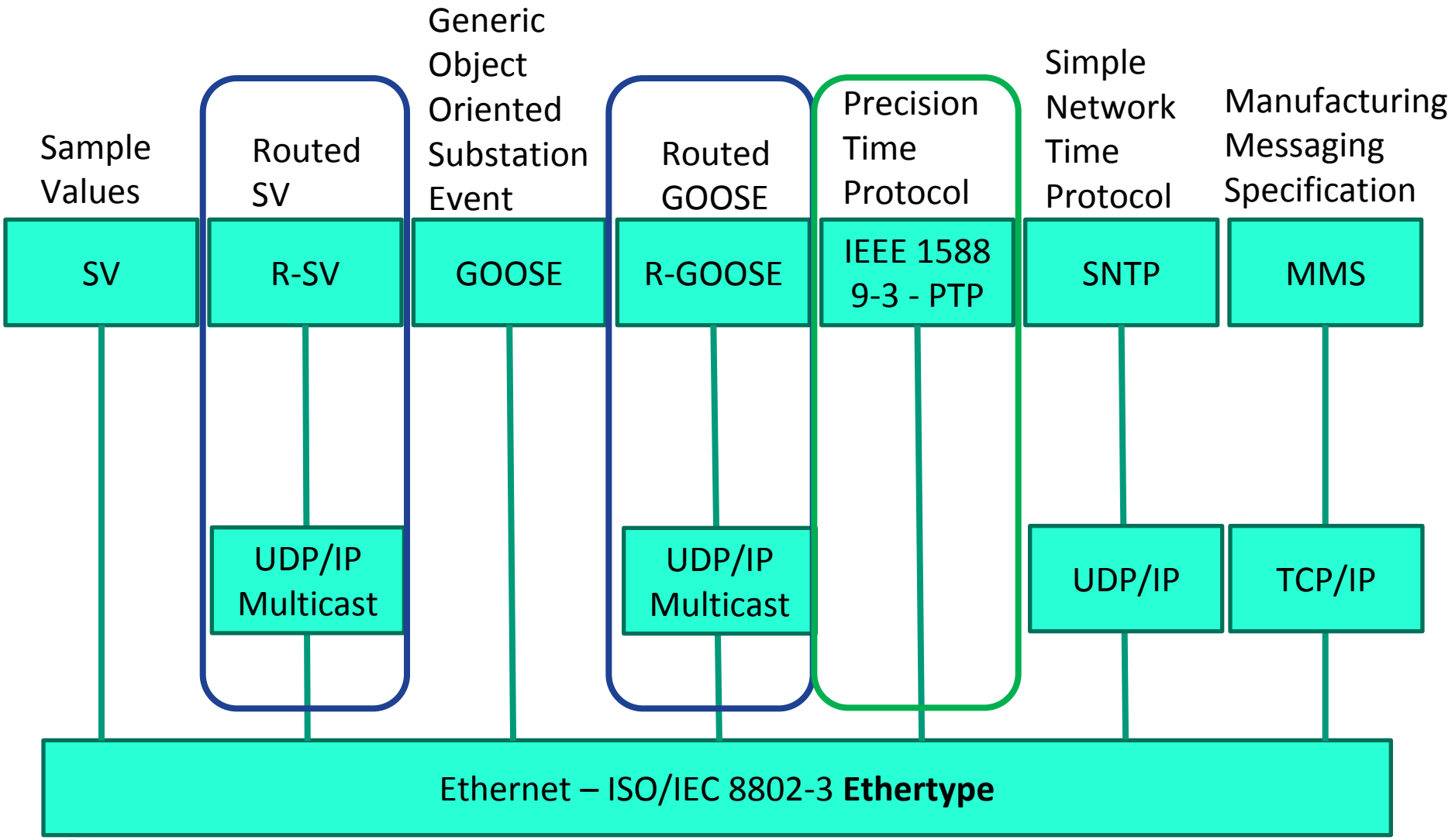
But people go hung up on the idea…..
So we have:

