Transforming the world of energy using open standards

Securing Routable GOOSE for Wide Area Remedial Action Schemes

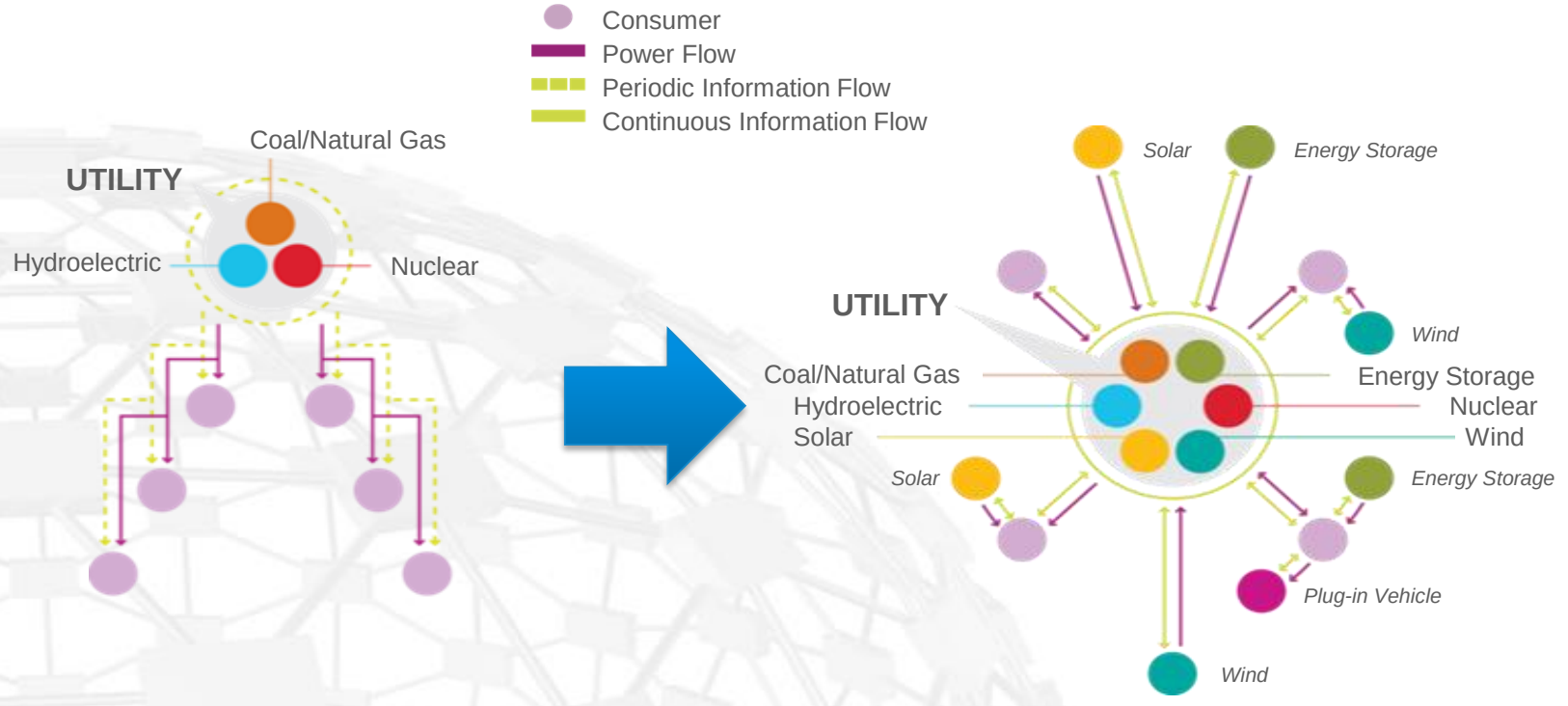
29 March 2019
i-PCGRID Workshop
San Francisco, CA USA

Ralph Mackiewicz
SISCO, Inc.
6605 19 1/2 Mile Road
Sterling Heights, MI 48314 USA
Tel: +1-586-254-0020 ext. 103
Mob: +1-586-260-2571
E-Mail: ralph@sisconet.com
URL: https://www.sisconet.com

Agenda

- Autonomous grid protection architecture
- Need for securing infrastructure
- End to End security for protection messaging
- Challenges and practical solutions

