IETF IoT frameworks and standards for secure communication at the 'energy edge'

Craig Rodine

Affiliation: Sandia National Laboratories
Department of Electric Grid Security and Communications

IETF 123
T2TRG, Monday 21 July 2025

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc. for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Outline

- ➢ Context and problem statement
- ➢ A strategic intervention
- ➢ Use case: Self-Healing Adaptive Resilient Power Systems
- ➢ Discussion

Context and problem statement

- Power distribution system engineers distrust communications
  - Focused (naturally) on safety, with deep cultural commitments.
  - Objections: comms is/are slow, unreliable, vulnerable, expensive, ‘exotic’.
- Protection schemes rely on ‘local measurements’ (V, I, f, ϕ)
  - End devices (e.g. relays) are self-contained and self-reliant.
  - They run algorithms over sensed data, may change device settings.
  - System stability is engineered via modeling, adjusting algos (not OTA).
- Problem statement
  - Deep skepticism towards digital communications is limiting what power systems designers can achieve.
  - Situation complicated by the inclusion of solar, storage, microgrids, etc.

A strategic intervention

- Introduce “just enough communications” in a promising use case.
- Satisfy all requirements (low cost, adequate performance, secure, sufficiently reliable, scalable).
- If possible, build on open standards and FOSS implementations.
- Demonstrate viability via co-simulation and lab/field prototypes.
- Strategic goals:
  - ➢ Raise power systems community confidence in practical, scalable communication-based control.
  - ➢ Apply and build on established IoT frameworks and standards.

Use case: Self-Healing Adaptive Resilient Power Systems (SHARPS)

- Goal: create techniques, algorithms, [eventually] devices enabling distribution-level power systems to self-heal.
  - ‘Self-healing’: when a severe event would normally lead to a widespread outage, the power system is able automatically to:
    - ➢Re-energize all loads for which a) there is sufficient source capacity and b) an intact source-load path;
    - ➢Maintain voltage and frequency regulation (requires maintaining generation-load balance); and
    - ➢Maintain system protection.
- Outcome: provide *highly robust*, *threat-agnostic* power system resilience.

SHARPS incremental improvements

➢ Fault isolation without blacking out entire off-grid system.

➢ Isolation of faults without requiring reclosure.

➢ More automated transition into intentional island mode.

These require *device self-identification for automatic coordination.*

Meaning: automatically setting the ID number of each line relay.

Exploring two approaches:

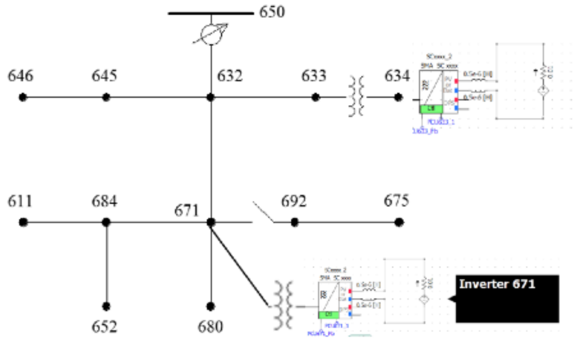
- Sequential switching ("tapping"—the Morse Code approach

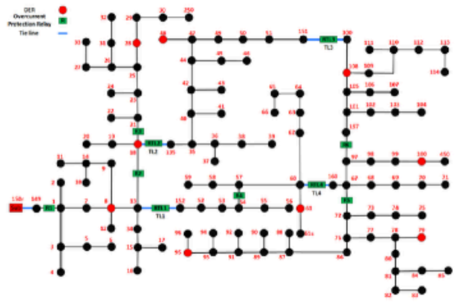
- Nearest-neighbor comms (inexpensive, non-real-time)

