Tactical Microgrid Standard (TMS)

Daniel Herring
dherring@ll.mit.edu

OMG MARS, Reston VA

2019-03-19

LINCOLN LABORATORY
MASSACHUSETTS INSTITUTE OF TECHNOLOGY

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.

Tactical Microgrids

- Self-sufficient power
- Warfighter owned and operated
- Thousands of sites, each unique

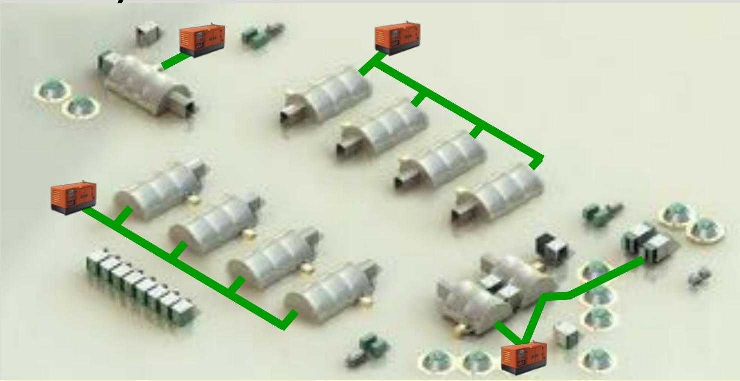
Tactical Power Over the Years

Generators

1) Spot Generation

- Inefficient
- Widely used since Vietnam

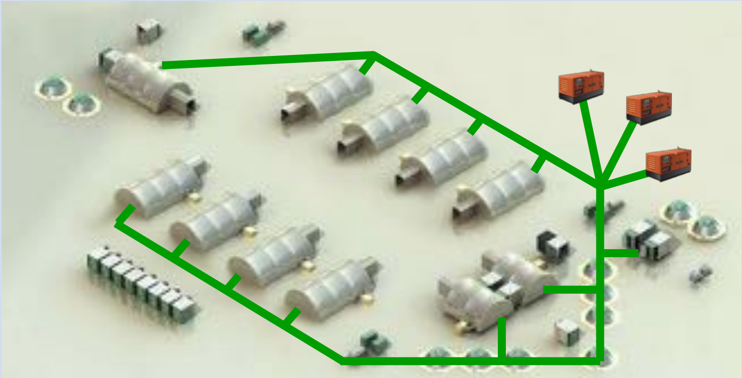
2) Consolidated Generation



- Requires expert operators
- Limited use

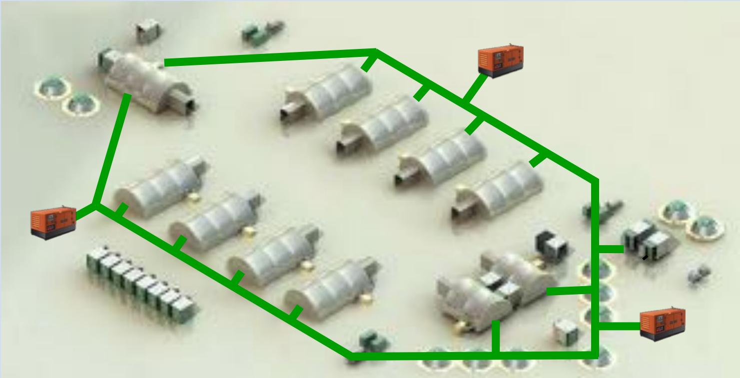
Microgrids

3) Central Microgrid



- Single point of failure
- Some deployment

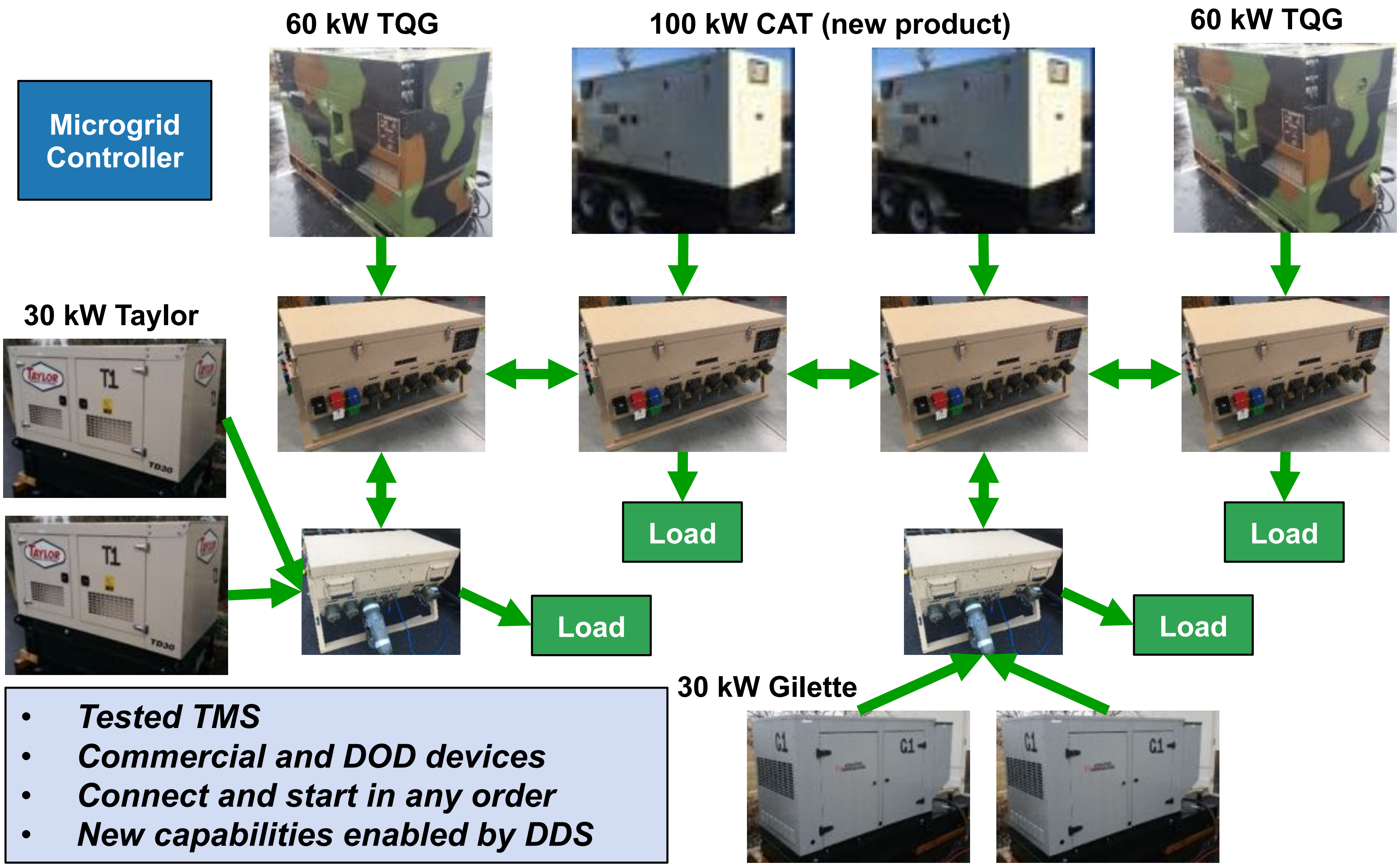
4) Distributed Microgrid



- More resilient
- Prototyping today

TMS Independent Verification Test

Humber-Garick Consulting Engineers & Schweitzer Engineering Laboratories

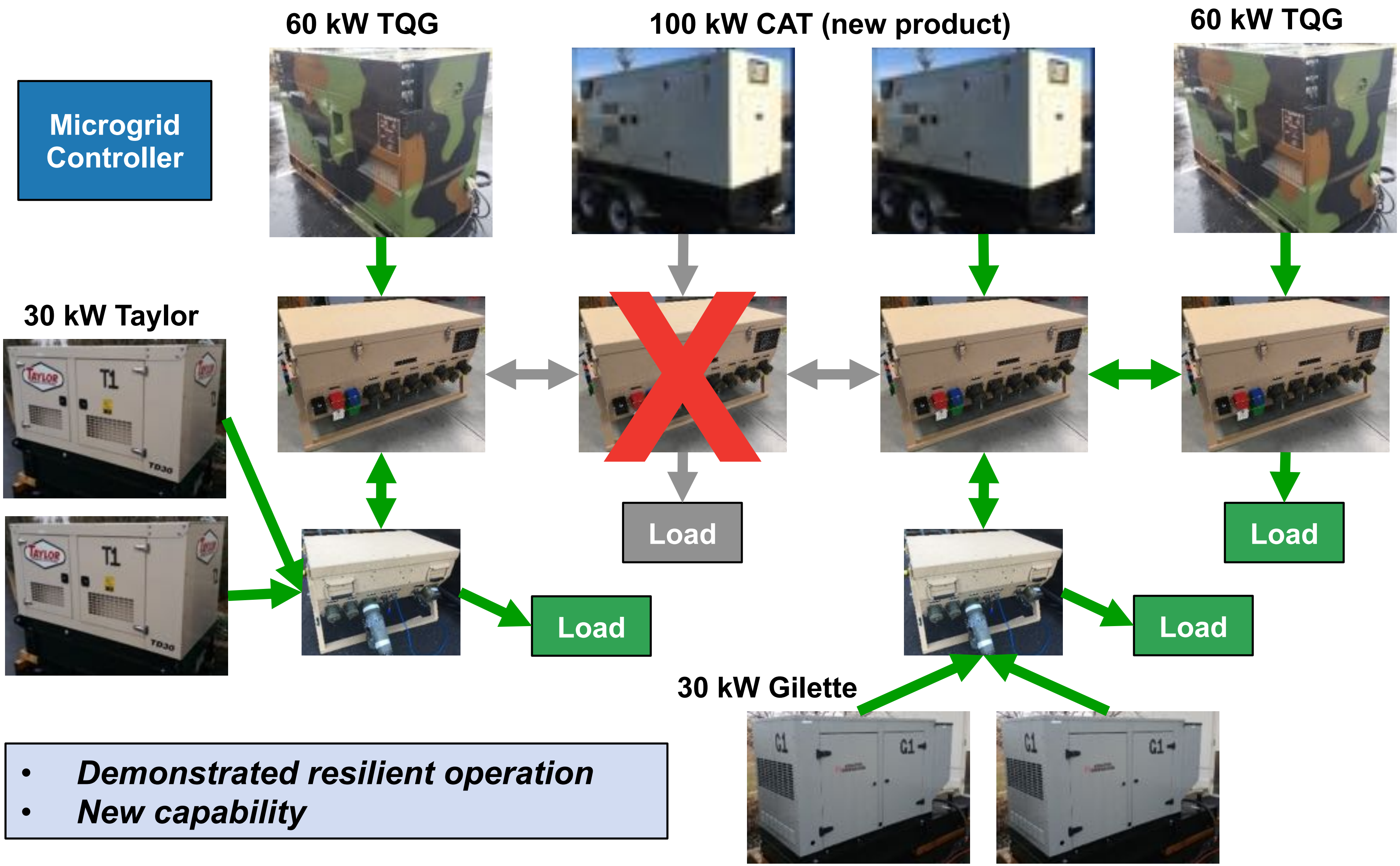


- ***Tested TMS***
- ***Commercial and DOD devices***
- ***Connect and start in any order***
- ***New capabilities enabled by DDS***