The Nature of the Electric Utility is Transforming



TRADITIONAL

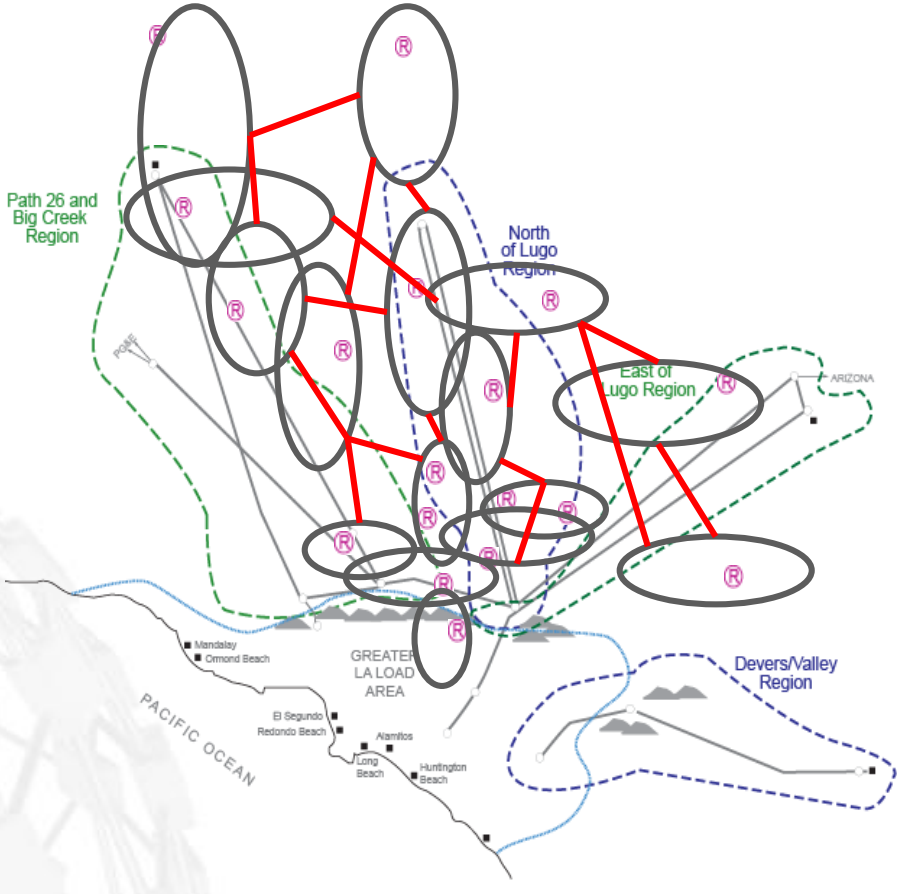
- Unidirectional power flow
- Large centralized energy resources
- Tag based Operational applications

