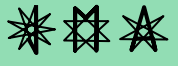
Security for the Electrical Power Grid

John M. Acken, Robert Bass, and Sonali Fernando
Portland State University

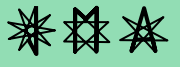
Presented at EDPS on 4 November 2021

This research supported by the Department of Energy Grant DE-OE0000922 titled: "Development of an Energy Services Interface for the EGoT".



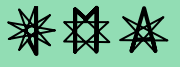
Security for the Electrical Power Grid

- Efficient Power Distribution
- Critical infrastructure Sectors
- Energy Grid of Things
- Communication Security
- Security for Prevention
- Monitoring for Unexpected Security Attacks
- Trust and Security
- Response to Attacks
- Summary

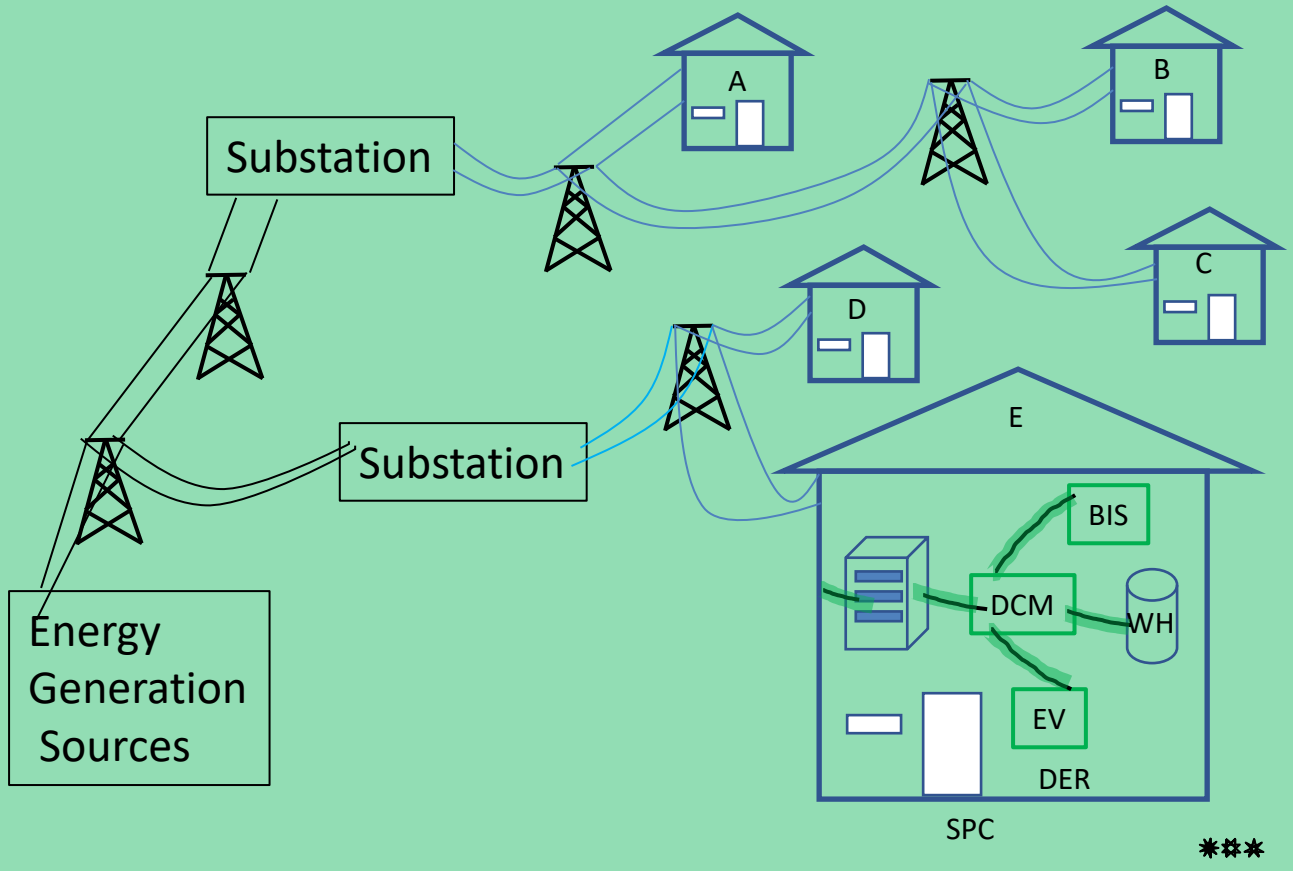


Efficient Power Distribution

- Traditional Power Grid
  - All centralized, deterministic energy providers
  - Fixed Distribution to Energy Consumers
  - Energy Providers offer services to consumers
- Distributed Resource views
  - Many Distributed, Stochastic Energy Providers
  - Bidirectional distribution between providers and consumers
  - Consumers and Providers offer service to each other
- Allows Demand – Resource Flexibility
- Provider and Customer Economic benefits

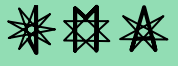


Power Distribution Example



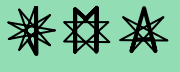
Security for the Electrical Power Grid

- Efficient Power Distribution
- **Critical infrastructure Sectors**
- Energy Grid of Things
- Communication Security
- Security for Prevention
- Monitoring for Unexpected Security Attacks
- Trust and Security
- Response to Attacks
- Summary



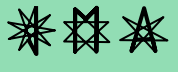
Cybersecurity & Infrastructure Security Agency

- https://www.cisa.gov/critical-infrastructure-sectors
- 16 Critical infrastructure sectors
- Internet in Communication sector plus Information Technology Sector
- Energy Sector
- EGoT is at the intersection of these sectors



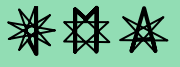
Security for the Electrical Power Grid

- Efficient Power Distribution
- Critical infrastructure Sectors
- **Energy Grid of Things**
- Communication Security
- Security for Prevention
- Monitoring for Unexpected Security Attacks
- Trust and Security
- Response to Attacks
- Summary