LINCOLN LABORATORY
MASSACHUSETTS INSTITUTE OF TECHNOLOGY

TMS Independent Verification Test

Humber-Garick Consulting Engineers & Schweitzer Engineering Laboratories

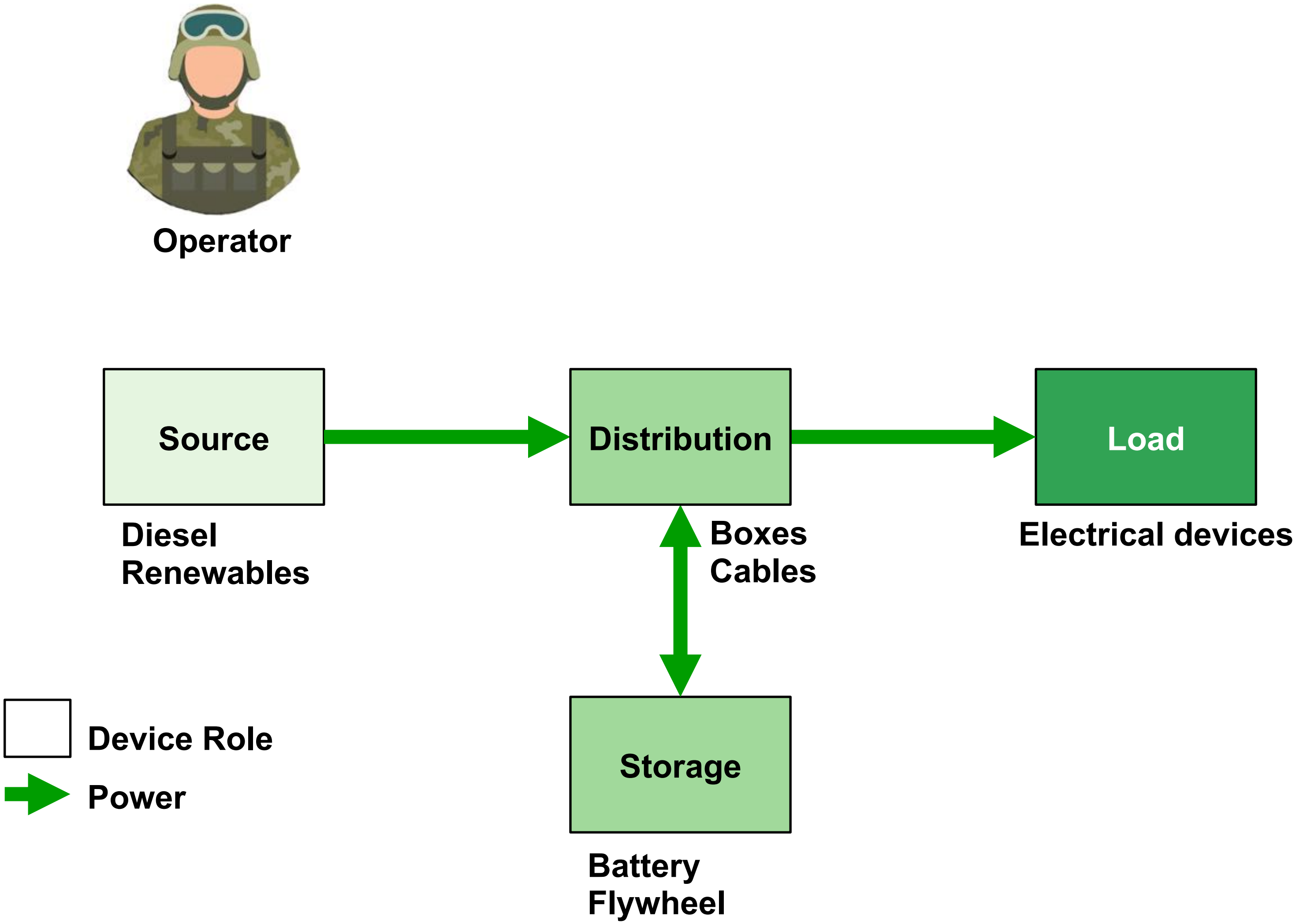


- *Demonstrated resilient operation*
- *New capability*

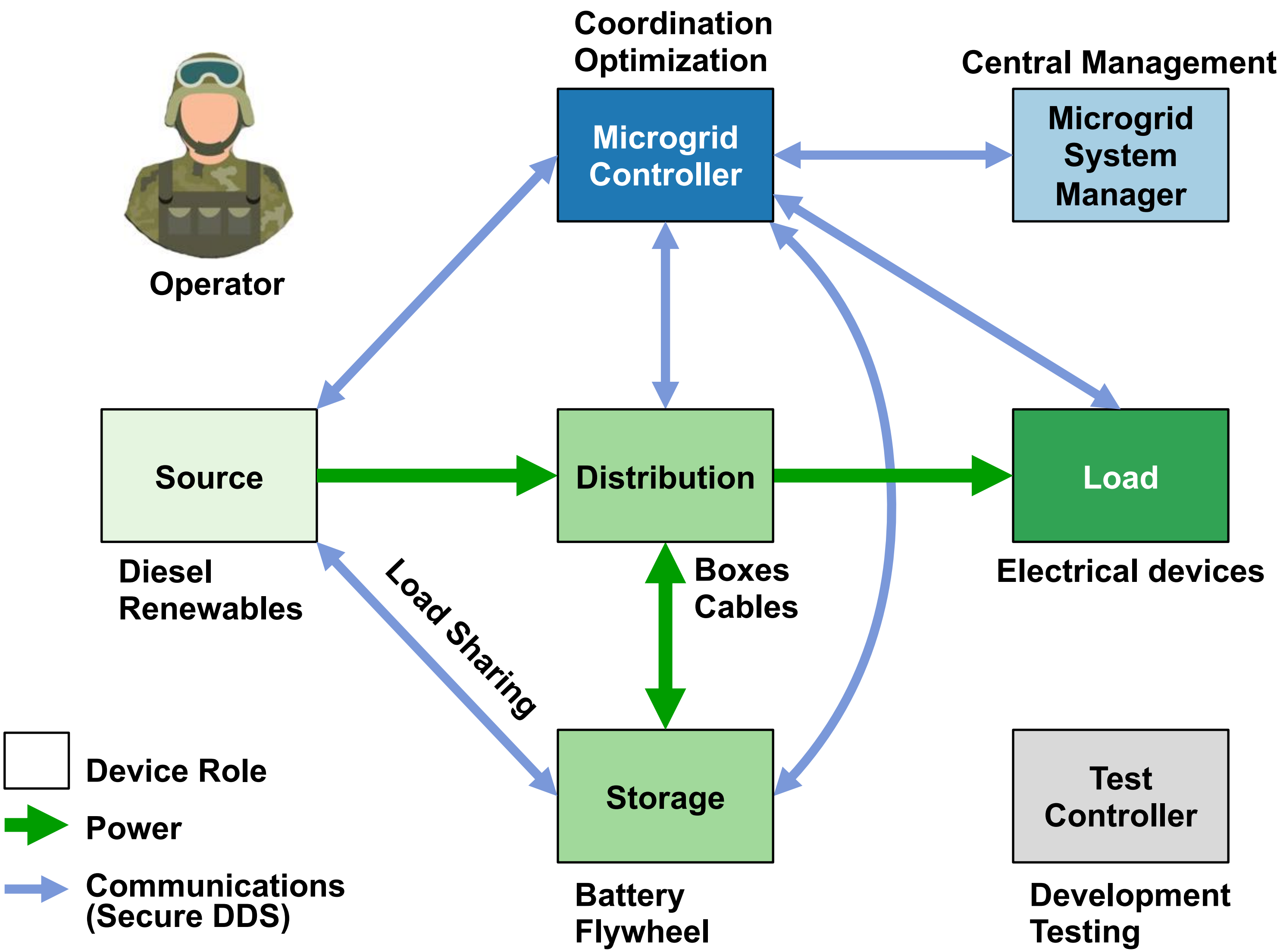