- R-GOOSE (for Routed GOOSE)
  - For routing of ***Event*** Data

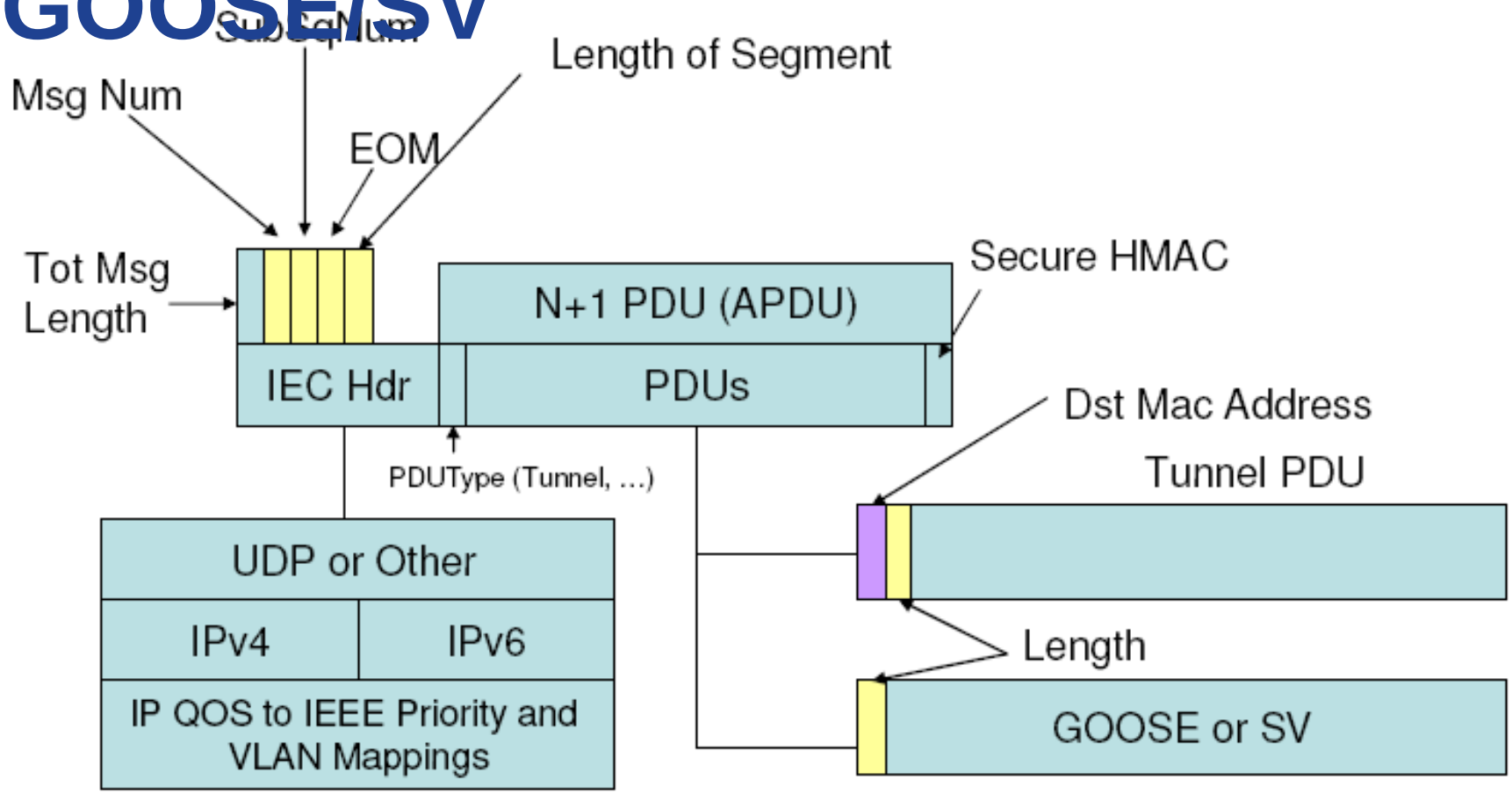
And

- R-SV (for Routed Sample Values)
  - For routing ***periodic*** data
    - Used for synchrophasors