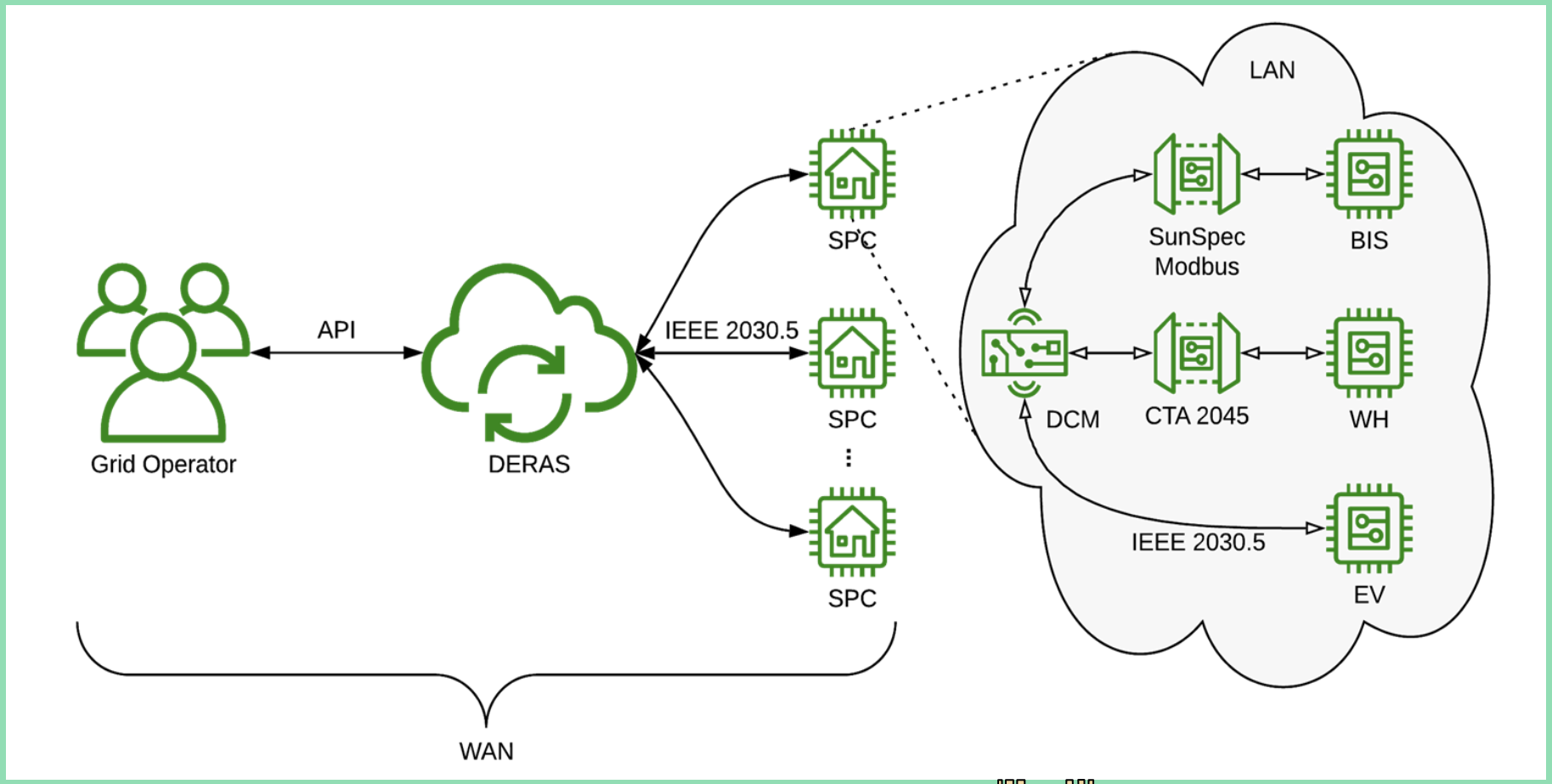


Energy Grid of Things Acronyms

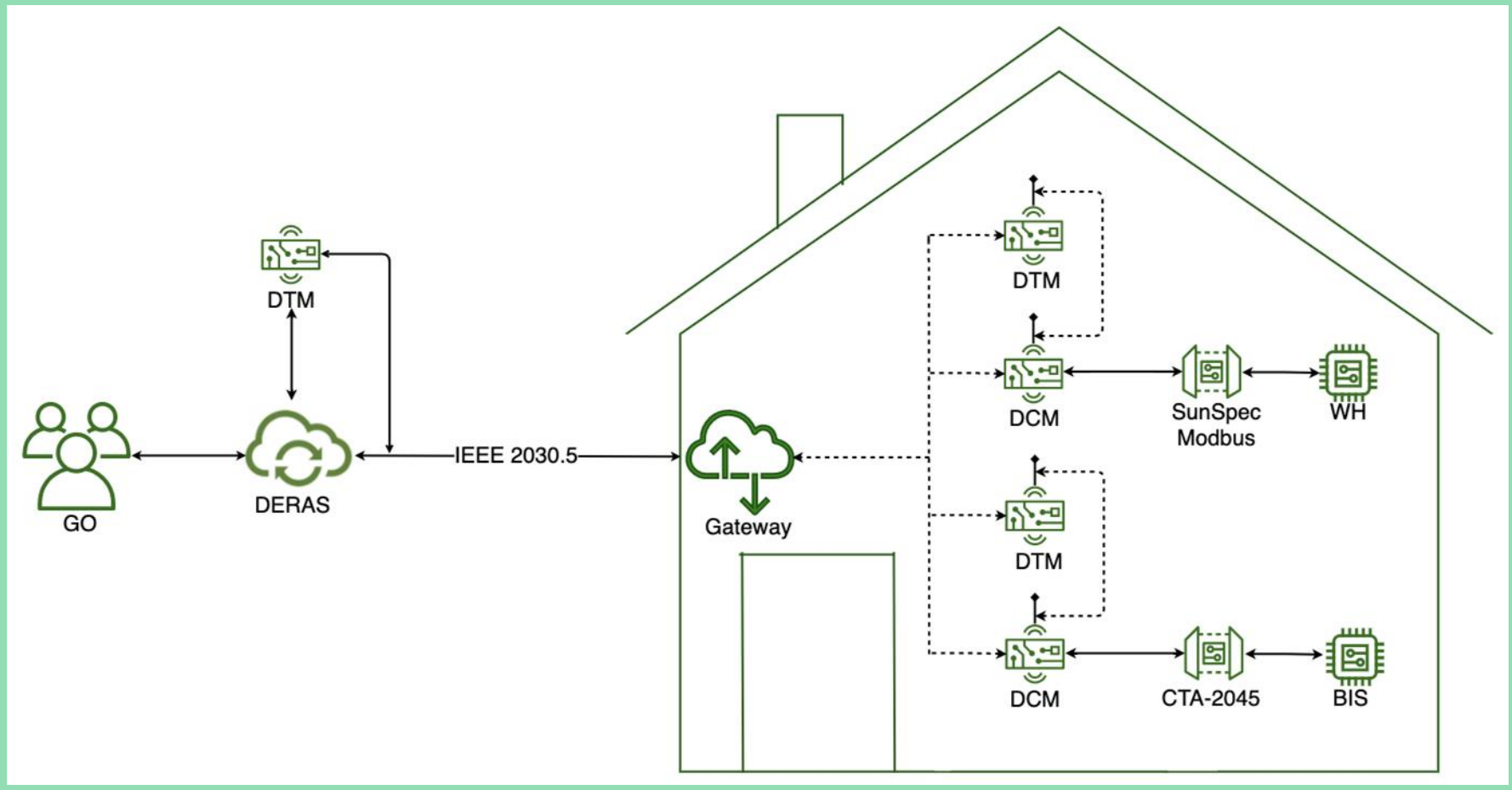
- GO: Grid Operator
- GSP: Grid Service Provider
- EGoT: Energy Grid of Things
- DERAS: Distributed Energy Resources Aggregator System
- CDTA: Central Distributed Trust Aggregator
- SPC :Service Provisioning Customer
- DCM: Distributed Control Module for DERAS
- DTMC: Distributed Trust Model at Client
- DER: Distributed Energy Resources
- EV: Electric Vehicle