Outline

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

Tactical Microgrid Power

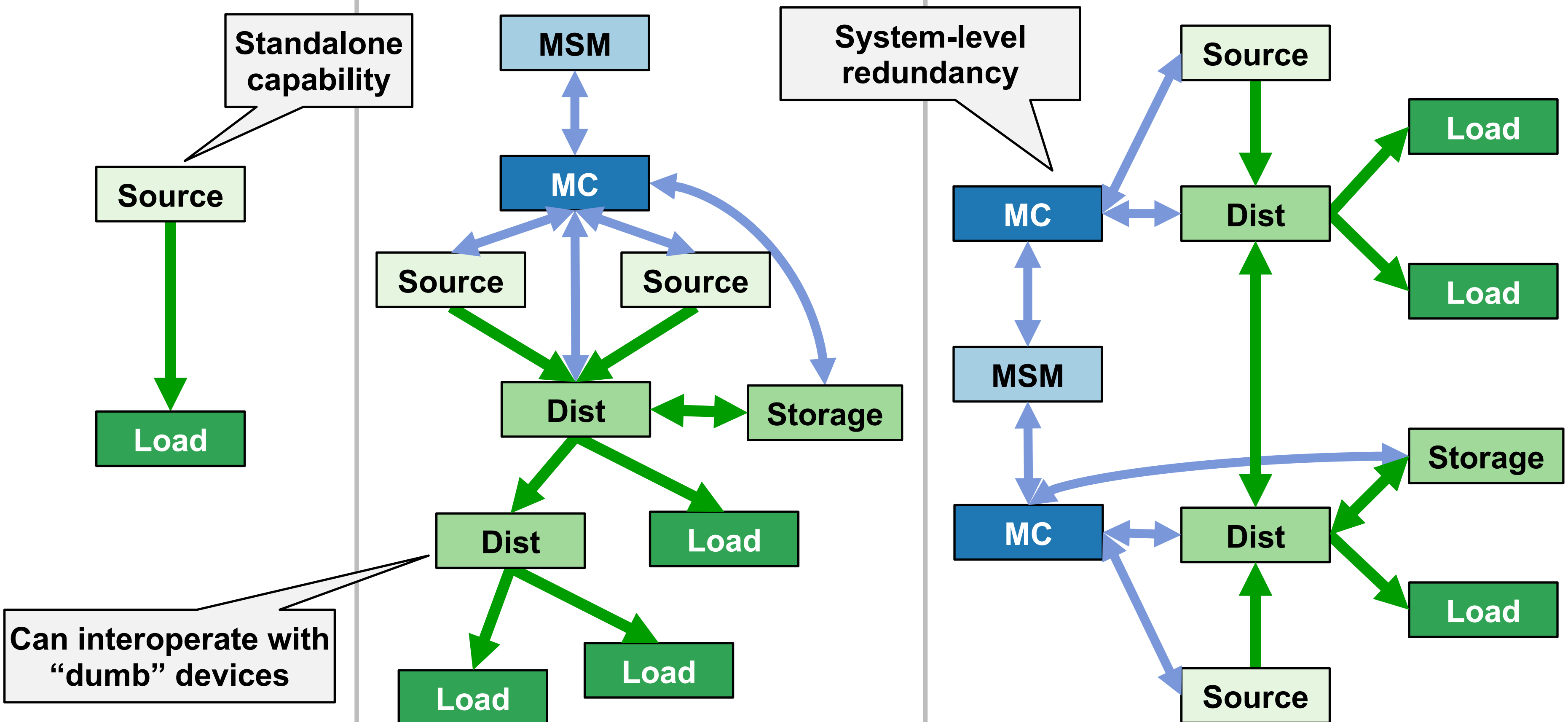


Tactical Microgrid Communications



Mission-Driven Configurations

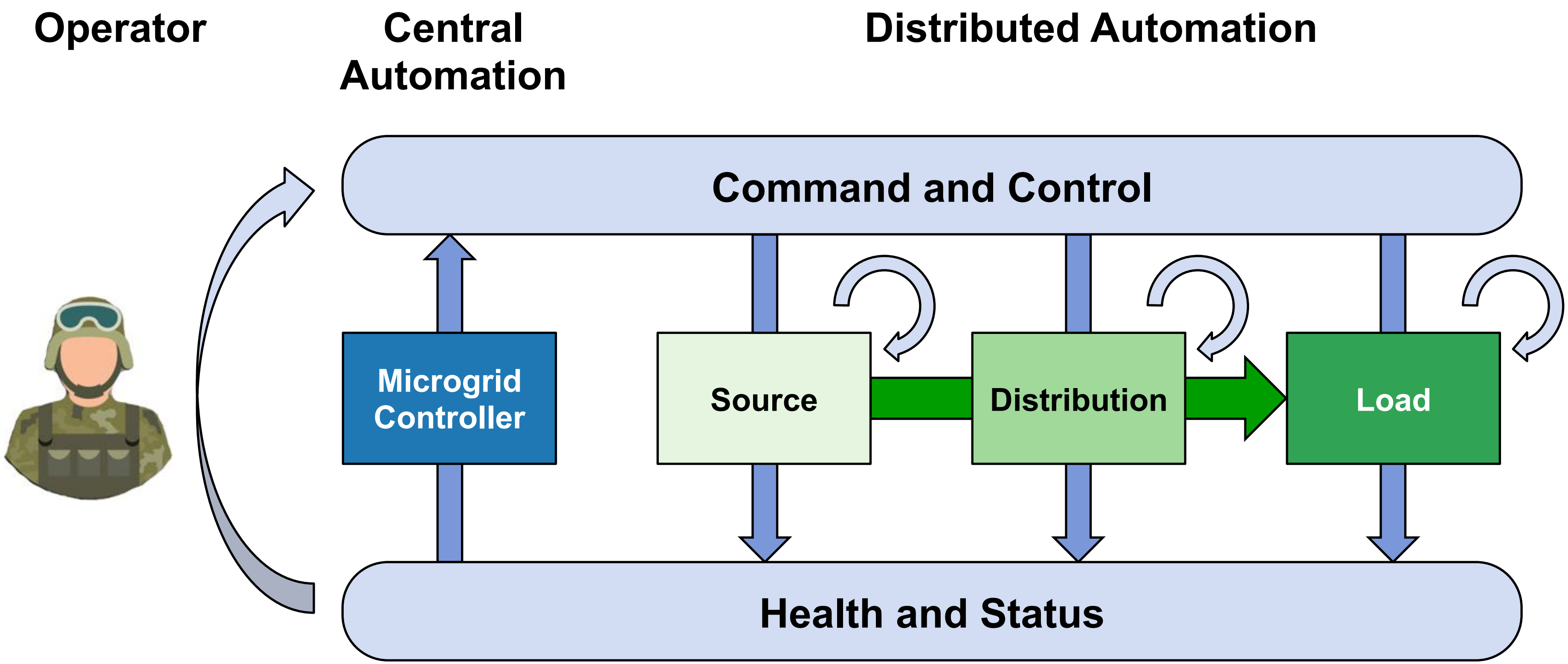
Spot Generation | Central Microgrid | Distributed Microgrid