61850 Profiles

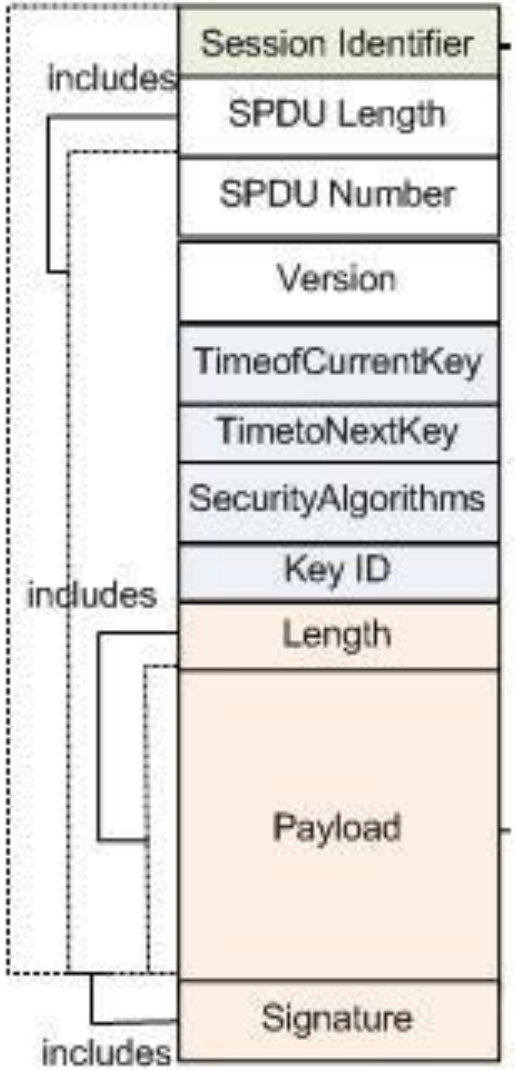


IEC 61850 90-5 Networked GOOSE/SV



IEC 90-5 Data Model

SPDU: Session Protocol Data Unit

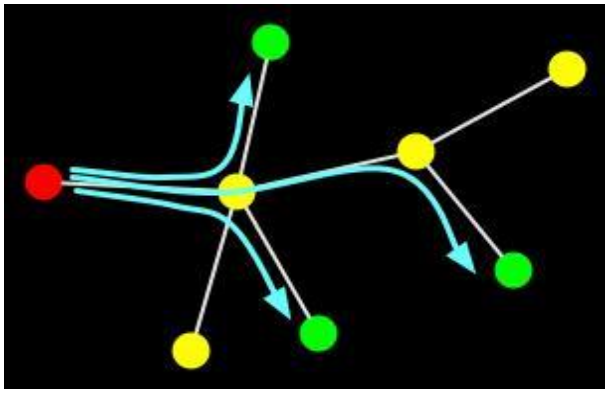


Detail Format

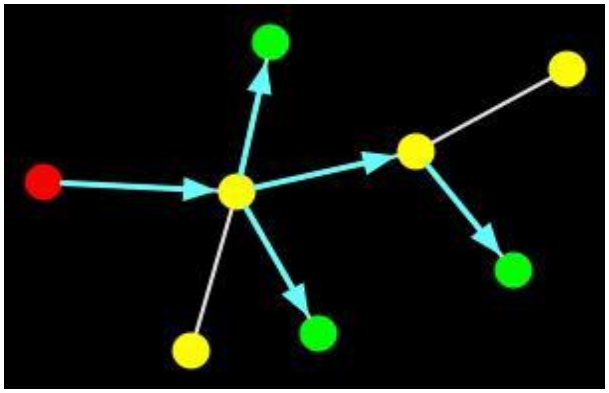
Total Max Size: 65535 bytes

Unicast vs. Multicast

Point-to-Point
Multiple Streams



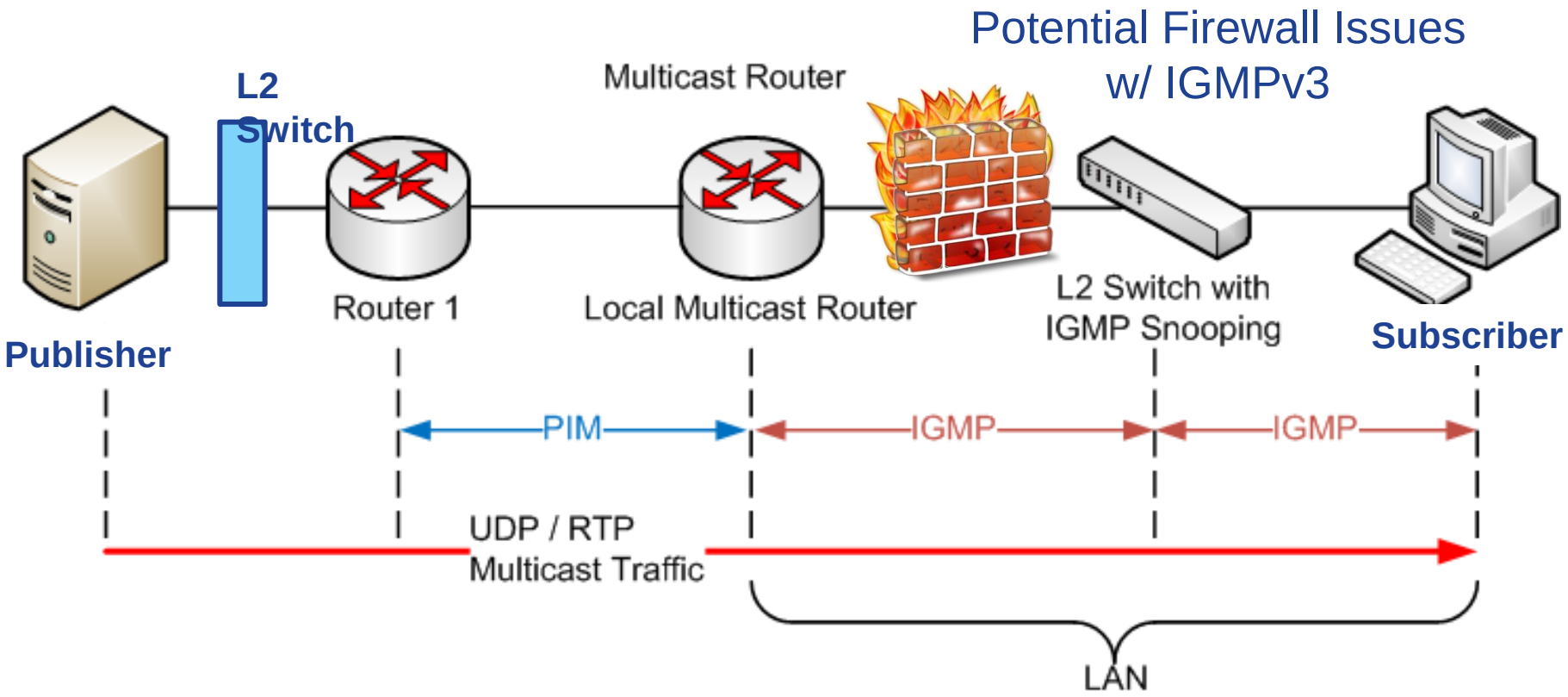
Multicast
One Output Stream



Unicast:

- Requires 3x Bandwidth (in this example)
- 3X Infrastructure $$$$

Multicast Path Establishment via Internet Gateway Management Protocol – IGMP Ver. 3



XML Configuration Example

```
<DataSet name="PMUdata">
        <FCDA ldInst="PMU" prefix="" lnClass="MMXU" lnInst="1" doName="A.PhsA" fc="M
        <FCDA ldInst="PMU" prefix="" lnClass="MMXU" lnInst="1" doName="A.PhsB" fc="M
        <FCDA ldInst="PMU" prefix="" lnClass="MMXU" lnInst="1" doName="A.PhsC" fc="M
        <FCDA ldInst="PMU" prefix="" lnClass="MMXU" lnInst="1" doName="Health" fc="ST
</DataSet>
```

Configures:

- Phase A, B, and C Amps
- IED Health Status

DUCK Impersonating GOOSE over T1….