TRANSFORMED

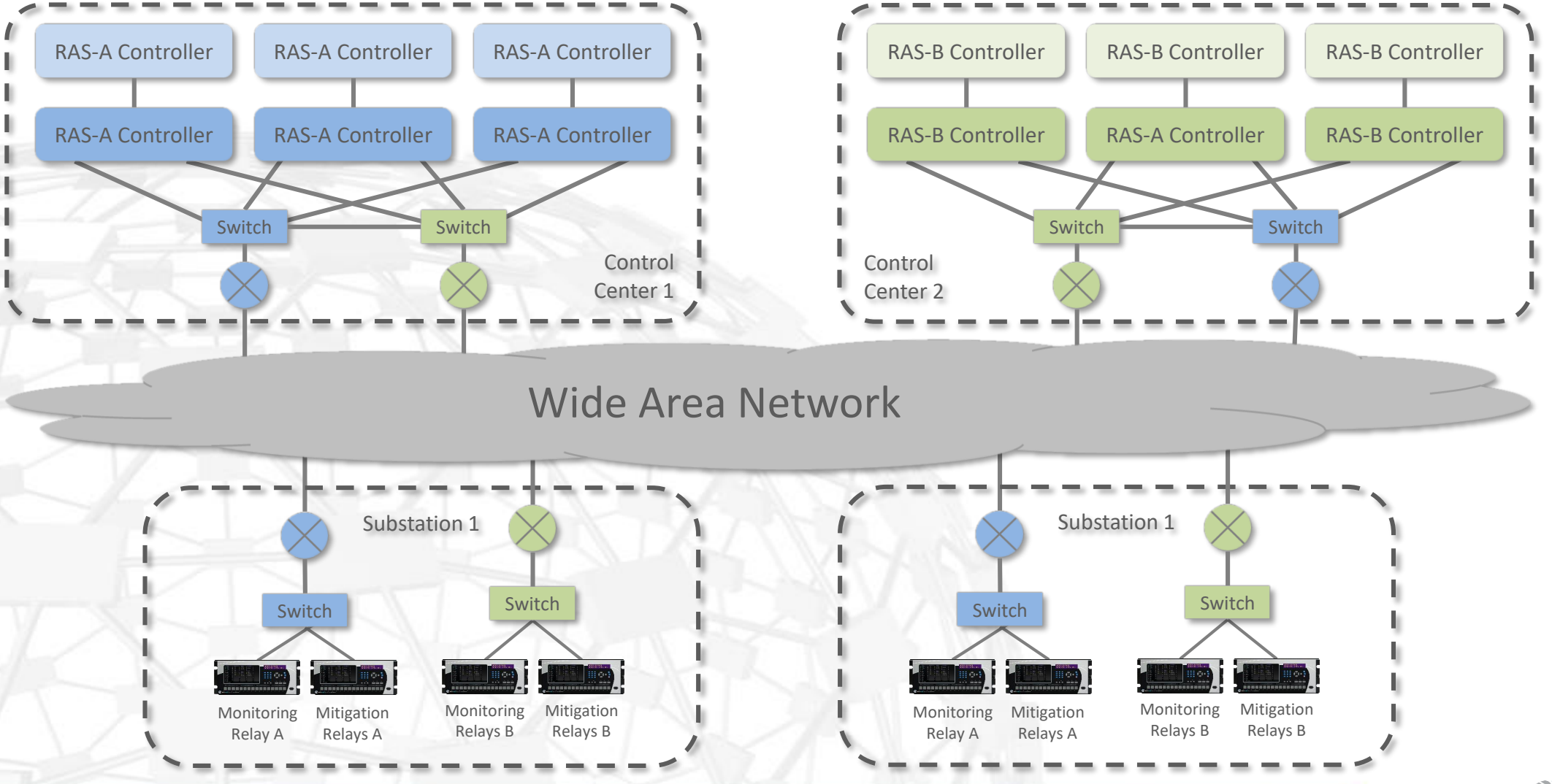
- Multi-directional power flow
- Numerous Distributed Energy Resources (DER)
- Model based Operational applications