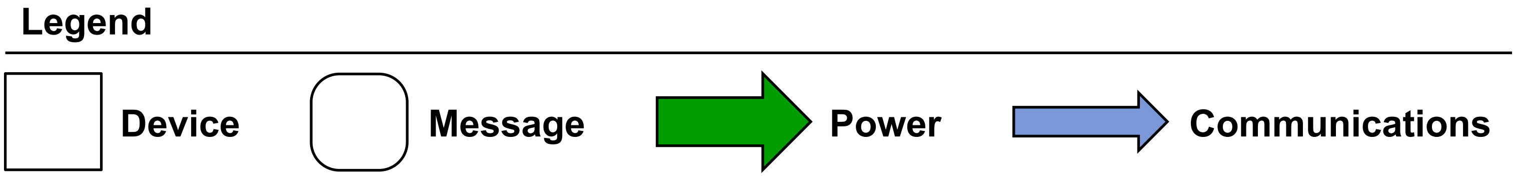


Assemble devices to meet mission needs.

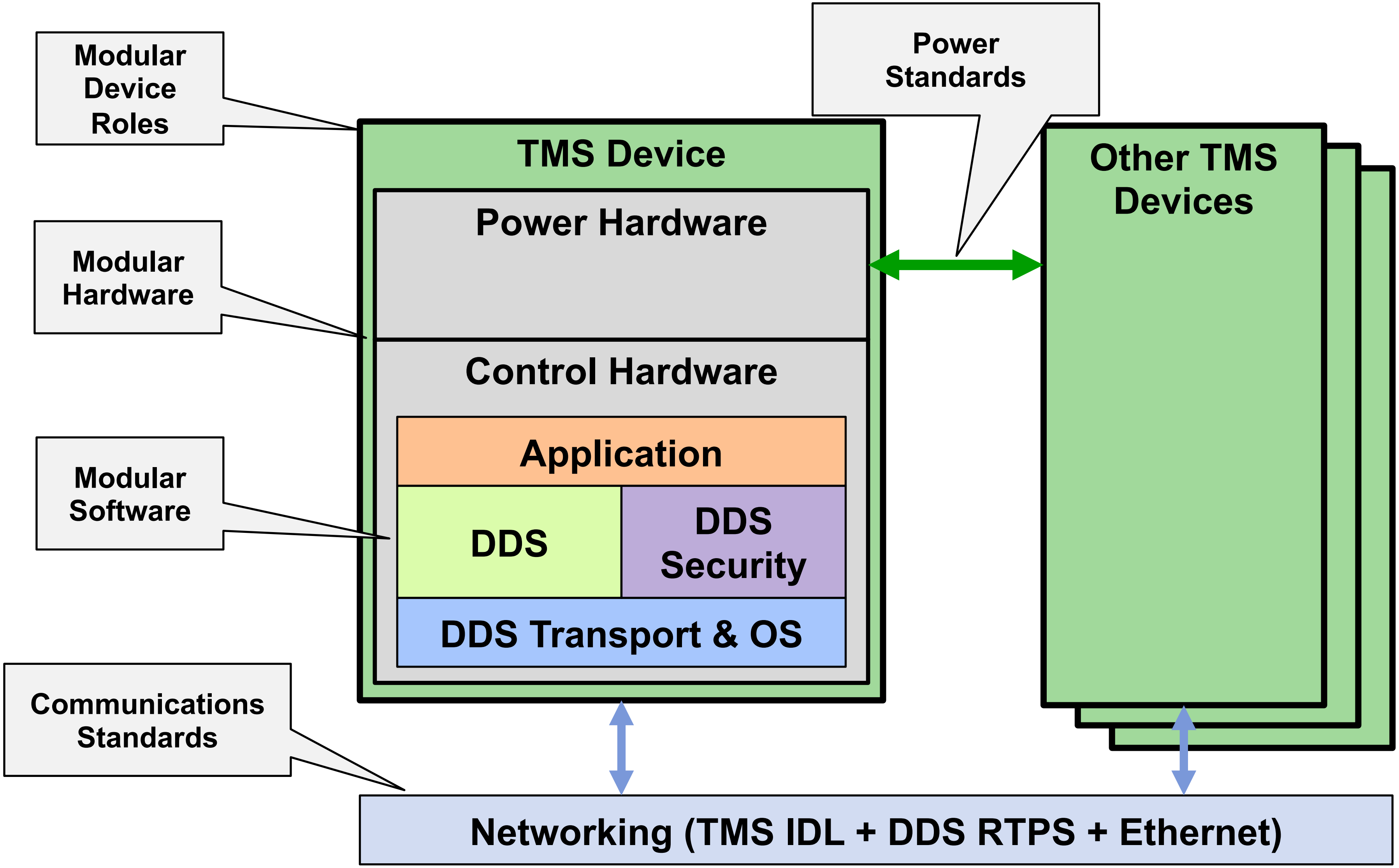
LINCOLN LABORATORY
MASSACHUSETTS INSTITUTE OF TECHNOLOGY

Microgrid Control Loops





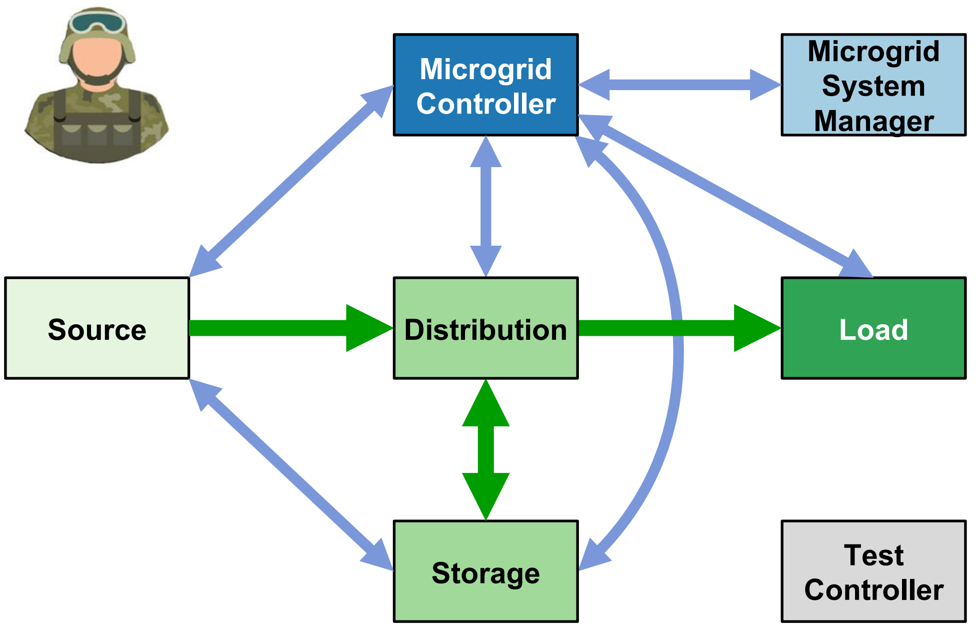
Key Interfaces



Cybersecurity
A socio-technical problem

System Lifecycle

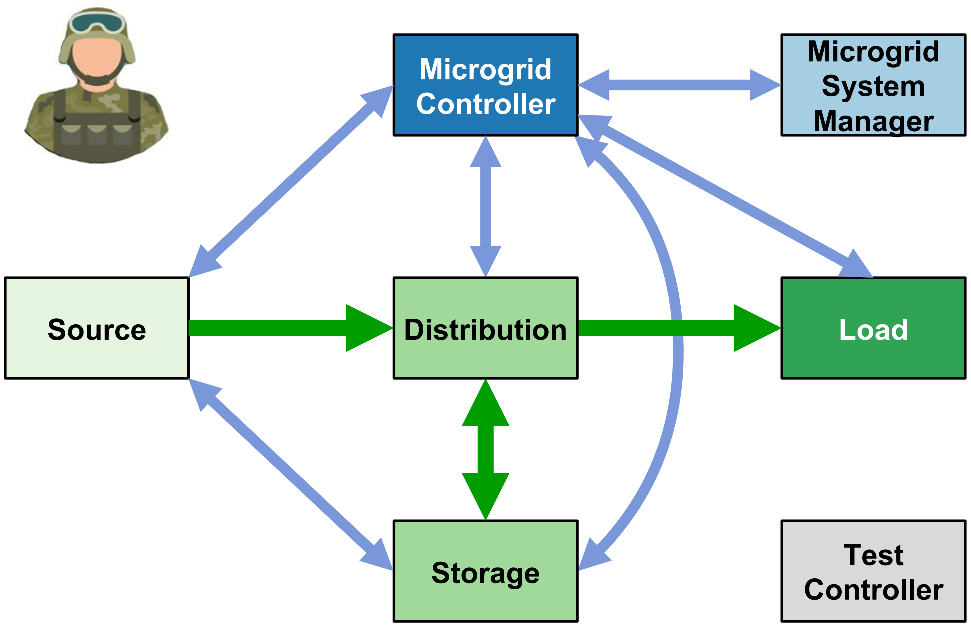
- Requirements
- Manufacturing
- Integration
- Acquisition
- Deployment
- Operations & Maintenance
- Sustainment



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?