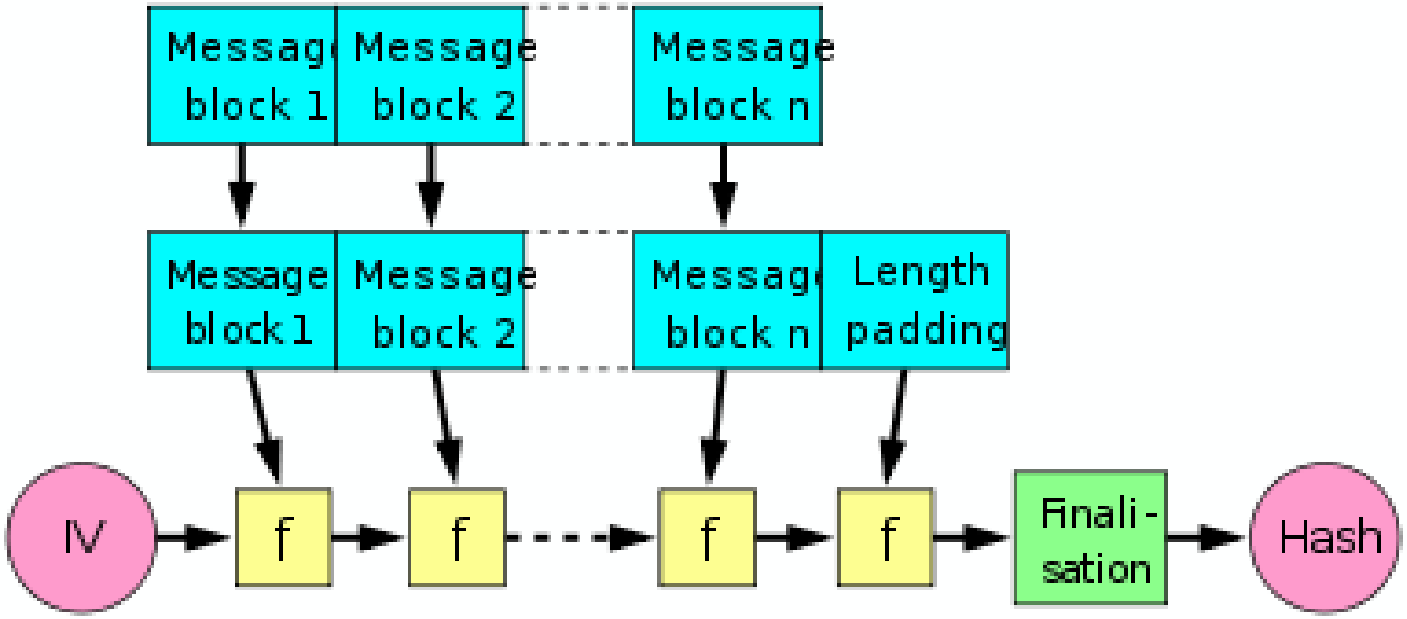
Need Authentication…..

