Enhancing DER Integration with OpenFMB

Key Observations:
1. Single-Purpose Functions
2. Proprietary & Silo’ed systems
3. Latent, Error-prone Data
4. OT/IT/Telecom Disconnected
5. No Field Interoperability!

Vendor A Solution
- Private Carrier
- Head End A

Vendor B Solution
- Proprietary Network
- Head End B

Vendor C Solution
- Public Carrier
- Head End C

Utility Central Office

Key Observations:
1. Multi-Purpose Functions
2. Modular & Scalable HW&SW
3. End-to-End Situational Awareness
4. OT/IT/Telecom Convergence
5. True Field Interoperability!

3G, LTE, Wi-Fi, Fiber, Ethernet, RF ISM, or PLC

Node

Field Message Bus
Any Medium

Copyright © 2016 Duke Energy All rights reserved.
Open Field Message Bus (OpenFMB) Framework

End Points Devices
- Smart Meter
- Line Sensor
- Capacitor Bank
- Solar PV Inverter

Lower Tiers Nodes (e.g. grid)
- Legacy Protocol Adapter
- Common Data Model Profile(s)
- OpenFMB protocol

Middle Tier Nodes (e.g. substation)
- Legacy Protocol Adapter
- Common Data Model Profile(s)
- OpenFMB protocol

Higher Tier Node
Central Office
(Utility Datacenter)
- MDM
- GIS
- DMS
- OMS

Legend
- Legacy Protocol Translation
- Common Semantic Model
- Open FMB IoT Protocol
- Client/Server Polling
- Pub/Sub Messaging

Virtual Firewall

Firewall

Open Field Message Bus (OpenFMB) Framework

Copyright © 2016 Duke Energy  All rights reserved.
OpenFMB Operation: Federated Deterministic Exchanges

- Periodic Readings - Pub every few seconds or near-real-time
- Data-Driven Events – on status change in near-real-time

Readings
KW A/B/C
KVAR A/B/C
V A/B/C
I A/B/C
Phase Angle A/B/C
KWh
TimeStamp
State of Charge

Status, Events, Alarms, & Control
Trip / Close
TimeStamp

Grid Edge Analytics

PV
Battery
Security/SDN Policy Manager

Open Field Message Bus

Recloser / Switch
Meter
Microgrid Optimizer
OpenFMB Framework Life Cycle

- Functional and non-functional requirements
- Interaction and sequencing

- Profile of applicable, existing data model

- Common software definitions and language

- Software tools to allow actors to interoperate

- System integration and validation testing

- Updates and versioning

https://openfmb.github.io/
OpenFMB Modeling Approach

- Top-down business driven
- Layered architecture
  - Start with use cases and requirements
  - Structured in a single UML model
  - **Sparx EA** as modeling tool
  - Traceability among layers
- Model driven artifacts generation
Duke Energy Microgrid Test Site: Mount Holly, NC

- PV Installations
- Islanding Switch
- Battery & Load-bank
- Behind the meter and control room
- Grid Equipment
Mount Holly Microgrid Components

Not Pictured: 100KW PV system, 10KW PV rooftop, 500KW load-bank
2017 Duke Energy Planned Pilot Circuit
OpenFMB use-cases considered at Rankin/Mount Holly Sites

• Microgrid Management
  – Microgrid Optimization
  – Unscheduled Islanding Transition
  – Grid-to-Island Reconnection

• DER Circuit Segment Management
  – Primary Scenario: Voltage, Frequency, Power Factor support
    • DER Point of Interconnection (POI) Coordination
    • Point of Common Coupling (PCC) Coordination with Microgrid Use-cases
  – Secondary Extensions:
    • Solar Smoothing: Battery Optimization
    • Volt-Var Management: Power Factor Optimization
    • Peak Demand: Shaving/Shifting
  – Tertiary Extensions:
    • Distribution Transfer-Trip
    • Anti-Islanding: Inadvertent Island Detection

• Management Services
  – Visualization: Geospatial Mapping
  – Certificate/Key Management: Authentication/Authorization
  – Policy-based Configuration: Physical Tamper Detection
Data Modeling

Reference Models

- **Standard UML**
  - Standards such as IEC 61968 / 61970 CIM & IEC 61850
  - Provide objects and relationships for OpenFMB requirements
  - Application independent, but defines all concepts needed for any application

Context (Profile)