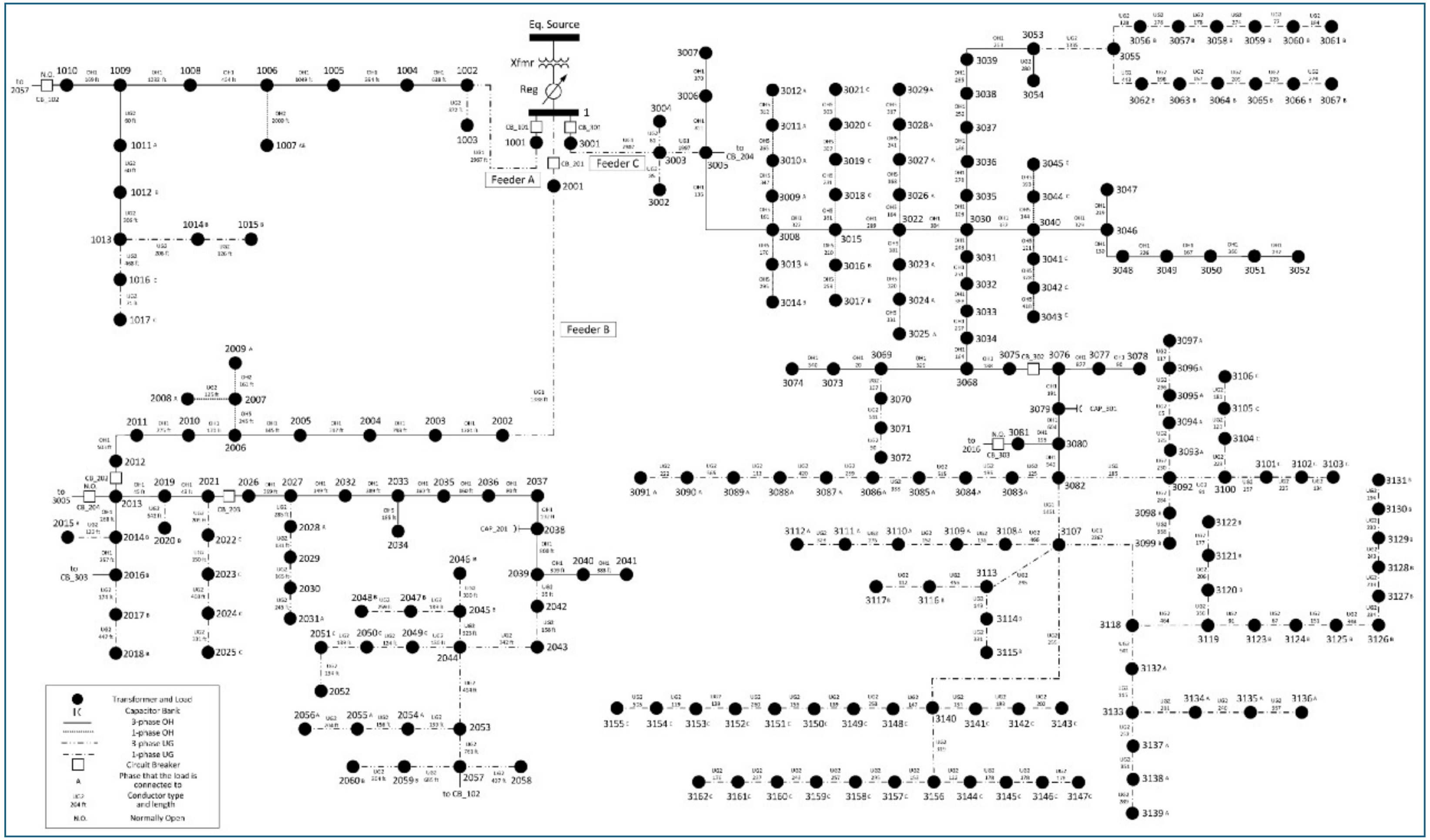
SHARPS wants SNNC (pron. “sink”)

- SNNC: Secure Nearest-Neighbor Communications
- Constrained network supporting SHARPS device self-ID
- Working hypothesis: use IEEE 802.15.4 + IETF IoT fws & stds
  - Draw on RFC 5548 (urban), RFC 5673 (industrial), more recent work
  - Coordinate with 6lo, IEEE 802.15.4, Wi-SUN
- Some challenges
  1. No-maintenance, no-touch
     - ➢Exploring energy harvesting; nickel-63 nuclear batteries
  2. RF physical design (antenna, power profile, etc.)
     - ➢Exploring work on IoT edge sensor nodes/mote SoCs
  3. Crafting L3-L7 IoT stack to meet SHARPS requirements.
     - ➢That’s why I’m here, in the main.