Automated

Ensure Process Control

Capability	Example
Authenticate	"Who are you?"
Maintain Identity	"I am X."
Authorize	"What are you allowed to do?"
Log	"What have you done, and when?"
Maintain Integrity	"Can I trust this data?"
Timekeeping	"What time is it?"

Manual

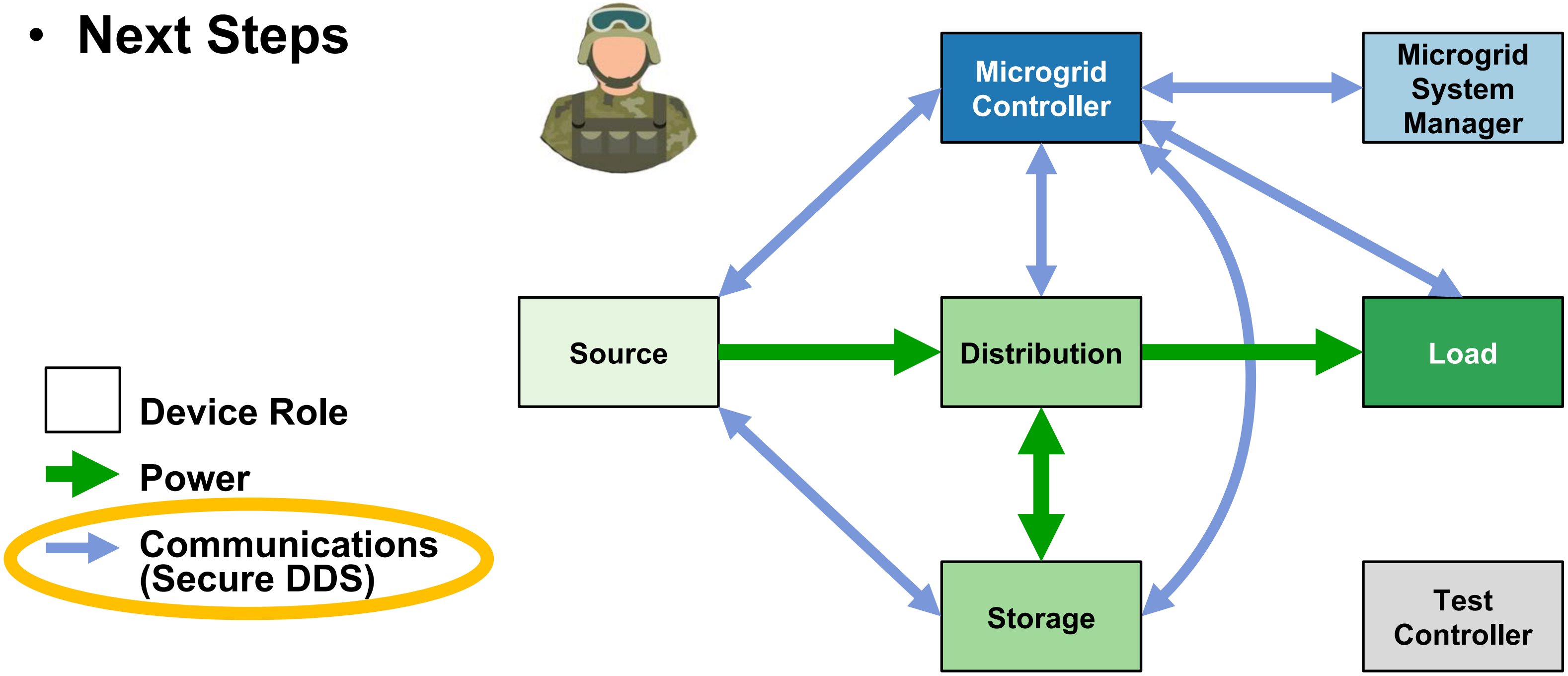
Safely Restore Control

Capability	Example
Manual Override	"Can I disable digital controls and manually operate the system?"
Break Glass	"Can I access the controls quickly in an emergency?"

