Tactical Microgrid Standard (TMS)

Daniel Herring
dherring@ll.mit.edu

OMG MARS, Reston VA

2019-03-19
DISTRIBUTION STATEMENT A. Approved for public release. Distribution is unlimited.

This material is based upon work supported by the Department of the Army under Air Force Contract No. FA8702-15-D-0001. Any opinions, findings, conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Department of the Army.

© 2019 Massachusetts Institute of Technology.

Delivered to the U.S. Government with Unlimited Rights, as defined in DFARS Part 252.227-7013 or 7014 (Feb 2014). Notwithstanding any copyright notice, U.S. Government rights in this work are defined by DFARS 252.227-7013 or DFARS 252.227-7014 as detailed above. Use of this work other than as specifically authorized by the U.S. Government may violate any copyrights that exist in this work.
Tactical Microgrids

- Self-sufficient power
- Warfighter owned and operated
- Thousands of sites, each unique
**Tactical Power Over the Years**

1) **Spot Generation**
   - Inefficient
   - Widely used since Vietnam

2) **Consolidated Generation**
   - Requires expert operators
   - Limited use

3) **Central Microgrid**
   - Single point of failure
   - Some deployment

4) **Distributed Microgrid**
   - More resilient
   - Prototyping today
TMS Independent Verification Test
Humber-Garick Consulting Engineers & Schweitzer Engineering Laboratories

- 60 kW TQG
- 100 kW CAT (new product)
- 60 kW TQG

- 30 kW Taylor

- Tested TMS
- Commercial and DOD devices
- Connect and start in any order
- New capabilities enabled by DDS

Microgrid Controller

30 kW Gilette

Load

Load

Load
**TMS Independent Verification Test**

Humber-Garick Consulting Engineers & Schweitzer Engineering Laboratories

- **60 kW TQG**
- **100 kW CAT (new product)**
- **60 kW TQG**

- **30 kW Taylor**
- **30 kW Gilette**

- **Microgrid Controller**

- **Demonstrated resilient operation**
- **New capability**
Outline

- TMS Overview
  - DDS Reference Implementation
  - Health and Status Telemetry: Data Diode
  - Control Plane Protection: DDS Security Plugin
  - Next Steps
Tactical Microgrid Power

Operator

Source
- Diesel
- Renewables

Distribution
- Boxes
- Cables

Load
- Electrical devices

Storage
- Battery
- Flywheel

Device Role
- Power
Tactical Microgrid Communications

- **Operator**
- **Source**
  - Diesel
  - Renewables
- **Distribution**
- **Load**
  - Electrical devices
- **Storage**
  - Battery
  - Flywheel
- **Microgrid Controller**
- **Microgrid System Manager**
- **Central Management**
- **Coordination Optimization**

Device Role:
- Power
- Communications (Secure DDS)

Test Controller
Development Testing

TMS Overview - 9
DH 2019-03-19
Mission-Driven Configurations

**Spot Generation**
- Standalone capability

**Central Microgrid**
- MSM
- MC
- Source
- Dist
- Storage
- Load

**Distributed Microgrid**
- Source
- Dist
- MSM
- MC
- Load
- Storage

Can interoperate with “dumb” devices

Assemble devices to meet mission needs.

TMS Overview - 10
DH 2019-03-19
Microgrid Control Loops

Legend

- Device
- Message
- Power
- Communications
Cybersecurity
A socio-technical problem

System Lifecycle

- Requirements
- Manufacturing
- Integration
- Acquisition
- Deployment
- Operations & Maintenance
- Sustainment

Cybersecurity enables trustworthy & reliable process control
Attacks Target
Components and Connections

Process Control Points
- Communication
- Control Signal
- Control Action
- Measurement
- Feedback

Example Attacks
- Delay: “Sorry, too late”
- Drop / Filter: “Oops, forgot”
- Modify: “Please run stop”

Malware Injection Opportunities
- Temporary Connection
- Persistent Network Connection
- Supply Chain
Cybersecurity for Microgrids

**System Operator Concerns**

- Am I in control?
- Is the system running well?
- How can I detect and fix problems?
- Are the safeguards operational?

**Safety**

**Availability**

**Integrity**

**Confidentiality**

---

### Ensure Process Control

<table>
<thead>
<tr>
<th>Capability</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authenticate</td>
<td>“Who are you?”</td>
</tr>
<tr>
<td>Maintain Identity</td>
<td>“I am X.”</td>
</tr>
<tr>
<td>Authorize</td>
<td>“What are you allowed to do?”</td>
</tr>
<tr>
<td>Log</td>
<td>“What have you done, and when?”</td>
</tr>
<tr>
<td>Maintain Integrity</td>
<td>“Can I trust this data?”</td>
</tr>
<tr>
<td>Timekeeping</td>
<td>“What time is it?”</td>
</tr>
</tbody>
</table>

### Safely Restore Control

<table>
<thead>
<tr>
<th>Capability</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manual Override</td>
<td>“Can I disable digital controls and manually operate the system?”</td>
</tr>
<tr>
<td>Break Glass</td>
<td>“Can I access the controls quickly in an emergency?”</td>
</tr>
</tbody>
</table>
Outline

• TMS Overview
  ➢ DDS Reference Implementation
• Health and Status Telemetry: Data Diode
• Control Plane Protection: DDS Security Plugin
• Next Steps
Why DDS?

