Introducing Garibaldi: Security Management for IEC 61850 and DNP3

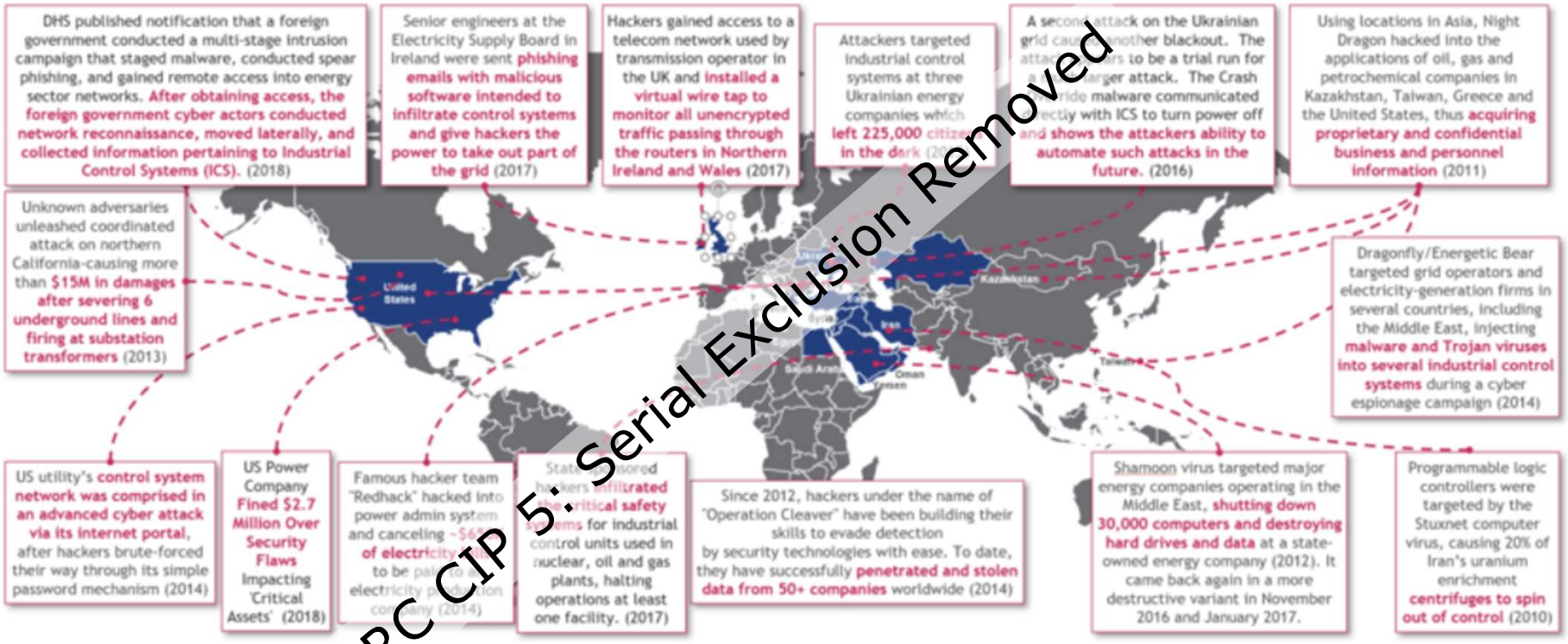
Key Distribution and System Management System

