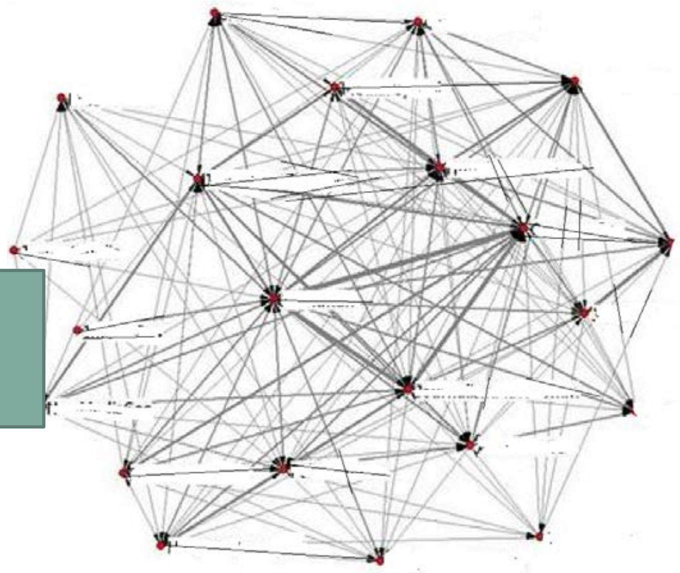
The State of Cyber Security in US Utilities

MARK ADAMIAK – PRINCIPAL

ADAMIAK CONSULTING LLC

General US Utility Communications

Jump Box
(e.g. Citrix)



Utility Enterprise Network

- Generally Firewalled
- External Access
- Multiple Attacks
  - 4000/mo - PJM

Provides Engineering Access for Settings and Data Acquisition

Utility Operations Network

- Non-routable IP Addresses
- Firewalled Access
- May be air-gapped
- Cryptographic Acceleration available in some HW
- Role-Based Access Control Available
  - RADIUS & Token
  - Adoption rate varies

Migration to Secure Transfer Mechanisms

Trusted Platform Module (TPM)

Password Management Systems

Secure FTP (SFTP)

Secure Shell (SSH)

Virtual Private Network (VPN)