***S**afety*
***A**vailability*
***I**ntegrity*
***C**onfidentiality*

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**

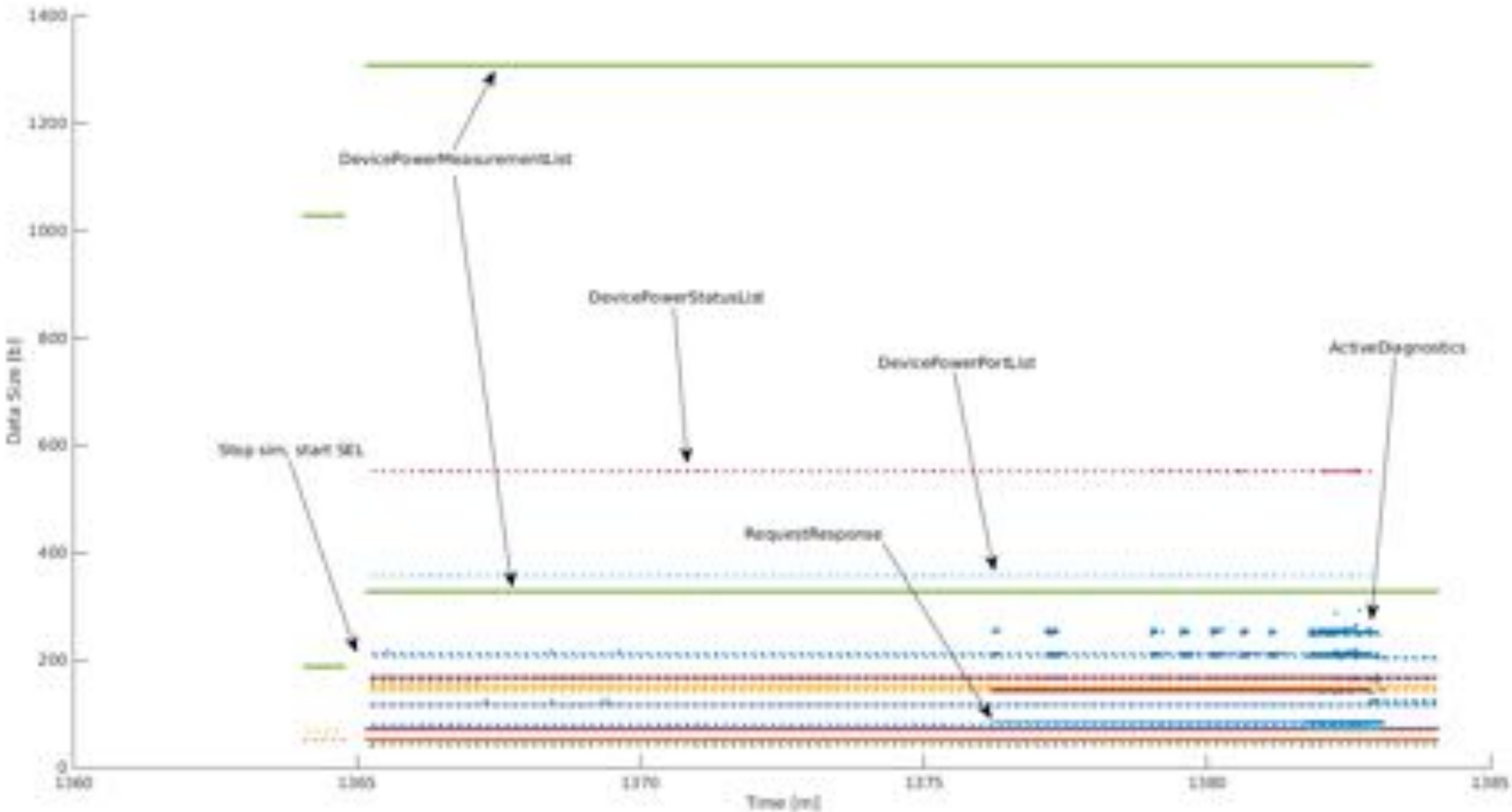
IDL Code: 1381 lines (+ 516 blank lines)

- **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**

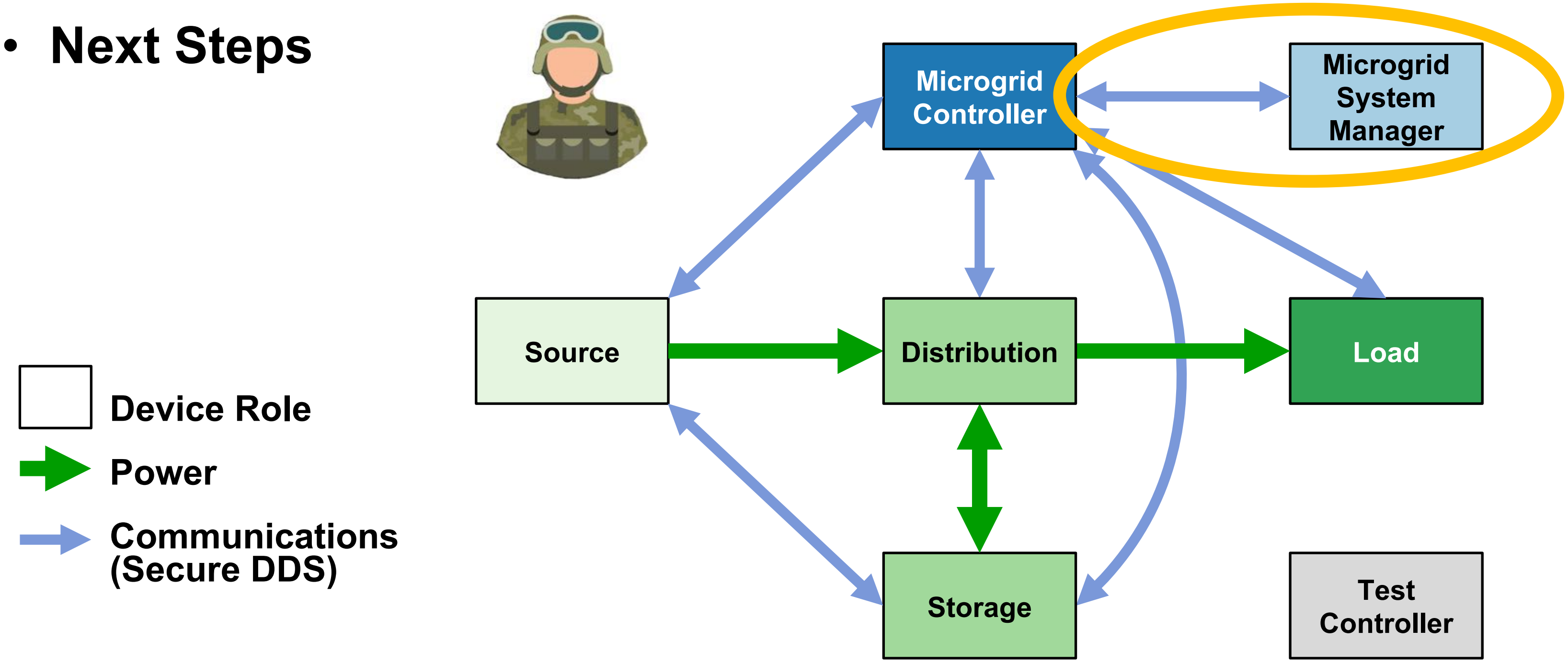


What's Next
for DDS Reference Implementation

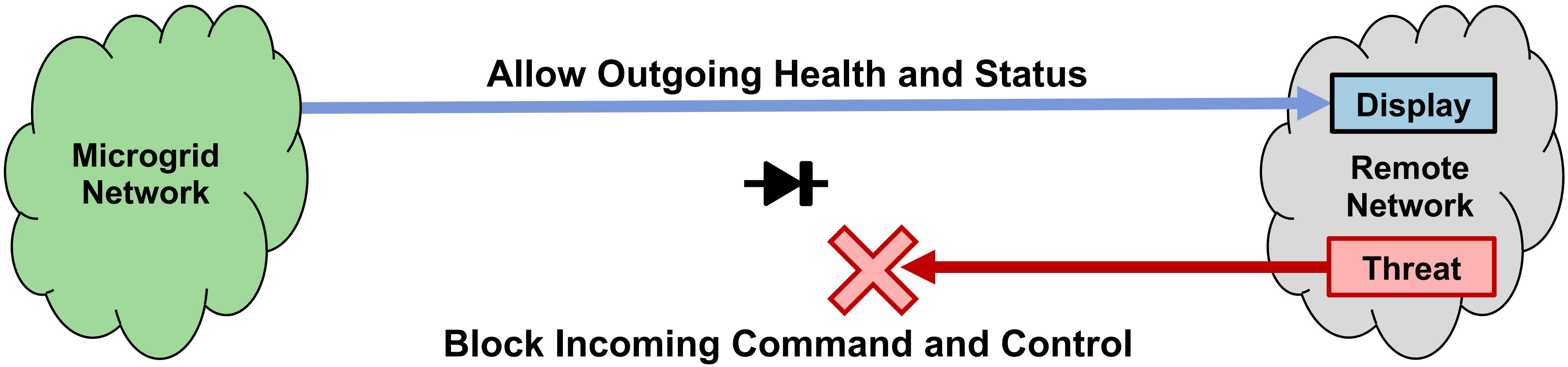
- **Additional IDL**
  New device types and capabilities
- **DDS XTypes**
  Backwards-compatible message versioning
- **DDS Security**
  API-compatible data protection
- **Support Tools**
  Acquisitions and development support