TRIANGLE MICROWORKS, INC.
SOLUTIONS FOR COMMUNICATION PROTOCOL DEVELOPMENT

PCItek

2020-01-26

Security Matters: Increasing Threats and Fines



NERC CIP 5: Serial Exclusion Removed

Sample of energy-related cyber attacks around the world over the past 10 years

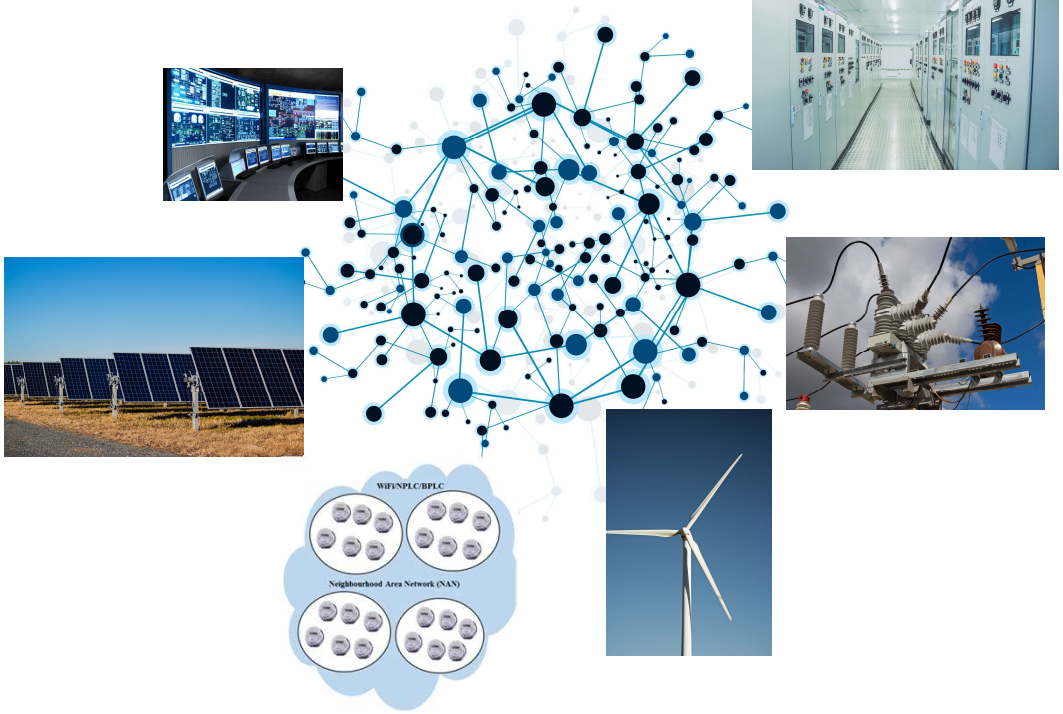
Image: BCG. Source: press reports and BCG analysis