Secure MMS (IEC 61850) via TLS

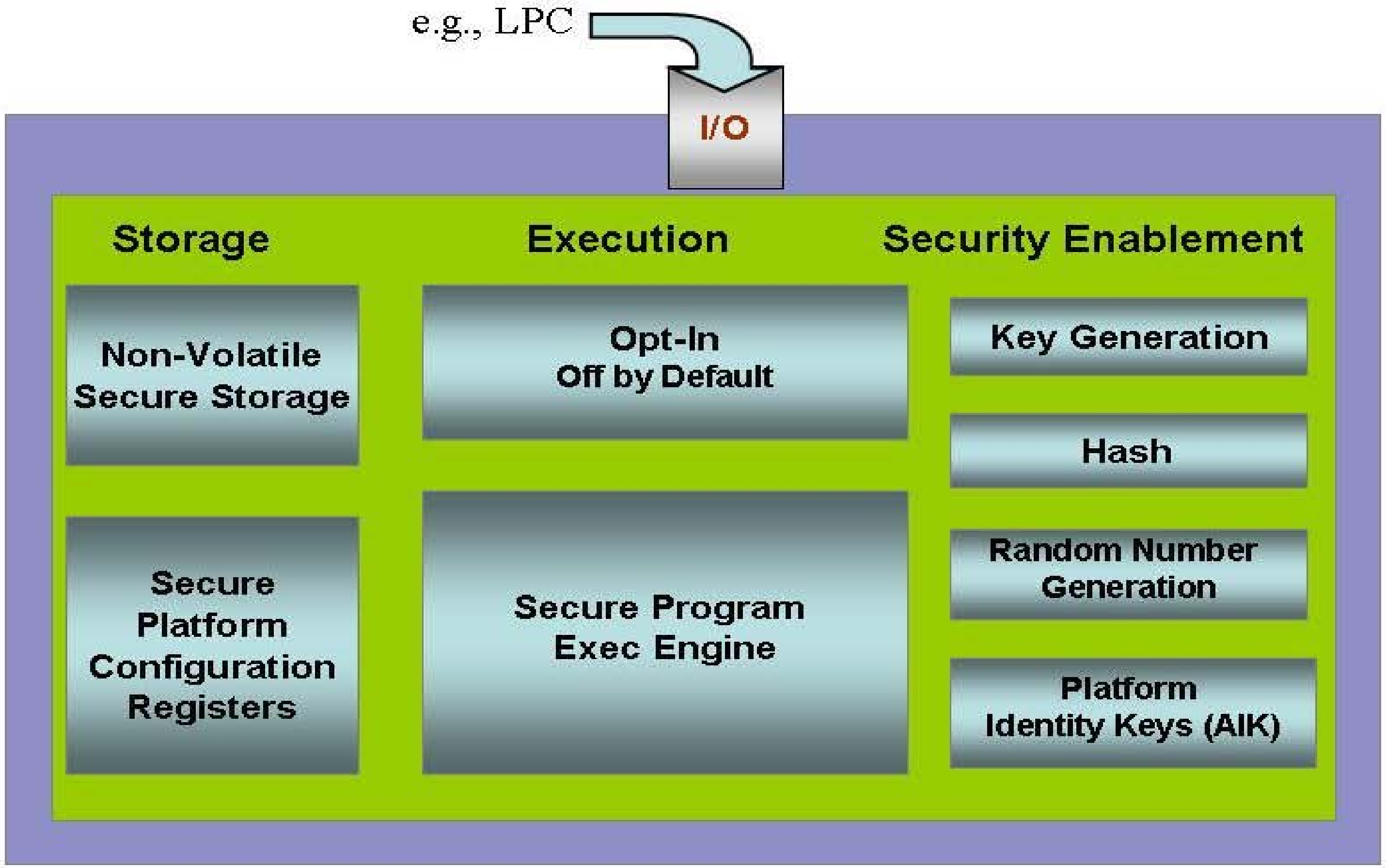
Secure Software Download

Secure PUSH mechanisms (R-SYNC)