Transformation Impacts SPS

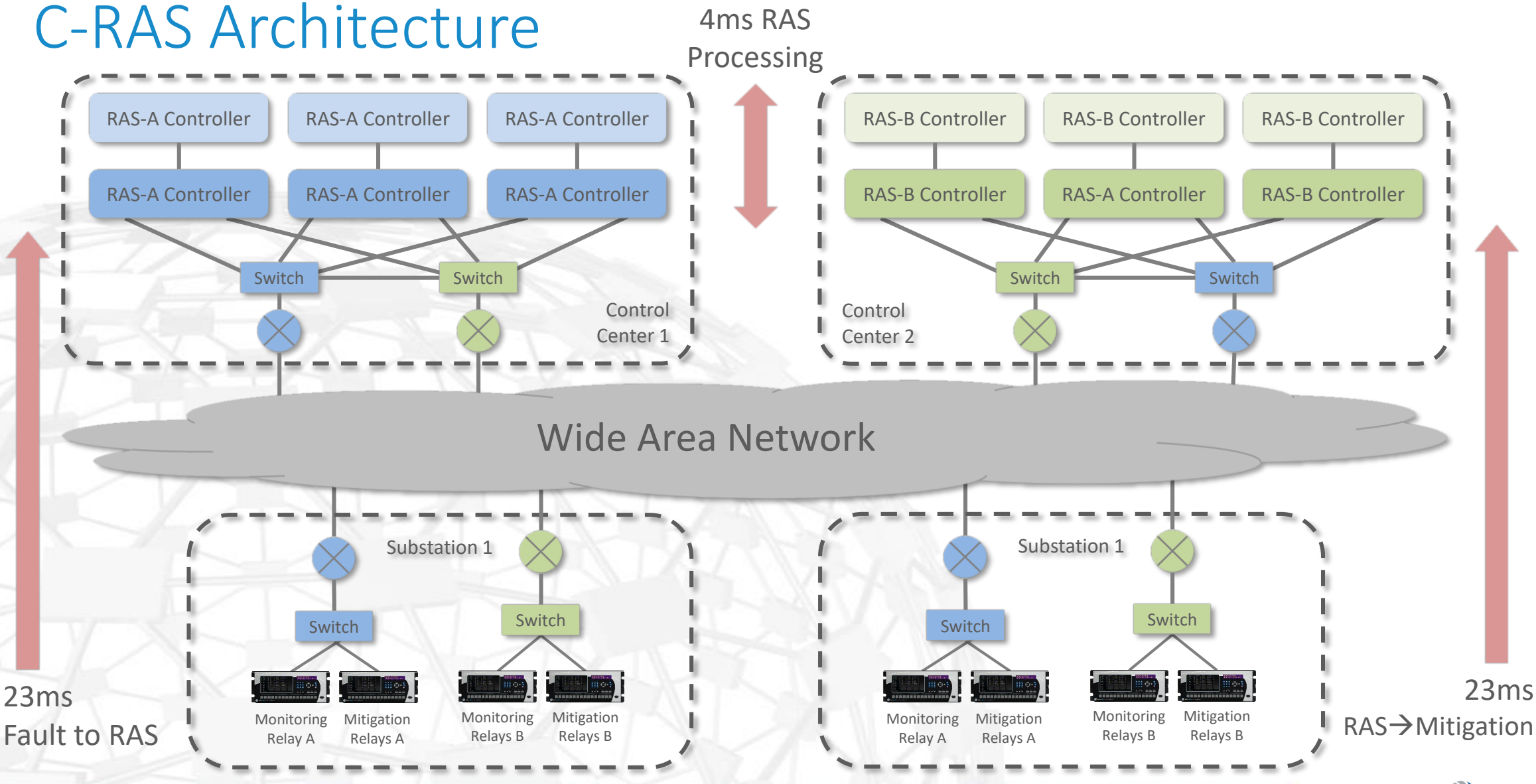
- Increasing system complexity requires proliferation of autonomous remedial action schemes (RAS) and SPS
- RAS needs information from outside its control area to perform autonomous action safely
- Information sharing and interactions between individual RAS using traditional techniques increases complexity and cost beyond what is practical
- Time critical control functions (<50ms fault to mitigation) makes multiparty distributed decision making difficult