Outline

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

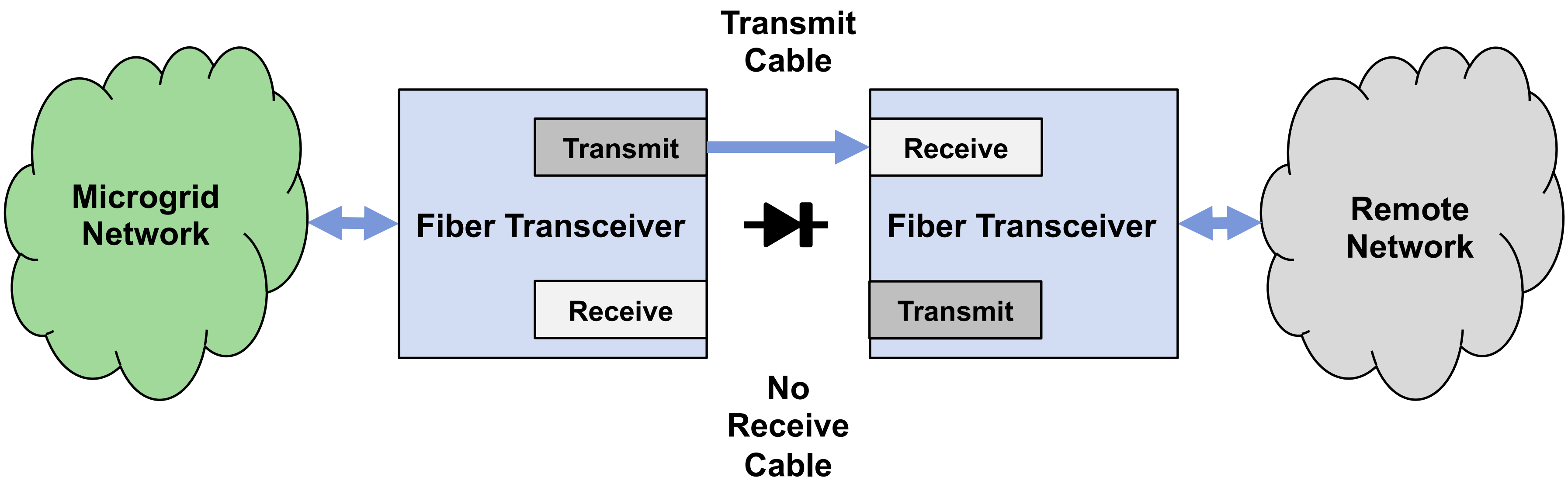


Data Diode = One-Way Access



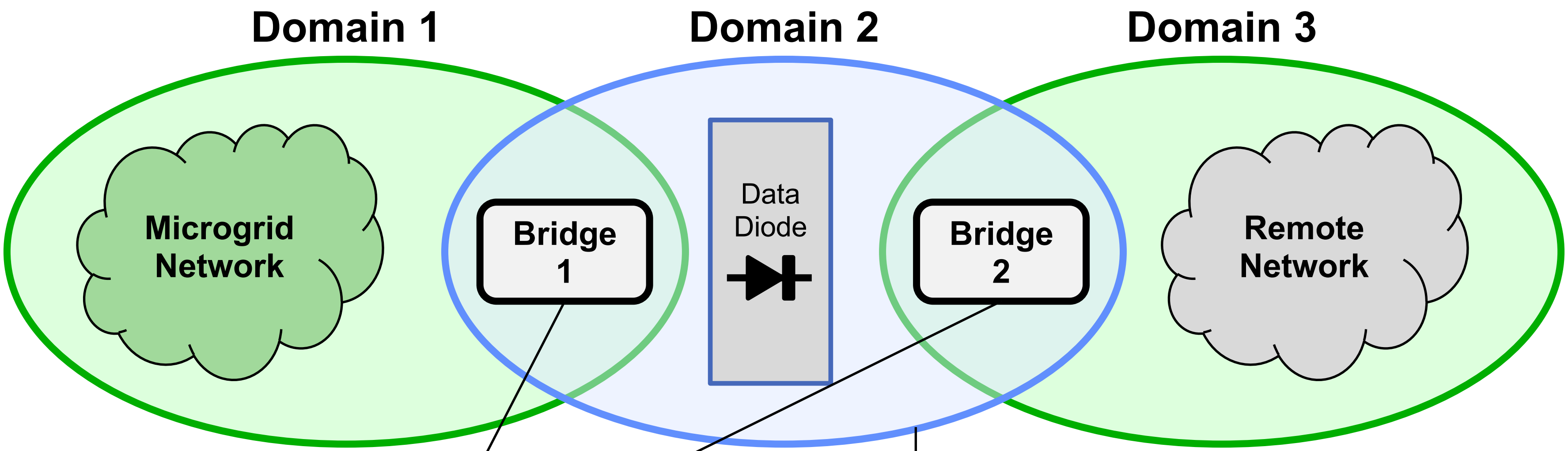
- Provide access for remote monitoring
- May filter outgoing traffic
- Block external threats

Data Diode Implementation



- Physical isolation
- No return path
- Cannot be reprogrammed

Data Diode Architecture for DDS



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

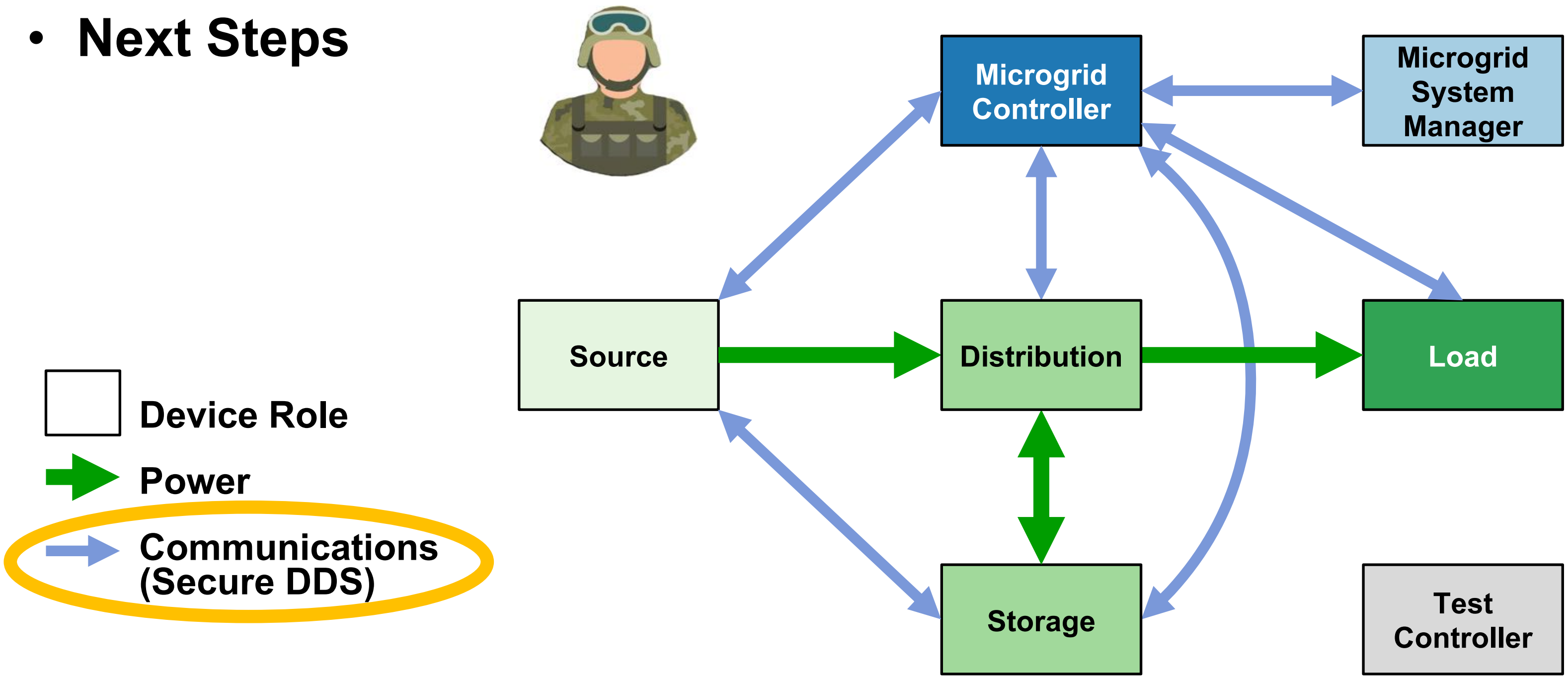
- Prototyped
  - Commercial data diode
  - RTI Connext DDS Micro
- Demonstrated
  - Hardware protection
  - One-way DDS traffic
- Developing
  - Full bridge software
  - Support for more DDS implementations
  - Tactical hardware package