Security Definition

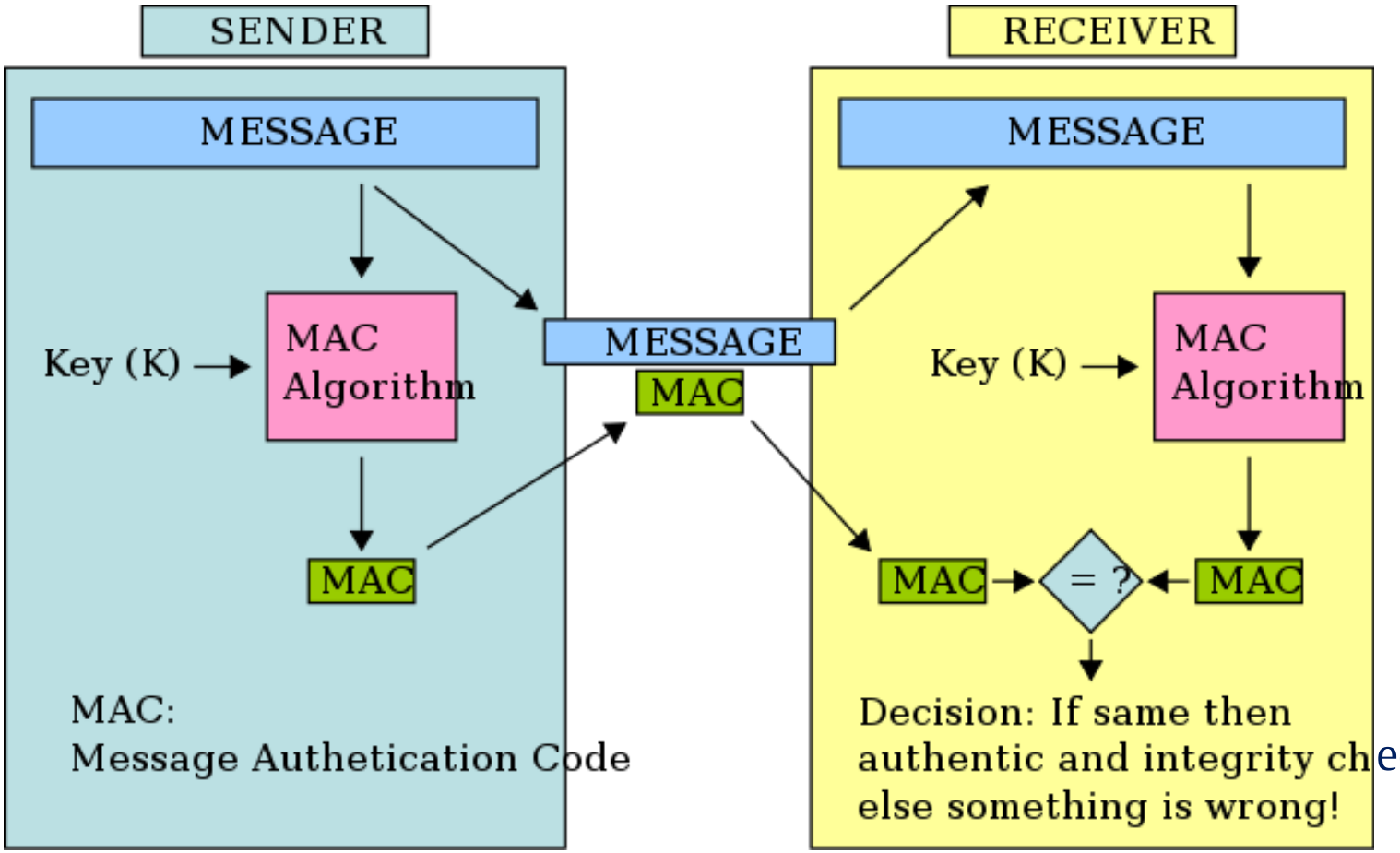
- Defines a SHA-256 (32 byte) Hash code for message authentication / integrity
- Defines the Advanced Encryption Standard (AES) as the encryption algorithm
- Identifies / Extends a Key management system
  - RFC 6407 The Group Domain of Interpretation - GDOI
  - The publisher manages the keys to all subscribers
  - Same key for Hash and Encryption

Hash Function Concept

- Processes an arbitrary-length message into a fixed-length output
- Typical implementation breaks the message into N blocks and operates on each block in sequence