C-RAS Architecture



C-RAS Architecture



C-RAS Supports This Transformation

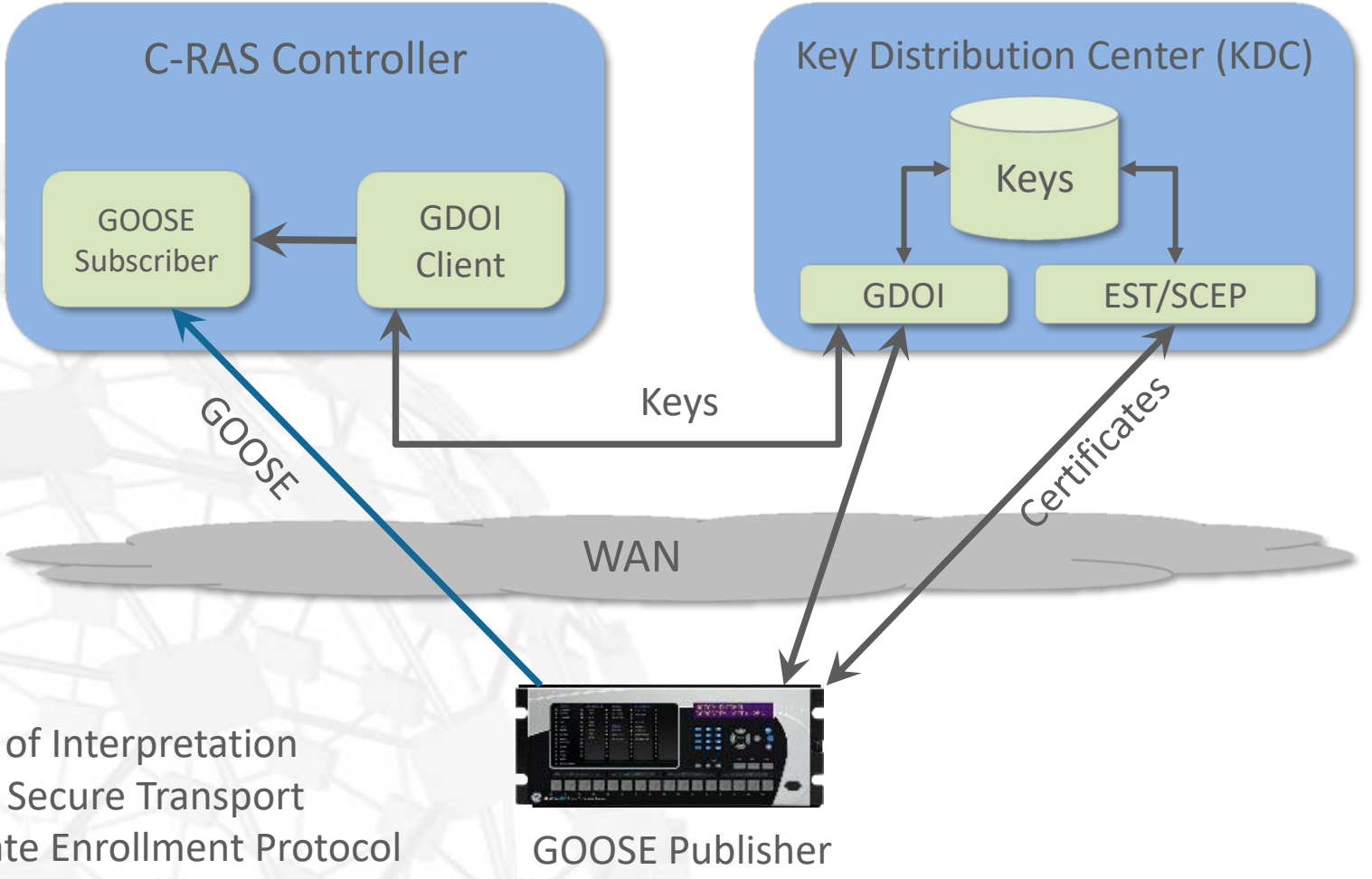
- High-performance multiply redundant system supports automated RAS processing with 100s of devices providing <50ms response from fault to mitigation
- Integration between RAS logic and EMS (load data, contingencies, generation data) and system operators is seamless and transparent enabling complex RAS for system and asset protection
- Made possible by the combination of modern network and computer technology with IEC 61850 Ethernet GOOSE and IP Multicast Routable GOOSE (R-GOOSE)
- Many other applications possible using the same platform with synchrophasor, DER, DMS, etc.

Securing R-GOOSE

- WAN is typically a private network with physical access restrictions to network connections for security
- Historically, such physical security was considered sufficient
- Some recent events and growing malware threats against energy control systems suggest otherwise
- The challenge is to apply cyber security controls to the communications and computing infrastructure without affecting performance and reliability
- This is becoming practical

