Messaging Lessons-Learned

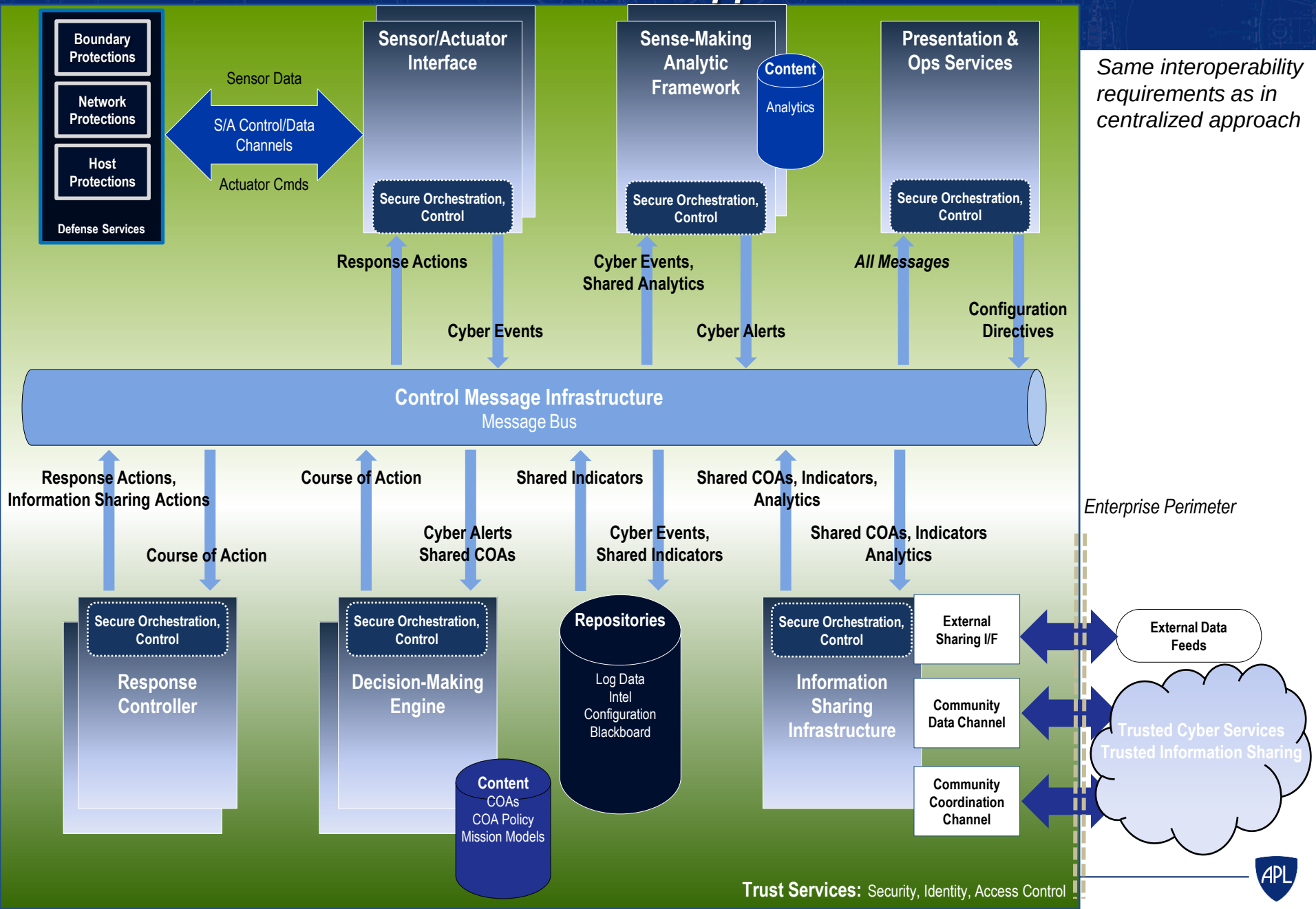
16 February 2016

Kim Watson

Kimberly.Watson@jhuapl.edu

JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

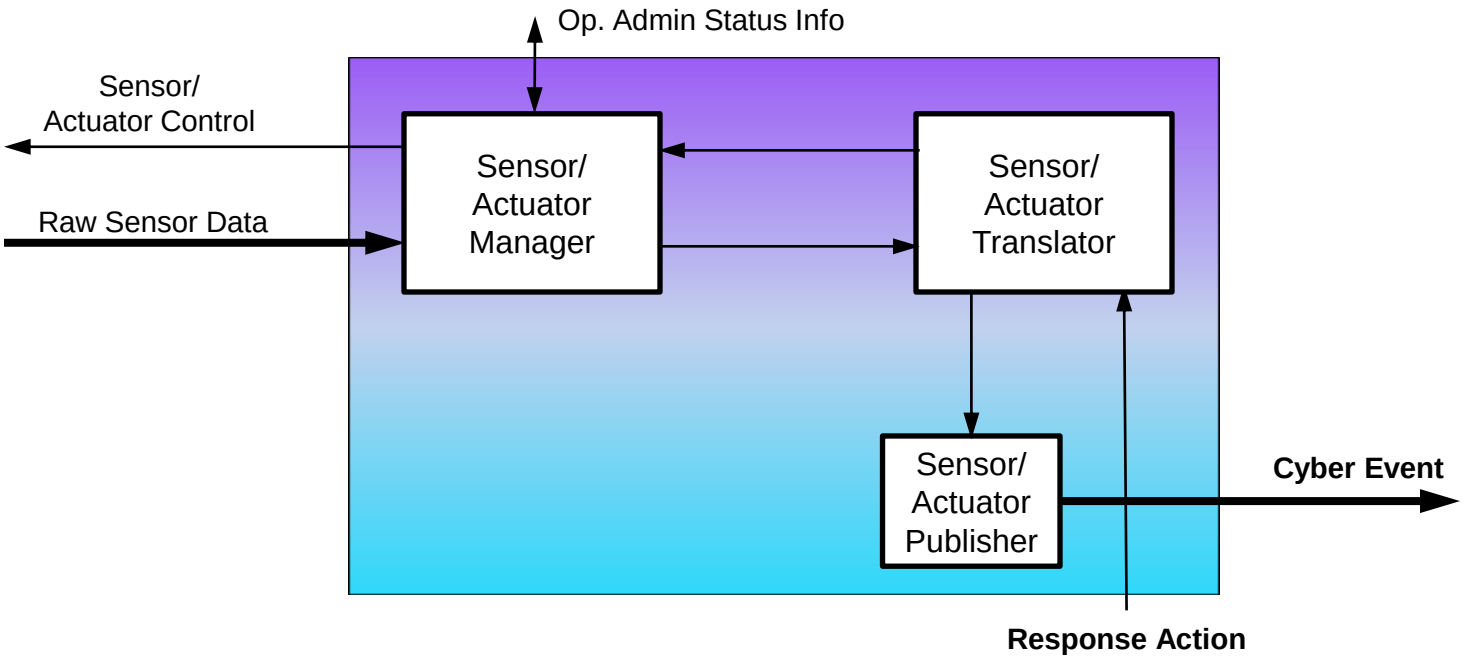
Message Fabric
Decentralized Service Orchestration Approach



Same interoperability requirements as in centralized approach

Message Content
Sensor Actuator Interface

Sensors and actuators have translators and managers that bridge the proprietary interfaces (*Raw Sensor Data*) to the standard Control Message Infrastructure format (***Cyber Events***)



Experimentation Result

- **Integration of sensors to the message bus only required "shimming"**
  - **Typical standard process for integration, nothing abnormal**
  - **Transforms data between application native format and Common Event Format (CEF) if necessary**
  - **Transports data in/out of the message bus**

The Sensor Actuator Interface is the right level of abstraction

4

Lessons Learned

- **Message Fabric**
  - **Products and applications did <u>not</u> need to know about each other or be pairwise integrated to be added into the environment**

- **Sensor/Actuator Integration**
  - **Cybersecurity tools did not have a common interface, data model, or trust model**
    - **The site or the vendors must perform the integration and associated management functions**
    - **Significantly limits the products and applications that can be included in any enterprise**

Message Buses support Scalability, Interoperability, and Simplicity

Implications of Lessons Learned

- **There is potential value in using a message bus when your environment includes:**
  - **Multiple consumers**
  - **Large scale integration**
  - **Dynamic environments**
  - **Extensive network connectivity**

- ***Sustainable* and *extensible* SRCE components need to have common or standardized connectors and data formats**
  - **Standards are not required internal to a single enterprise if the site is willing to be limited by vendor integration**