• Strong Technology
  – Fully distributed pub/sub
  – Machine-readable IDL
  – Rich Quality of Service (QoS)
  – Portable API and interoperable wire protocol
  – Security architecture

• Healthy Ecosystem
  – Open standard
  – Stable governance
  – Multiple independent commercial implementations
  – Continuous innovation
  – Used across multiple industries
How We Use DDS

• TMS Data Model
  Middleware Agnostic
  – Message Design
    • Device roles and representation
    • Mechanism, not policy
  – Data Flows
    • Publishers and subscribers
    • Traffic Shaping

• DDS Reference Implementation
  – IDL Files
  – Topic Names
  – Quality of Service (QoS) Settings
  – Sequence Diagrams
  – Development Considerations
DDS Implementation Summary
As of February 2018

PDF Documentation:
- 10-page Data Model Requirements
- 100-page Data Model Object Definitions
- 30-page Implementation Guide

IDL Code: 1381 lines (+ 516 blank lines)
- 34 topic name constants
- 82 structures
- 14 typedefs
- 23 enums
- 127 numeric constants
Sample DDS Statistics
From July 2018 Independent Verification Test

- 9-15 devices
- 40-1308 B payloads
- 344 kbps average total
What’s Next
for DDS Reference Implementation

• Additional IDL
  New device types and capabilities

• DDS XTypes
  Backwards-compatible message versioning

• DDS Security
  API-compatible data protection

• Support Tools
  Acquisitions and development support
Outline

- TMS Overview
- DDS Reference Implementation
  - Health and Status Telemetry: Data Diode
- Control Plane Protection: DDS Security Plugin
- Next Steps

Device Role
- Power
- Communications (Secure DDS)
Data Diode = One-Way Access

- Provide access for remote monitoring
- May filter outgoing traffic
- Block external threats
Data Diode Implementation

- Physical isolation
- No return path
- Cannot be reprogrammed
Data Diode Architecture for DDS

- **Domain 1**: Microgrid Network
- **Domain 2**: Bridge 1
- **Domain 3**: Remote Network

**Bridges**
- Subscribe to left
- Publish to right
- Periodic re-transmit “reliable” topics

**Diode QoS Changes**
- Static discovery
- Infinite lease
- Best effort reliability
Data Diode Status

• Prototyped
  – Commercial data diode
  – RTI Connext DDS Micro

• Demonstrated
  – Hardware protection
  – One-way DDS traffic

• Developing
  – Full bridge software
  – Support for more DDS implementations
  – Tactical hardware package
What’s Next for Data Diode

- Develop capability on other DDS implementations
  Some modifications required
  - RTI Connext DDS Pro
  - Twin Oaks CoreDX DDS
  - Others?

- DDS API Standardization
  Make this a standard feature

- DDS Security Integration
  How to maintain end-to-end data protection

- Forward Error Correction
  Improved reliability without acknowledgement

- Multicast?
  Eliminate need for second bridge?
Outline

- TMS Overview
- DDS Reference Implementation
- Health and Status Telemetry: Data Diode
  ➢ Control Plane Protection: DDS Security Plugin
- Next Steps

Device Role

Power

Communications (Secure DDS)
DDS Security Architecture

Legend
- Application
- DDS Middleware
- DDS Security
- DDS Transport & OS

https://www.omg.org/spec/DDS-SECURITY/
Strong Identity
Cryptographic Bindings

Much more than secure communications.
End to end, across the stack.
Tactical Microgrid Cybersecurity
Usability Requirements

• Simple Operations and Maintenance
  – Policies and Procedures
  – User interface (MIL-STD-1472)

• Dynamic Reconfiguration
  – Add and remove devices without editing files
  – Per-device trust levels: owned, allied, neutral, untrusted

• Stronger Protections
  – Multiple layers of defense
  – Integration with other defenses

• Detect and Respond to Faults and Threats
  – Anomaly / intrusion detection
  – Trust rooted in physical presence of operator
What’s Next for DDS Security

- **Start with Built-in Plugin Baseline Capability**
  - Encrypted communications
  - On-site administration

- **Develop Custom Plugin Full Capability**
  - Address all requirements
  - Incremental functionality upgrades
  - Long-term support
Outline

- TMS Overview
- DDS Reference Implementation
- Health and Status Telemetry: Data Diode
- Control Plane Protection: DDS Security Plugin

Next Steps
Recap of What’s Next for TMS

• DDS Reference Implementation

• Data Diode

• DDS Security
Future TMS Needs for DDS

Functionality

- Testing
  - Validation and Verification
  - System Integration
  - Stress Testing
- Operation
  - Check participants
  - Check topics
  - Check IDL version
  - Check QoS
  - Check data
  - Intrusion detection

Tooling

- Service Contracts
  - Data dependencies, values
  - Timing constraints
- Recording and Playback
- Test Vectors and Fuzzing

Objective: standards-based, non-proprietary solutions.
Conclusion

- See good future for both TMS and DDS
- Standardization brings economies of scale
- Many opportunities
- Look forward to further collaboration
Standards Development and Implementation

- US Army Corps of Engineers
- MIT Lincoln Laboratory
- Humber-Garick Consulting Engineers
- US Army C5ISR
- Schweitzer Engineering Laboratories

Adoption

- US Army PM E2S2
- US Marine Corps

Plus many, many industrial and government organizations.