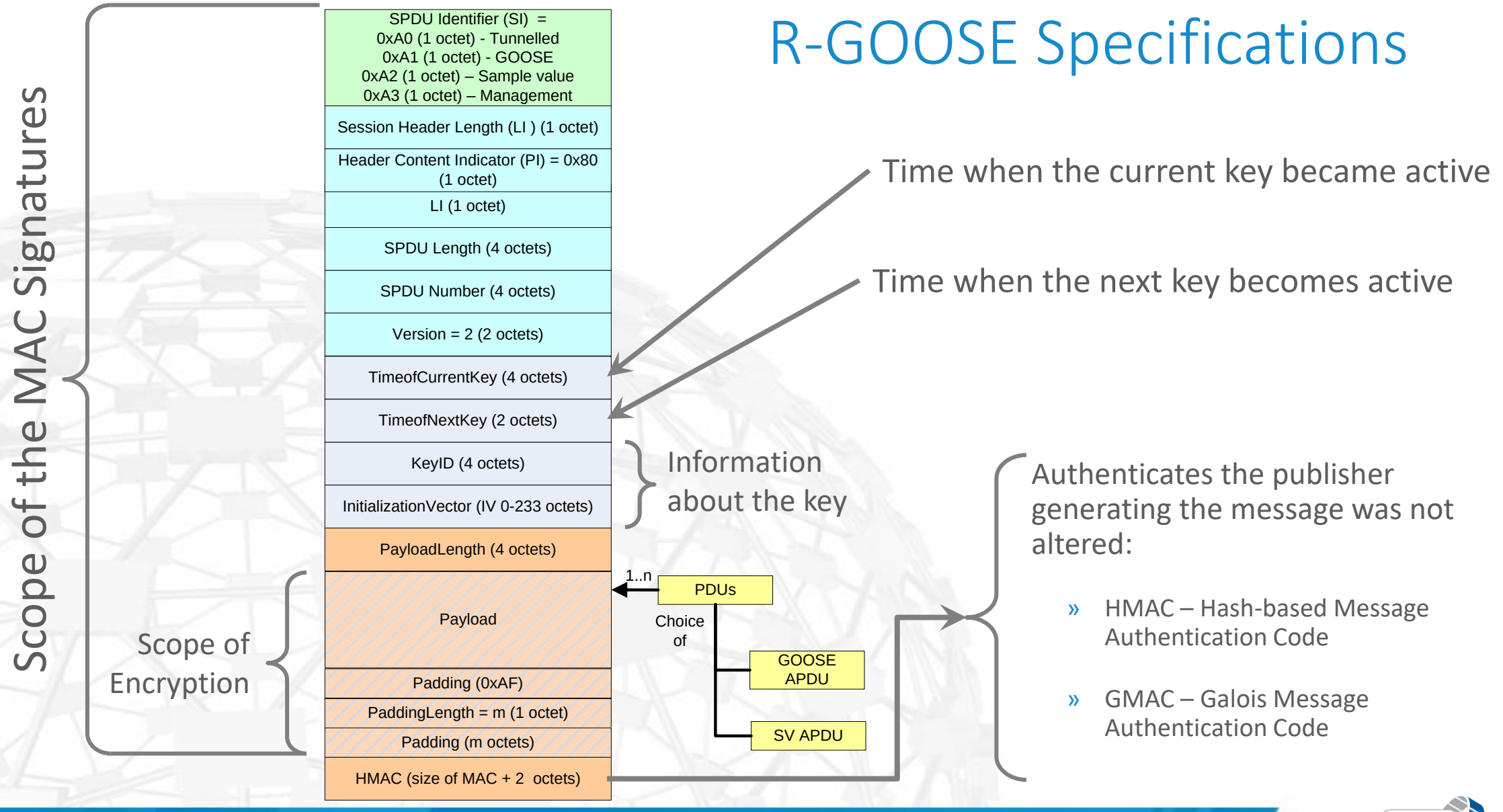
Security for R-GOOSE

- GDOI Client obtains keys from the KDC to validate and decrypt received R-GOOSE messages
- IED uses SCEP or EST to obtain and manage certificates used to identify itself



GDOI – Group Domain of Interpretation
EST – Enrollment over Secure Transport
SCEP – Simple Certificate Enrollment Protocol