What's Next
for Data Diode

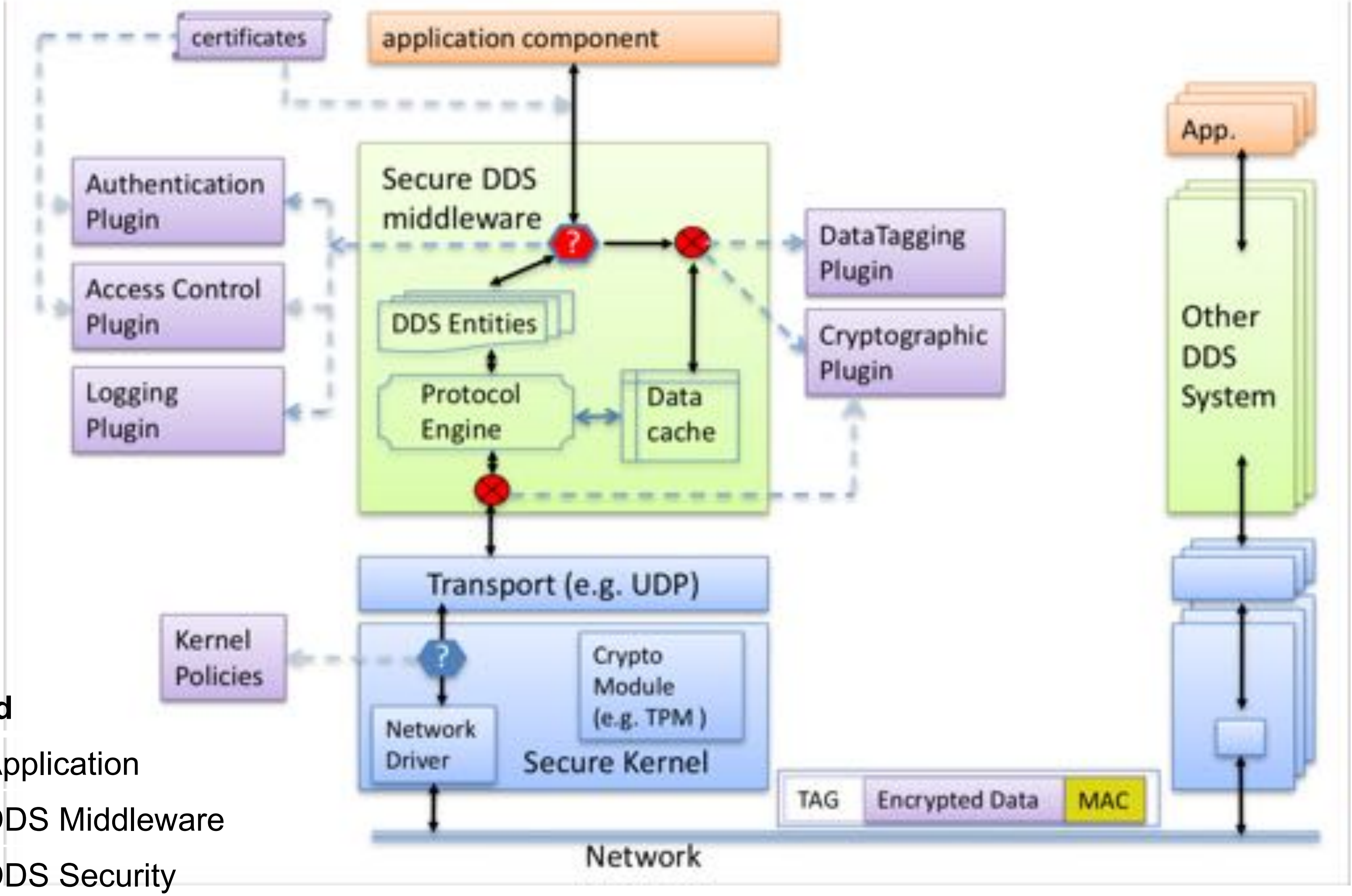
- **Develop capability on other DDS implementations**
  Some modifications required
  - **RTI Connext DDS Pro**
  - **Twin Oaks CoreDX DDS**
  - **Others?**
- **DDS API Standardization**
  Make this a standard feature
- **DDS Security Integration**
  How to maintain end-to-end data protection
- **Forward 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



DDS Security Architecture



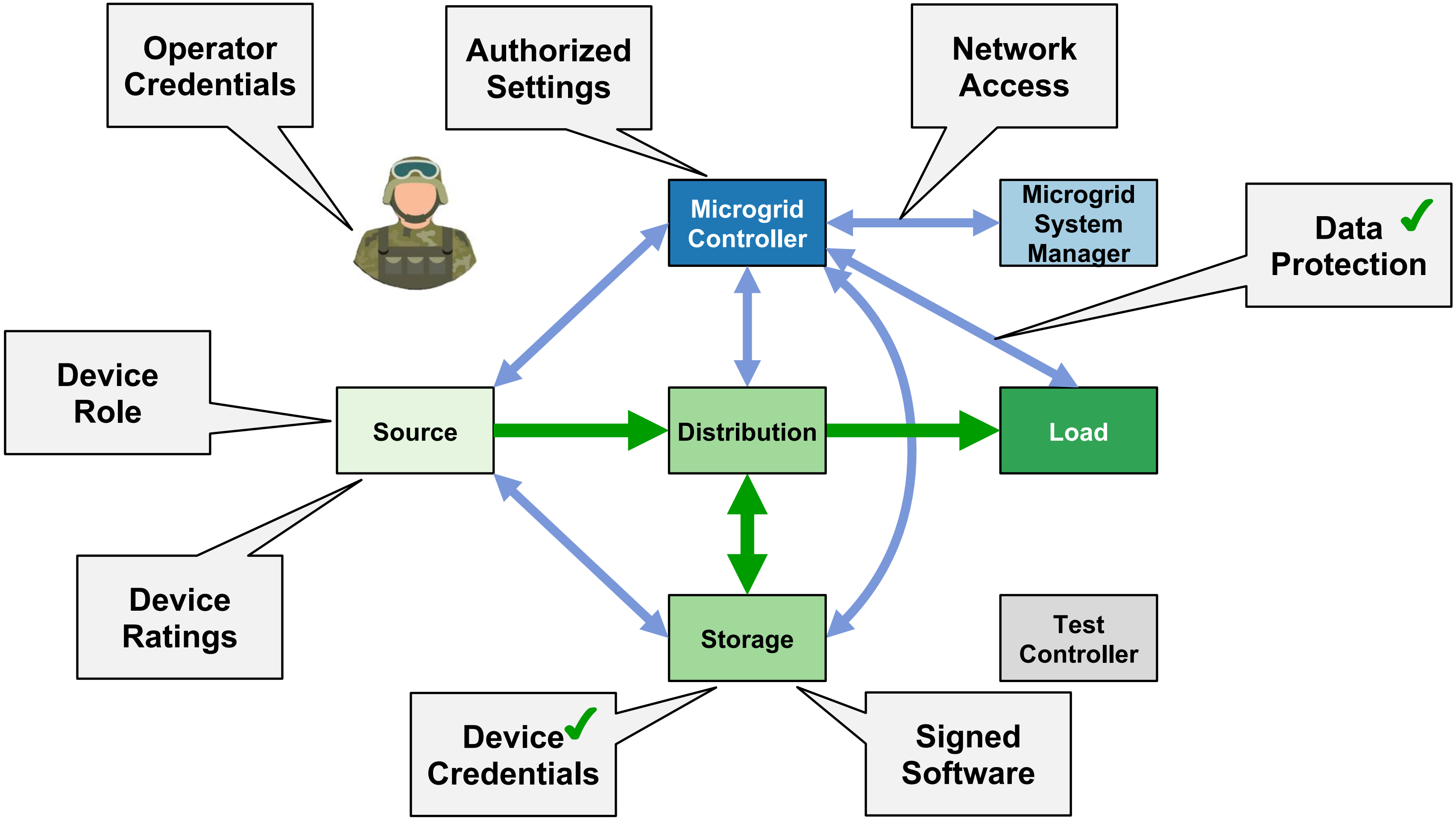
Legend

- 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

Tactical Microgrid Standards Consortium (TMSC)

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.