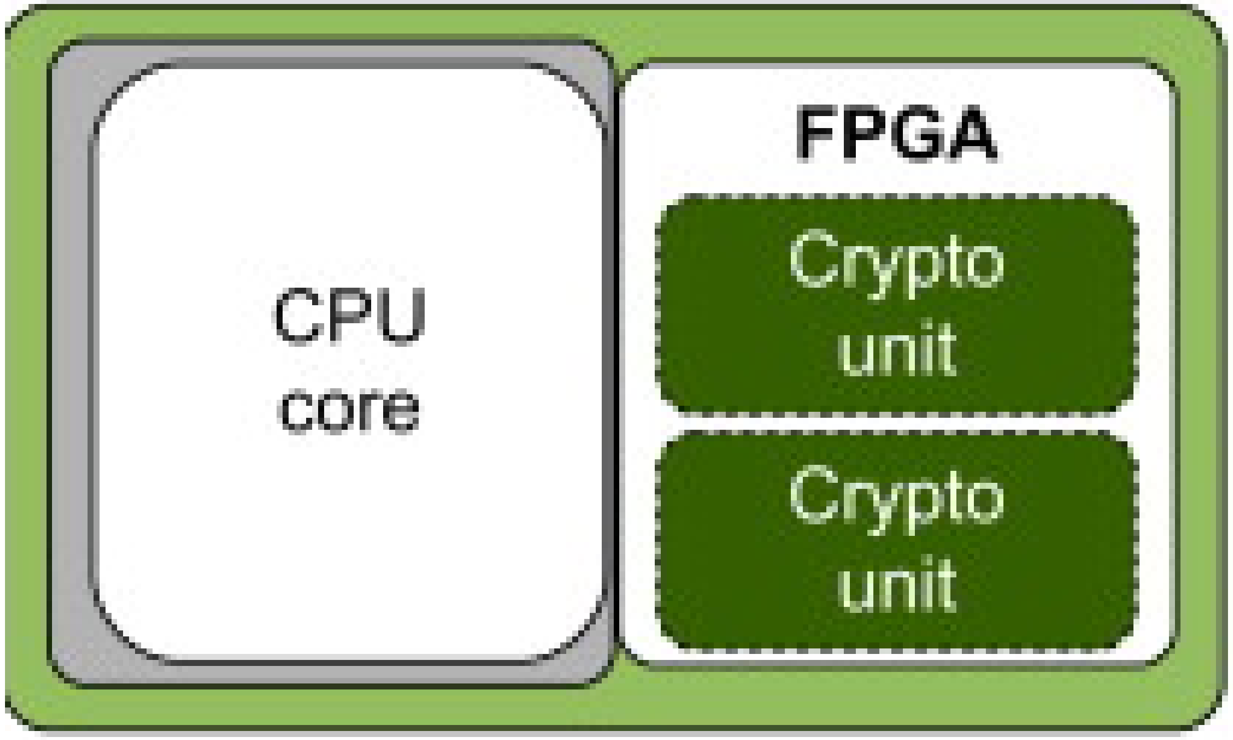
SYSLOG

Ver 1 – UDP based – no retries
Ver 2 – secure with TCP

Trusted Platform Module - TPM

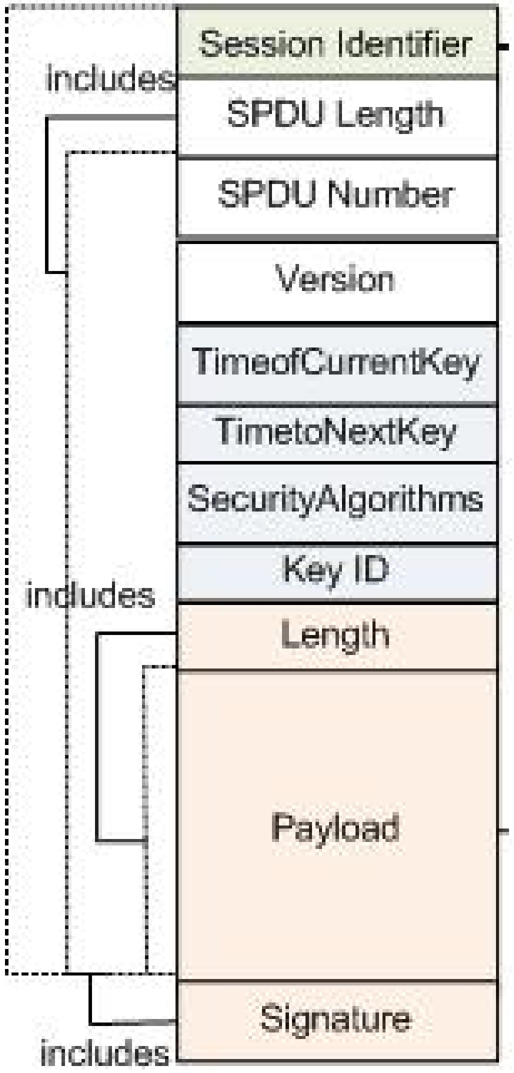

e.g., LPC
I/O
Storage
Execution
Security Enablement
Non-Volatile Secure Storage
Secure Platform Configuration Registers
Opt-In Off by Default
Secure Program Exec Engine
Key Generation
Hash
Random Number Generation
Platform Identity Keys (AIK)

CPUs available with Cryptographic Accelerators



Routable GOOSE Data Model

- Symmetric Keying
- Key Distribution via RFC6407 – Group Domain of Interpretation (GDOI)
- Certificate Based Group Membership
- Authentication via SHA256
- Encryption via AES-128