Implications for SRCE

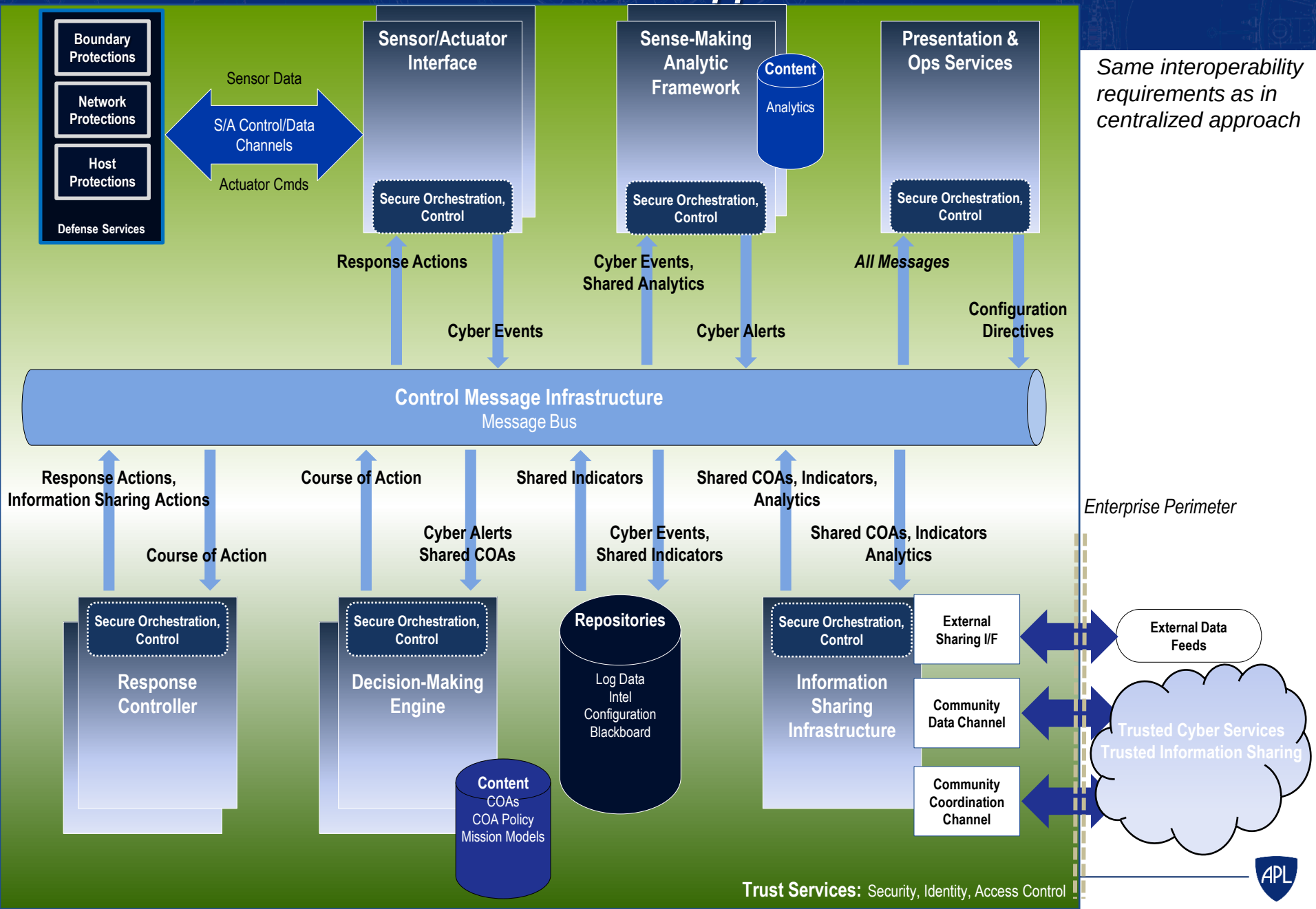
- **Long Term Need: A common message fabric with standard message sets, services, and interfaces**

  - **Short Term: Common Connector**
    - **Products and applications come with at least one of a small set of ways to "plug" into message bus instances**
    - **May not need to be standardized as much as a small list where vendors must support at least one**

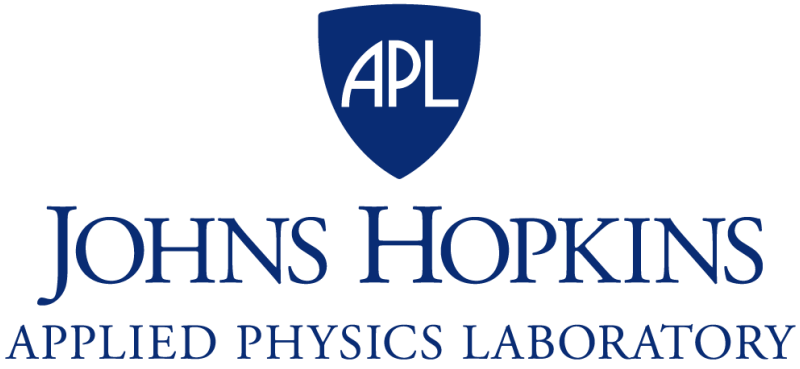
  - **Short Term: Initial common data model**
    - **Cyber Alerts and Response Actions**

Standardization offers more flexibility and avoids significant custom integration

Message Fabric
Decentralized Service Orchestration Approach



Same interoperability requirements as in centralized approach


APL
JOHNS HOPKINS
APPLIED PHYSICS LABORATORY