TRIANGLE MICROWORKS, INC.
SOLUTIONS FOR COMMUNICATION PROTOCOL DEVELOPMENT

PCItek

Personal cyber security is hard enough

Utility security manages millions



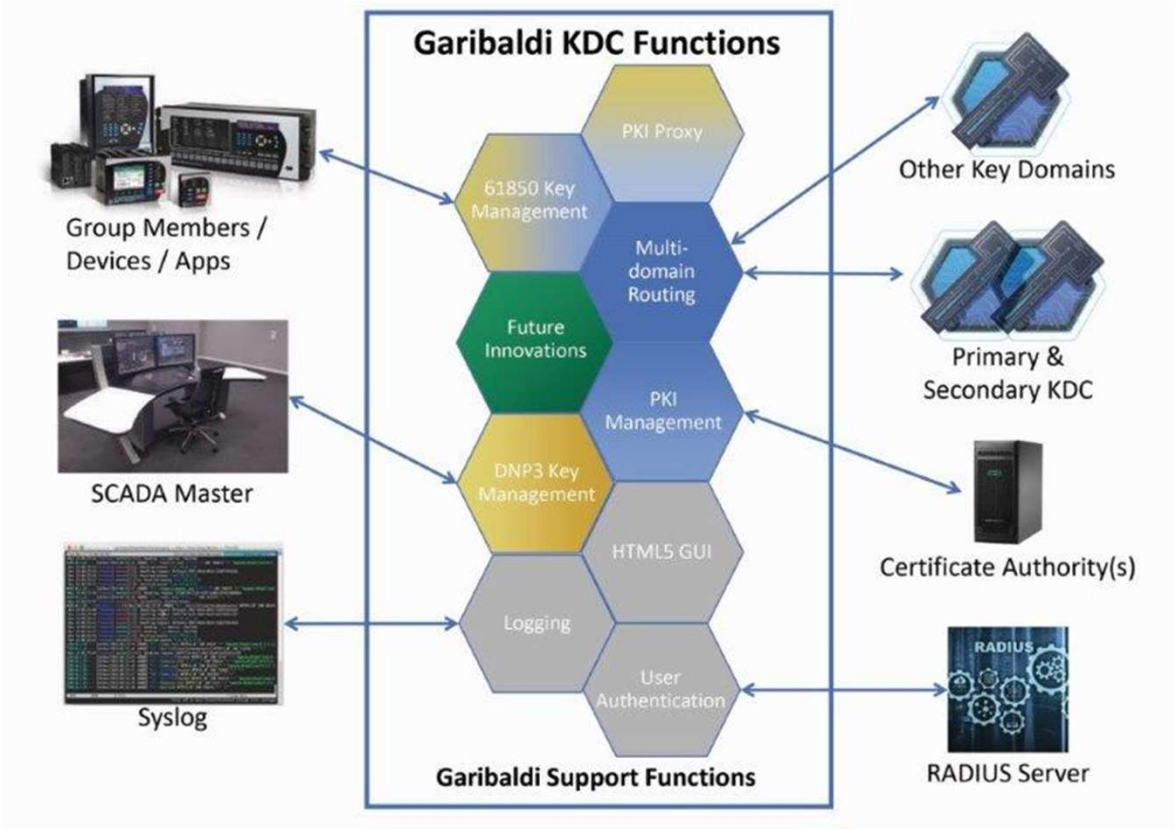
TRIANGLE MICROWORKS, INC.
SOLUTIONS FOR COMMUNICATION PROTOCOL DEVELOPMENT

PCItek

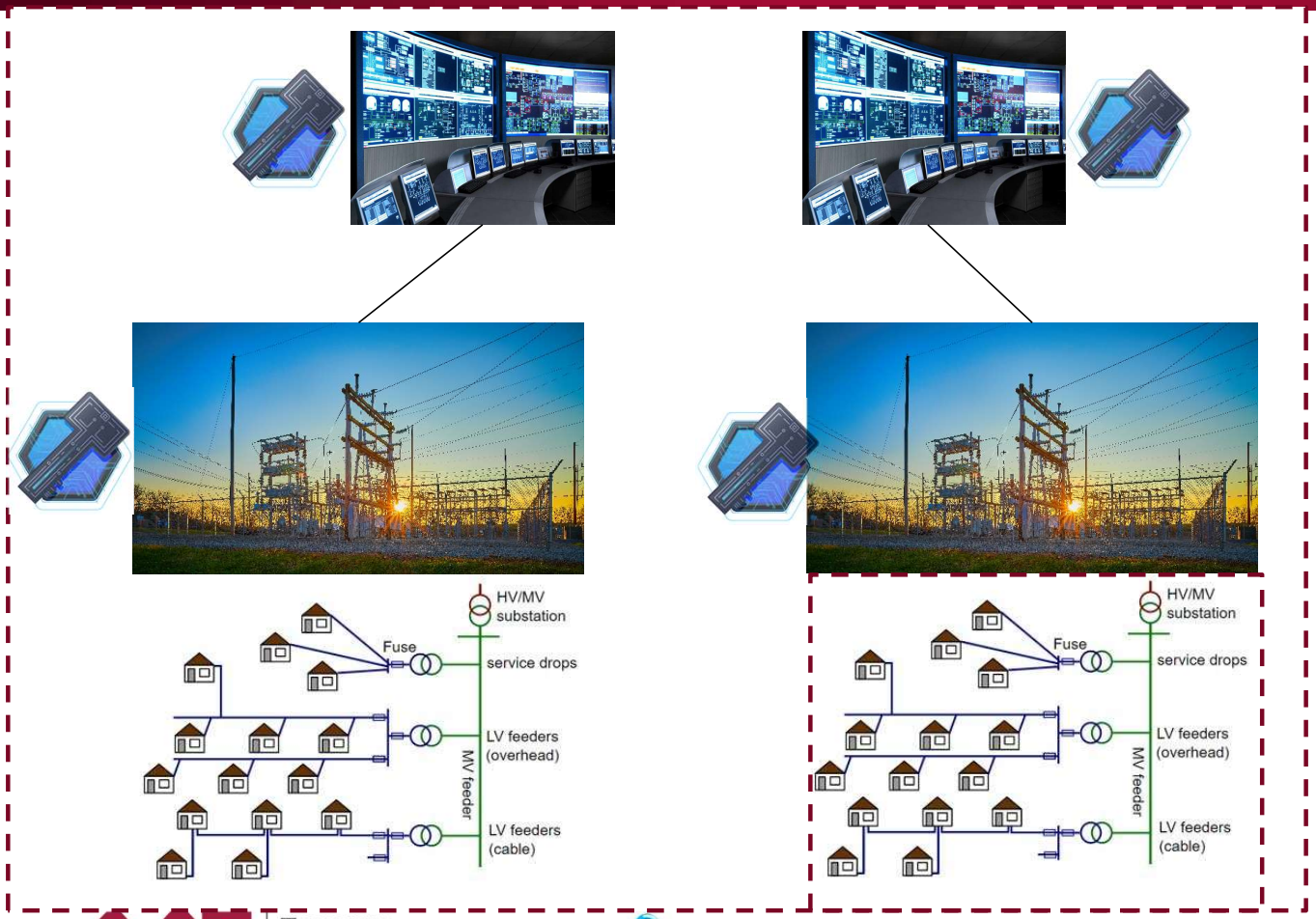
Garibaldi Solves major part of the problem