Detail Format

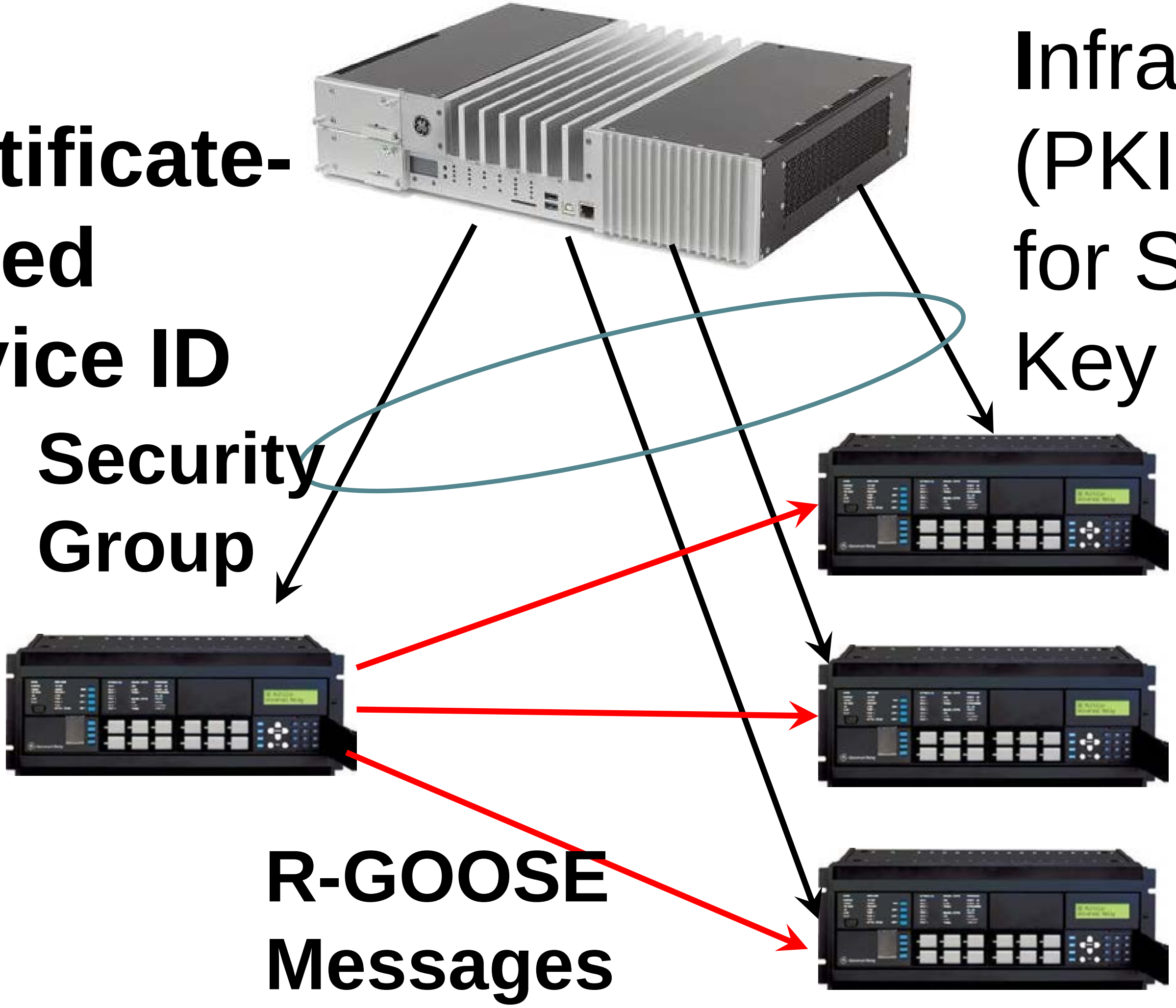
SPDU: Session Protocol Data Unit

Information for Key Exchange

Optionally Encrypted – AES128

Secure Hash Algorithm – SHA256

Architecture with Key Distribution Center (KDC)