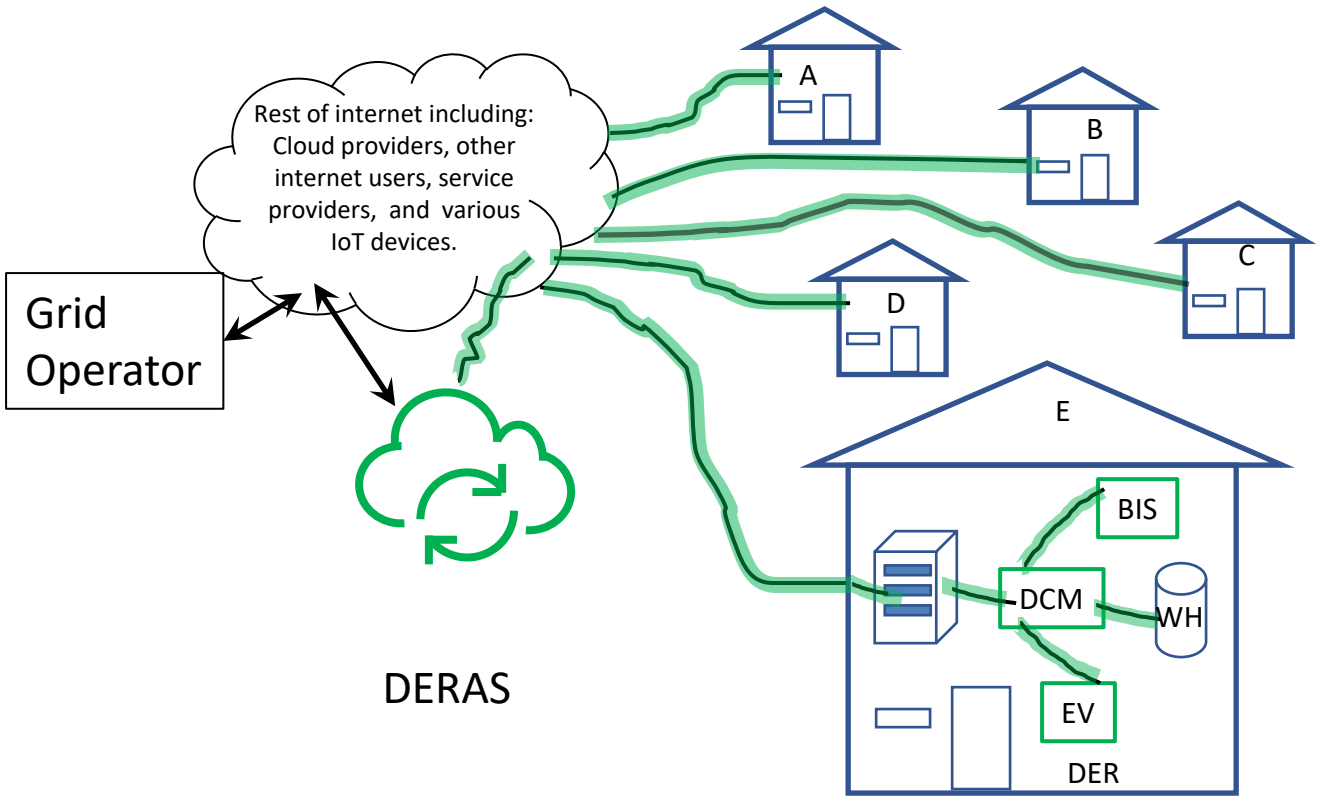
Overall Energy Grid of Things



Customer view of Energy Grid of Things

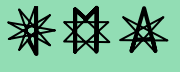


Internet Communication for Energy Grid of Things



Security for the Electrical Power Grid

- Efficient Power Distribution
- Critical infrastructure Sectors
- Energy Grid of Things
- **Communication Security**
- Security for Prevention
- Monitoring for Unexpected Security Attacks
- Trust and Security
- Response to Attacks
- Summary



Information Security

Information Security Triad:

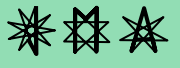
- Confidentiality
- Integrity
- Availability

==========

- Access Control
- Non-Repudiation

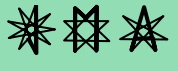
Example Attacks

- Eavesdropping
- Imposter (circumvent authentication)
- Password attacks (circumvent authentication)
- Denial of service
- Man in the middle
- Phishing



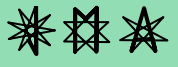
Energy Services Interface Security

- Protect the information
- Observe information flow for anomalies
- Act or respond to anomalies
- Diagnoses or identify causes of anomalies
- Make necessary modifications to system
- Standardize communication between the service provider and the client



Security for the Electrical Power Grid

- Efficient Power Distribution
- Critical infrastructure Sectors
- Energy Grid of Things
- Communication Security
- **Security for Prevention**
- Monitoring for Unexpected Security Attacks
- Trust and Security
- Response to Attacks
- Summary



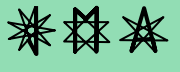
Authentication for Access

Multifactor Authentication

- Information (password) = what you know.
- Physical items (key) = what you have.
- Biometrics (fingerprints) = what you are.
- Location (GPS) = where you are.

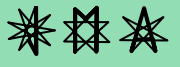
==========

- Certificates



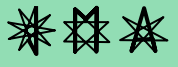
Information Protection

- Encryption
- Secure Hashing
- Access Control
- HTTPS
- Standard for Smart Energy Profile Protocol
  IEEE 2030.5