- Manages large numbers of multicast group's key and policy distribution.
- Manages system enrollment allowing revocation
- Manages access control for DNP3 SAv6
- Operates in centralized or de-centralized environments.
- Part of PCItek's Cyber Enterprise N-tier Administrative Resilient Infrastructure (CENtARI™) Product Suite.

Introducing Garibaldi: Key Distribution and Access Control



Garibaldi and Security Domains



Concept allows deployments:

- Centralized
- Decentralized (Mesh)

Determining the correct amount of resiliency and standalone security Requirements is key.

Security Addressed by IEC 61850 and DNP3 Security

Security Functions	IEC 61850		IEEE 1815 (DNP3)	
	Messages	Policy	Messages	Policy
Authentication of peers communicating with each other	GOOSE/SV	Garibaldi	SAv6	Manual
Prevention of message tampering	GOOSE/SV	Garibaldi	SAv6	Manual
Confidentiality (e.g. encryption)	GOOSE/SV	Garibaldi	SAv6	Manual
System membership*	GOOSE/SV	Garibaldi	AMP	Garibaldi
Determining rights of usage*	SCL	Garibaldi	AMP	Garibaldi
Revocation of Membership or Rights*		Garibaldi	AMP	Garibaldi

* - Needed to help prevent incidents like Ukraine

Capabilities (continued)

- IEC 61850 key and policy distribution for GOOSE,R-GOOSE, SV, and R-SV via:
  - Pull, Push, and multicast push.
  - Individual keys generated per DataStream (increases security)
  - Distribution and management per IEC 62351-9

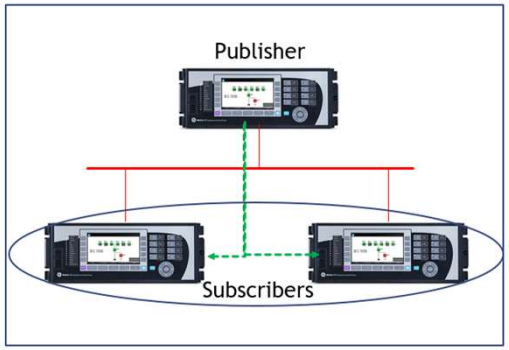
- DNP3 Management per Authority Management Protocol (AMP*) for DNP3 SAv6.

* Specification anticipated to be completed 2nd Qtr 2020. IOP anticipated 4th Qtr 2020.