KDC

Certificate-based Device ID

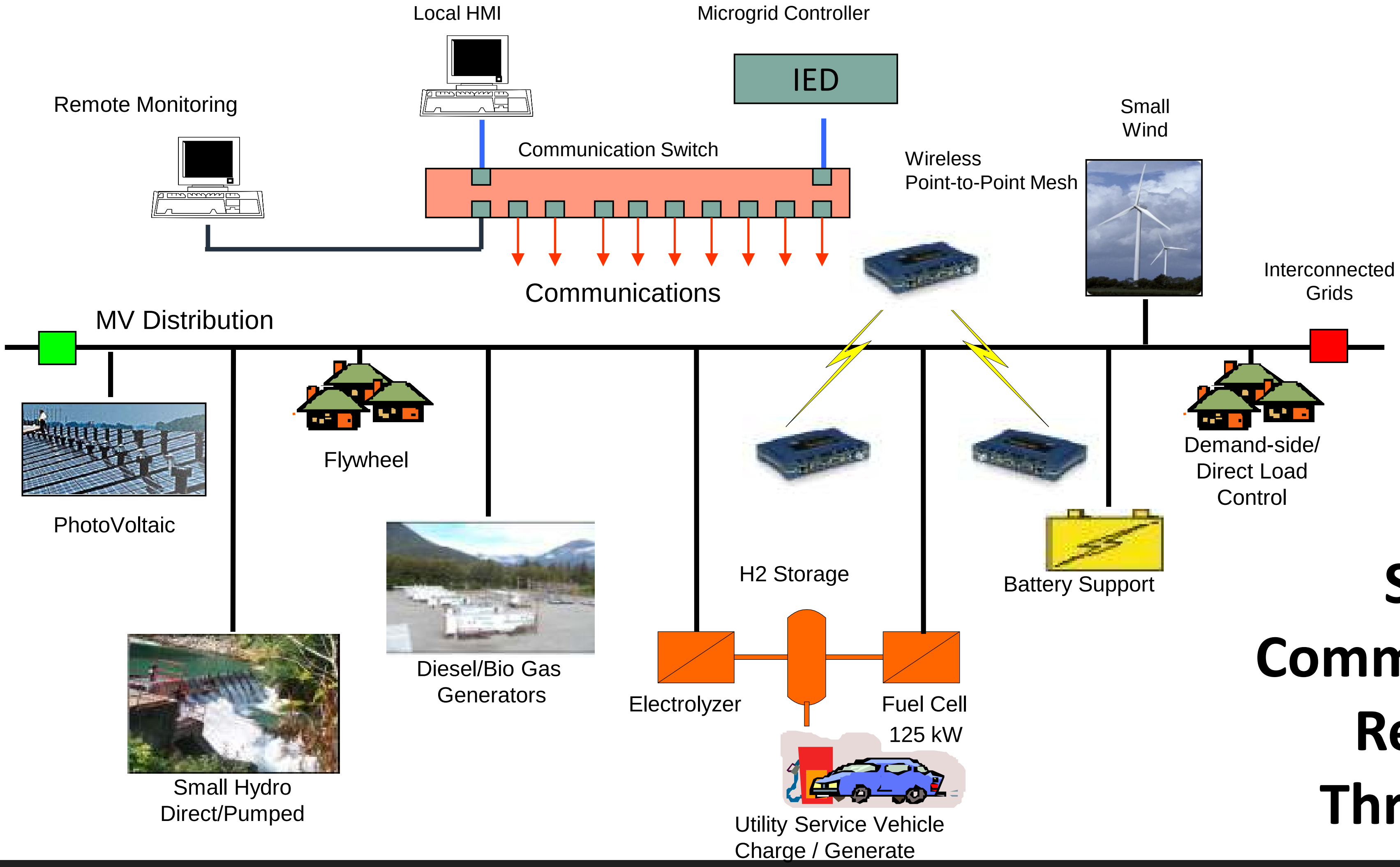
Public **K**ey **I**nfrastructure (PKI) via GDOI for Symmetric Key Exchange

Security Group

One-to-Many Multicast

R-GOOSE Messages

Future Application: MicroGrids



Secure Communications Required Throughout