R-GOOSE Specifications

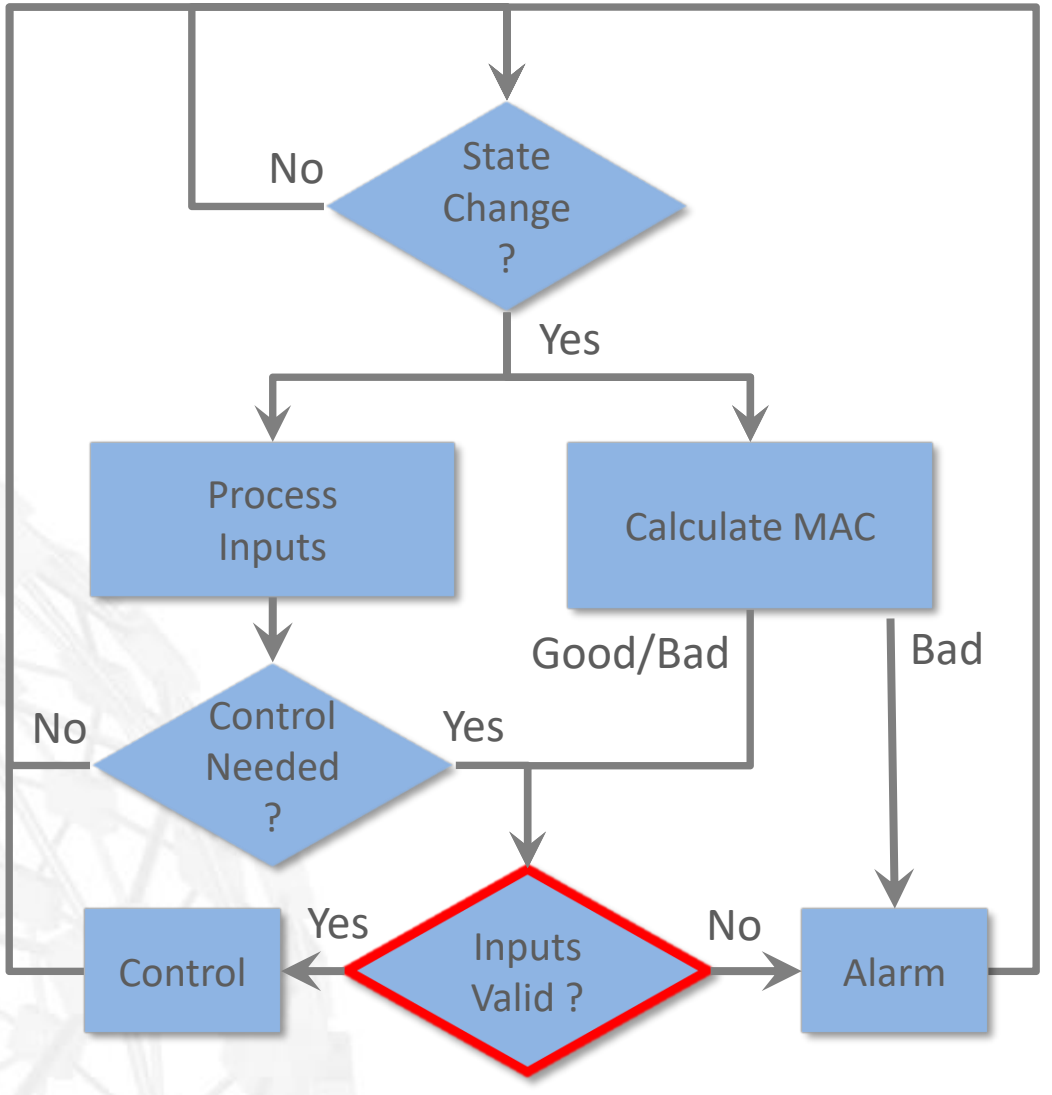


Challenge to Meet Performance

- IED Processing is relatively simpler computationally because there are fewer R-GOOSE messages to process
- RAS Controllers have many hundreds of R-GOOSE messages to process creating a computational challenge to avoid affecting performance during fault conditions
- At steady state messages that do not reflect change of state need not be validated
- When faults occur what is needed is to validate the data used to make control decisions, not necessarily all data

Validate When Needed

- Separating the signature processing from the path for decision making minimizes the latency impact on control actions
- This can be a concern when scaling up to large systems with 100s of RAS
- Eventually, universal implementation of security in hardware might alleviate this concern



What About Encryption?

- With encryption communications becomes opaque
  - » Monitoring and communications analysis (intrusion detection, etc.) is ineffective except for end points with access to the keys
- Required for use on public networks
- Typical usage is private VPN networks
- Presenter's opinion: end point encryption for protection can wait
  - » Users need to walk before running with complete end-to-end security
  - » Authenticating communications addresses many of the risks of current systems

Why Implement Security?

"There is a great interest in and capability demonstrated for messing around with the engineering that is the foundation supporting modern economic life, national security and the well being of society."

-- Vytautas Butrimas, NATO Energy Security Center of Excellence

Transforming the world of energy using open standards

Thank You

Ralph Mackiewicz
SISCO, Inc.
6605 19 1/2 Mile Road
Sterling Heights, MI 48314 USA
Tel: +1-586-254-0020 ext. 103
Mob: +1-586-260-2571
E-Mail: ralph@sisconet.com
URL: https://www.sisconet.com