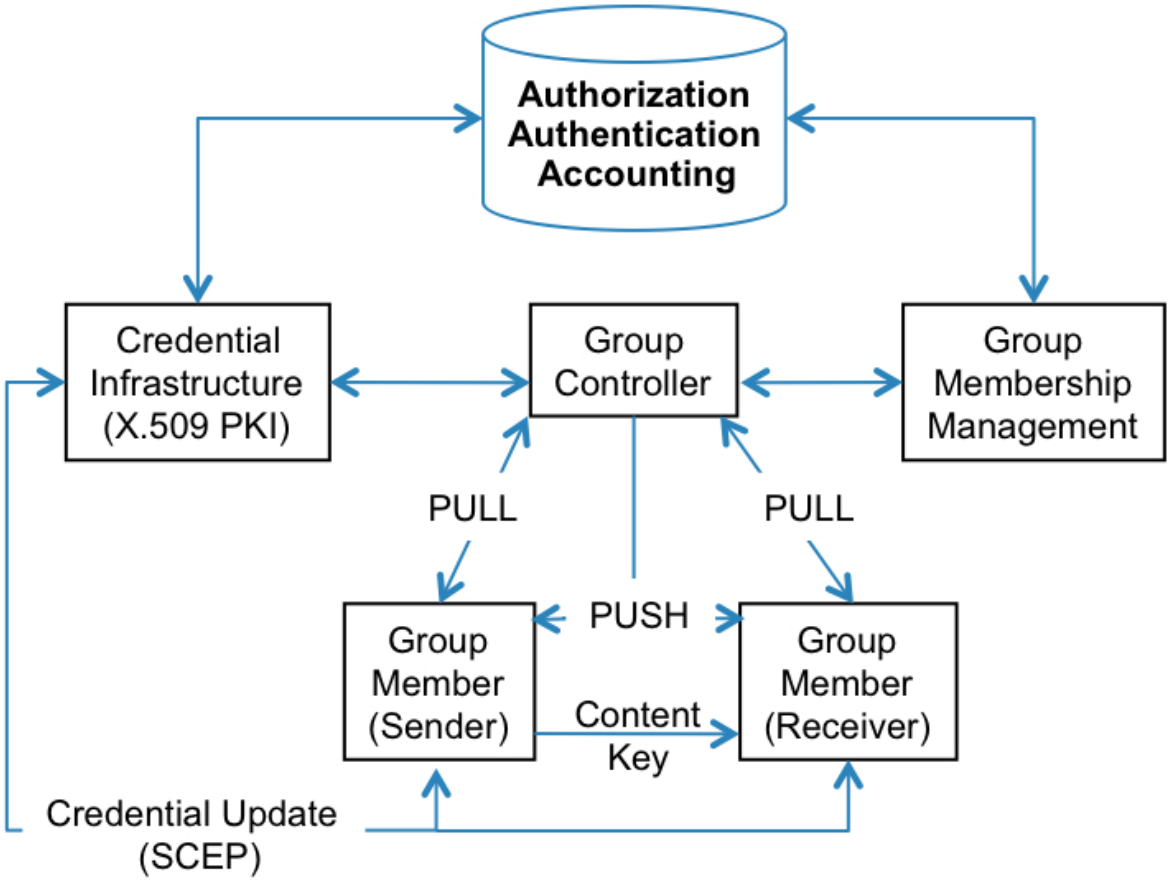


Cryptographic Hash Concept



Also known as a Hash based Message Authentication Code – **HMAC**
Also called a Message Integrity Code **- MIC**

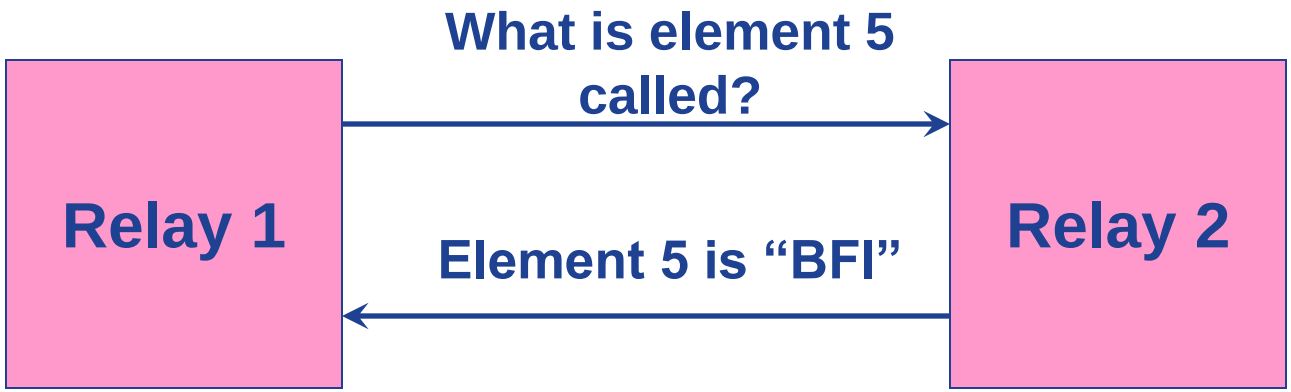
Group Domain of Interpretation - GDOI



- Publishers act as Controllers
- Receiving Group Members “Pull” new keys
- Centralized Authorization Management

GOOSE Services

- **GetGoReference – Retrieve the Data Name for a specific dataset member reference**
- **GetGOOSEElementNumber– Retrieve the position of a member in a Dataset**



GOOSE Services Enable Virtual Wire Check and Self Description!