SHARPS system models **Iowa 240-bus distribution model**

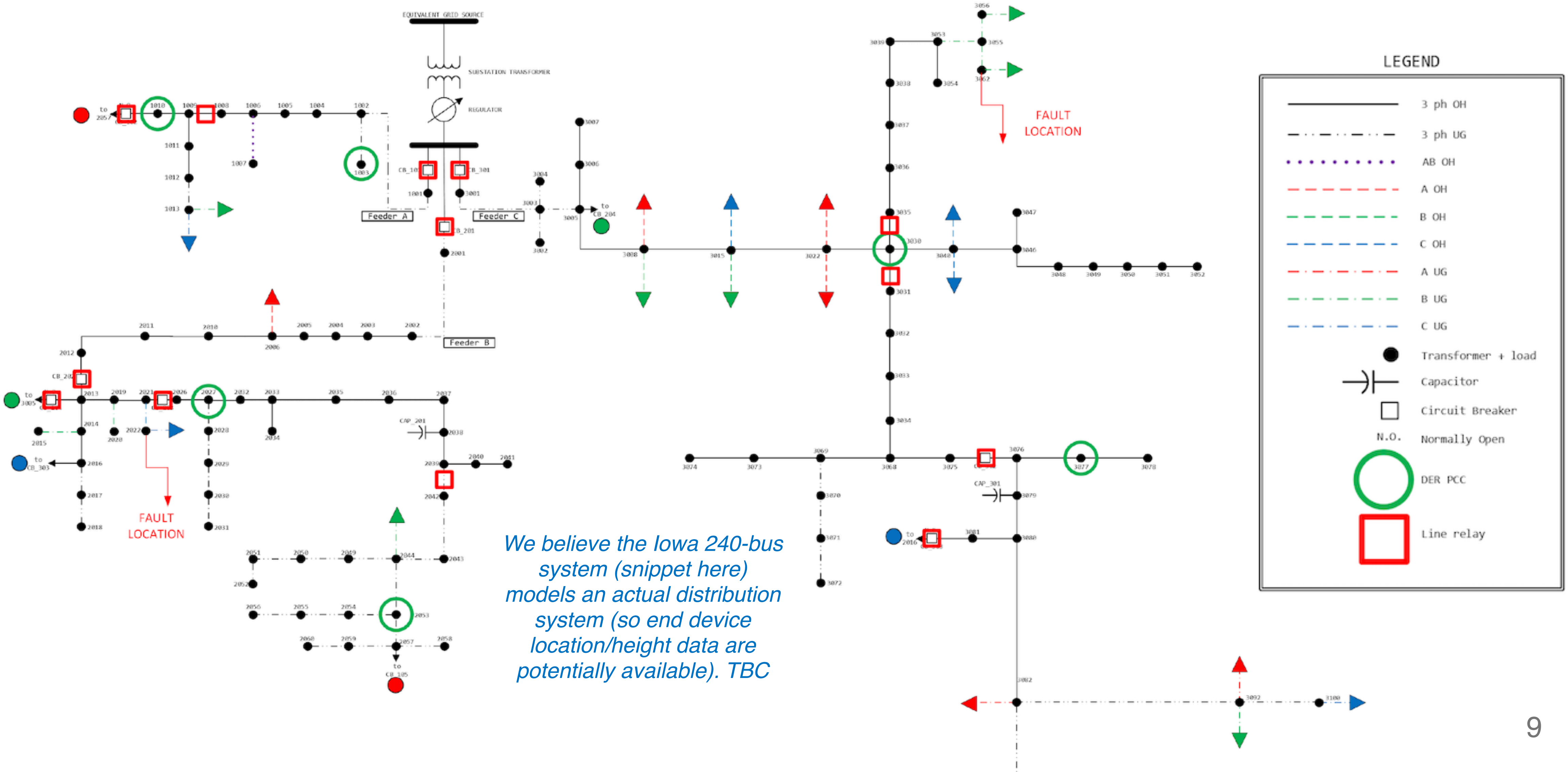






https://wzy.ece.iastate.edu/testsystem.html

SHARPS model end devices



We believe the Iowa 240-bus system (snippet here) models an actual distribution system (so end device location/height data are potentially available). TBC

IETF IoT relevance (presumably)

- IPv6, 6LoWPAN, RPL foundation for this LLN
- CoAP + CBOR for maximum on-air efficiency
- SenML + CDDL to define data types for SHARPS
- EDHOC + COSE/OSCORE for end-to-end security
- SUIT, RATS for end-device lifecycle security

Additional use cases

There are several candidates; the next one on our roadmap:

- ➢ Fault Location, Isolation, and Service Restoration (FLISR)
  - Generalizes what SHARPS is working to create.
  - Centralized and distributed flavors, both would benefit from IETF IoT.

https://ieeexplore.ieee.org/document/7016420

https://shorturl.at/sLfgd

https://selinc.com/solutions/p/flisr/

ASK (current need – thanks in advance!)

Experience with or recommendations for ITEF IoT/CN simulation? papers, tools, or approaches?

Summary Table

Parameter	NS-3	OMNeT++	NetSim	CupCarbon	Matlab/Simulink	GNS3
Supported Protocols	LoRaWAN, Zigbee, 6LoWPAN, RPL, MQTT, Wi-Fi, Bluetooth	LoRaWAN, Zigbee, 6LoWPAN, RPL, MQTT, CoAP, Wi-Fi	Zigbee, 6LoWPAN, LoRaWAN, Sigfox, Wi-SUN, MQTT, CoAP	LoRa, Zigbee, 6LoWPAN, Sigfox, Wi-Fi	Zigbee, LoRa, Wi-Fi, Bluetooth	Zigbee, LoRaWAN, Bluetooth, Ethernet, Wi-Fi
Scalability	High	High	Medium	Medium	High	Medium
Ease of Use	Medium	Medium	High	High	High	High
Visualization	NetAnim, PyViz	GUI-based	Built-in tools	2D/3D visualization	Plotting tools	Topology visualization
Extensibility	High	High	Medium	Medium	High	Medium
Platforms	Windows, macOS, Linux	Windows, macOS, Linux	Windows	Windows, macOS, Linux	Windows, macOS, Linux	Windows, macOS, Linux
Best For	Protocol testing, large-scale networks	Custom protocols, routing	IoT protocol performance analysis	Smart city networks	Prototyping and signal processing	Testing network topologies

Discussion

Thank you for your kind consideration!

c.rodine@ieee.org