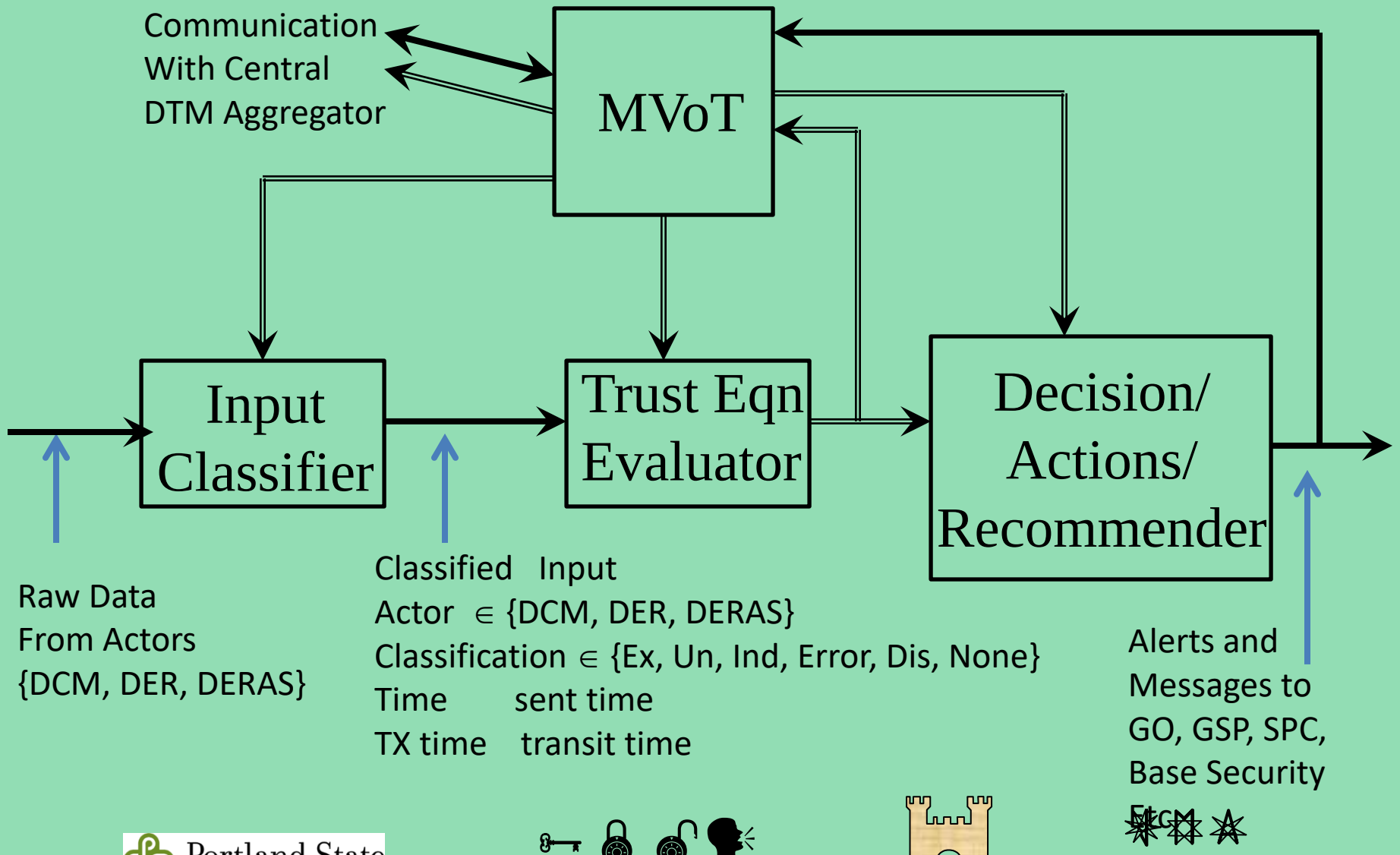


Security for the Electrical Power Grid

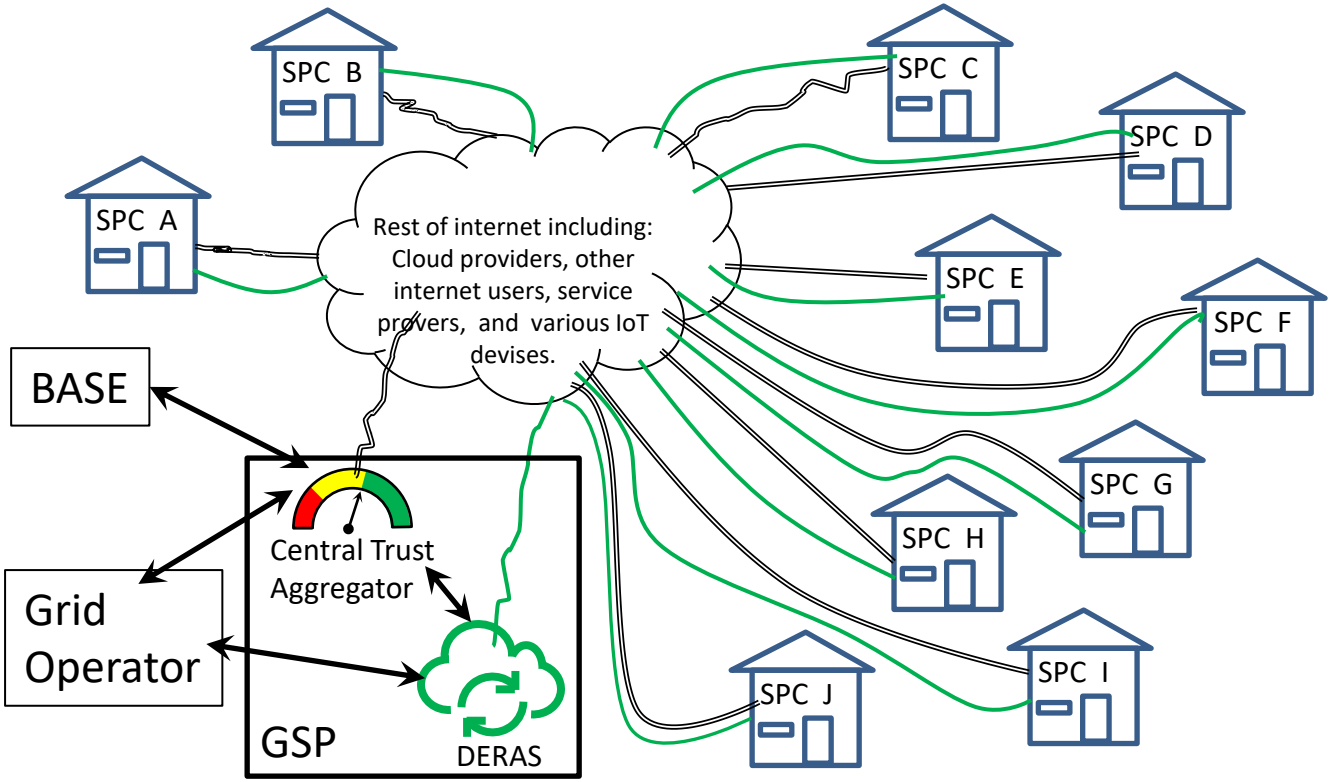
- Efficient Power Distribution
- Critical infrastructure Sectors
- Energy Grid of Things
- Communication Security
- Security for Prevention
- **Monitoring for Unexpected Security Attacks**
- Trust and Security
- Response to Attacks
- Summary



Monitoring for Unexpected Security Attacks

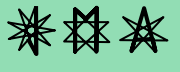


Energy Grid of Things Monitoring System



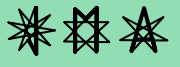
Security for the Electrical Power Grid

- Efficient Power Distribution
- Critical infrastructure Sectors
- Energy Grid of Things
- Communication Security
- Security for Prevention
- Monitoring for Unexpected Security Attacks
- **Trust and Security**
- Response to Attacks
- Summary



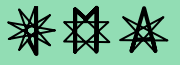
Trust as it relates to Security

- Depends upon History
- Depends upon relationship
- Depends upon value received
- Depends upon potential loss



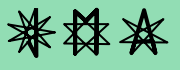
Security for the Electrical Power Grid

- Efficient Power Distribution
- Critical infrastructure Sectors
- Energy Grid of Things
- Communication Security
- Security for Prevention
- Monitoring for Unexpected Security Attacks
- Trust and Security
- **Response to Attacks**
- Summary



Responses and Actions

- Alarms
- False Alarms
- Relative weight TP, TN, FP, FN
- Thresholds for Alerts
- Decisions for Operational Changes
  - Turn off
  - Block
  - Charges / fines



Summary

- Smart Power Grid is critical Infrastructure
- Information Security central for EGoT
- Security Protection for known attacks
- Information Monitoring for Anomalies
- Trust Evaluation for Security monitoring

- Portland State University research funded by DOE to address Security for the Smart Grid.