Member Validation and Policy Delivery

Membership

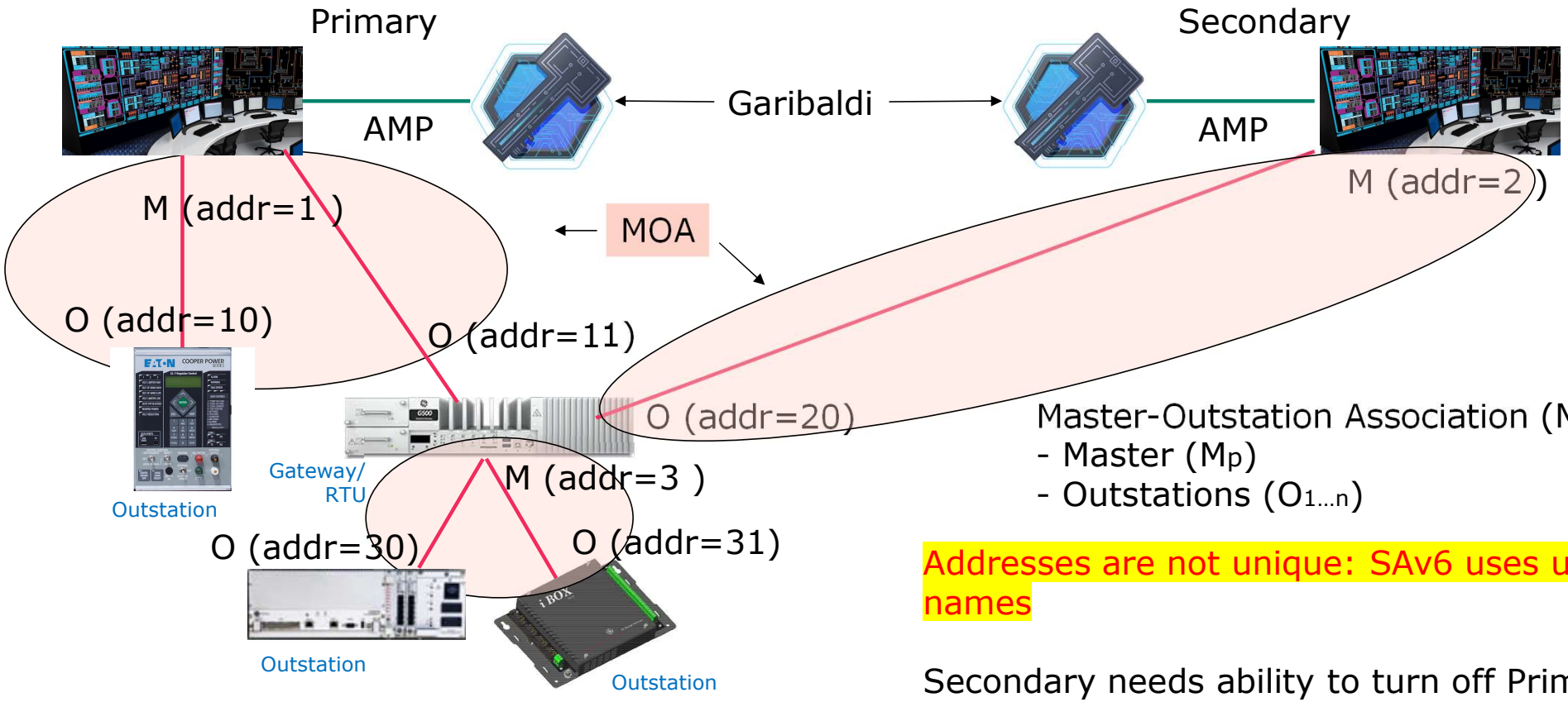
- Determined by SCL
- Manual Entry
- Digital Certificates



Policy Distribution

- Delivery typically 24 hours:
  - PULL
  - PUSH
  - Multicast PUSH
  - Key Delivery Assurance (KDA)
- Delivers:
  - Group Keys
  - Encryption Algorithm
  - Authentication/MAC Algorithm

DNP3 SAv6/AMP: Attacking the difficult issues



Master-Outstation Association (MOA)
- Master (M_p)
- Outstations ($O_{1...n}$)

Addresses are not unique: SAv6 uses unique names

Secondary needs ability to turn off Primary communications (prevent Ukraine)

TRIANGLE MICROWORKS, INC.
SOLUTIONS FOR COMMUNICATION PROTOCOL DEVELOPMENT

PCItek

AMP and Garibaldi

- Can revoke rights previously given to peers of a MOA

  This will allow compromised devices/applications to be removed from the system.

- Cannot grant rights to devices/applications that are not supposed to be part of the system.