- **OpenFMB Profiles**
  - Contextual layer restricts information model and extends as needed
    - Cherry-picking reference model for given profile
    - Restrictions and extensions
    - Mandatory and optional
    - Propose extension to the standards / reference models

Message Syntax

- **Message/File Format (XSD, IDL and etc.)**
  - Message syntax describes format for instance data
    - Model driven artifacts generation
    - Serialization of instance data
    - May modify container or associations for message payloads
    - Mappings to various technologies can be defined
Traceability
Platform Independent Model

- Logical model (Profile) built based on the mapping
IDL Generation Tool

- RTI IDL4 for IDL generation
- Link to RTI plug-in

https://github.com/rticommunity/idl4-enterprise-architect/
Platform Specific Model

- Physical implementation artifacts such as XSDs & IDLs are generated from the logical model.
OpenFMB Security Analytics Framework

Use-Case Planning

Data Model

Pub/Sub

Transport

Behavior Analysis

Describe
Identifying Normal Behavior & Good Actors: Commissioning, Updating & Operating

Define
Profiles, Topics, Semantics, Behavior: Operational Functions & Security Policies

Messaging
White-listed, Authenticated, & Encrypted Payloads:
DDS Secure on top of the UDP/IP or TCP/IP

Transport
Transport Layer Security (TLS) 1.2 or plug-in

Security Behavior Analysis
Intrusion Detection & Machine Learning:
Domain Knowledge: Detect, Isolate, Restore
## Standard DDS Security Plug-in Capabilities

| Authentication | Public Key Infrastructure (PKI) with a pre-configured shared Certificate Authority (CA)  
|               | Digital Signature Algorithm (DSA) with Diffie-Hellman for authentication and key exchange |
| Access Control | Specified via permissions file signed by shared CA  
|               | Read and write data topics  
|               | Control over ability to join systems |
| Cryptography   | Protected key distribution  
|               | AES encryption  
|               | HMAC-SHA for message authentication and integrity |
| Data Tagging   | Tags specify security metadata, such as classification level  
|               | Can be used to determine access privileges (via plugin) |
| Logging        | Log security events to a file  
|               | Distribute securely over DDS |
1 – Authentication (asymmetric encryption)
2 – Access Control List (ACL)
3 – Shared Secrets

Access Control
- at Topic level
- or at Instance level

Level of Protection
- Confidentiality / Encryption
- Integrity
- Authentication
- Applies to Data (payload) and/or Meta Data (Headers / Discovery)
- Choices for Domain Governance

Legend
- W – Writer
- R – Reader
- CA – Certificate Authority
- ACL – Access Control List
- DDS – Data Distribution Service
- RTPS – Real-time Pub/Sub
## Integrating SDN into the OpenFMB Framework

<table>
<thead>
<tr>
<th>Ethernet</th>
<th>IP</th>
<th>TCP / UDP</th>
<th>Payload</th>
</tr>
</thead>
<tbody>
<tr>
<td>Layer 2</td>
<td>Layer 3</td>
<td>Layer 4</td>
<td>Layers 5-7</td>
</tr>
</tbody>
</table>

**SDN Flow Control:**
Policy-based Network Management

**Conventional SCADA protocols:**
Unencrypted Raw Data

<table>
<thead>
<tr>
<th>Ethernet</th>
<th>IP</th>
<th>TCP / UDP</th>
<th>OpenFMB Profile Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Layer 2</td>
<td>Layer 3</td>
<td>Layer 4</td>
<td>Layers 5-7</td>
</tr>
</tbody>
</table>

**OpenFMB w/ SDN:**
End-to-End Data Management with Whitelisted and Authenticated Topics
Best Practices / Lesson Learned

• Clear understanding of Microgrids and distributed systems
• Great Teamwork needed across Standards, SGIP, NAESB, OMG, Utilities, and Vendor communities
• Use Case and Data Modeling Team consists of Power Systems, Data Modeling, Computer Architecture, and Embedded Systems Engineers
• Reliability & Determinism of Network & Protocols
• Deny-by-Default/White-listing and Traffic Engineering
• Intrusion Detection & Behavior Analysis
• Authentication, PKI, Certificates, Confidentiality, & Authorization
• Logging, Auditing, & Adherence to Standards
• Configuration, Security, Patch Management
• System Wide Visualization & Case Tracking
• Specific Procurement Language for Hardware and Systems
Discussion – Q&A