Proposed Capability-Based Reference Architecture for Real-Time Network Defense

16 November 2015

DISTRIBUTION STATEMENT A -

APPROVAL FOR PUBLIC RELEASE: DISTRIBUTION IS UNLIMITED

Based on work funded by the Department of Homeland Security

Gregg Tally

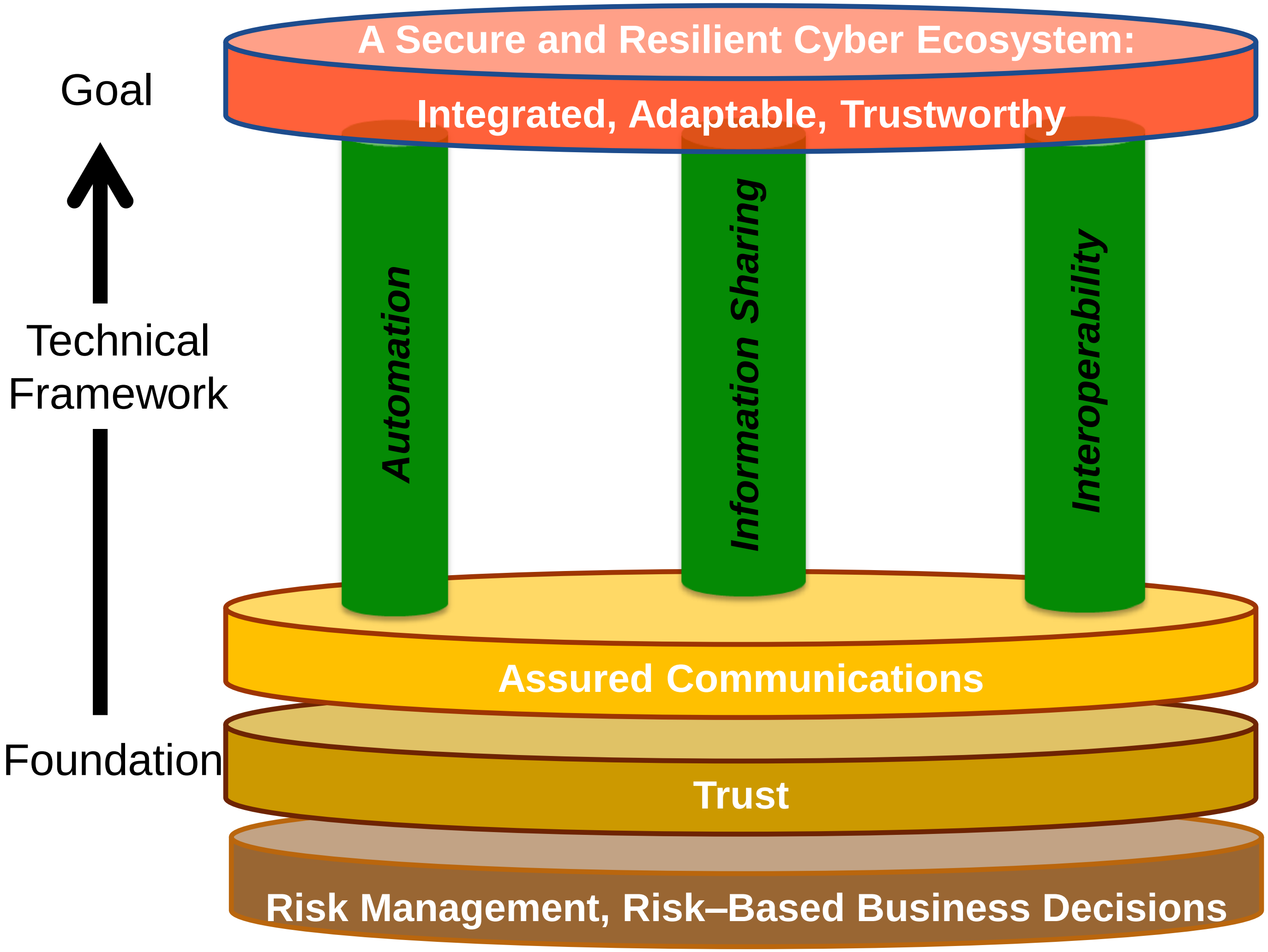
Gregg.Tally@jhuapl.edu

JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

Problem Statement

- **Current asymmetric advantage to the attackers**
  - **Tools support automation of the attack process vs. manual cyber defense operations**
  - **Attackers able to re-use tools and techniques across multiple targets vs. ad hoc information sharing by defenders**
- **Cyber-attack response times are too slow**
  - **Human in the loop, limited analyst time**
  - **Large numbers of cyber events never analyzed**

Pillars of A Cyber Ecosystem


Goal
Technical Framework
Foundation
A Secure and Resilient Cyber Ecosystem:
Integrated, Adaptable, Trustworthy
Automation
Information Sharing
Interoperability
Assured Communications
Trust
Risk Management, Risk–Based Business Decisions

Integrated Adaptive Cyber Defense (IACD)

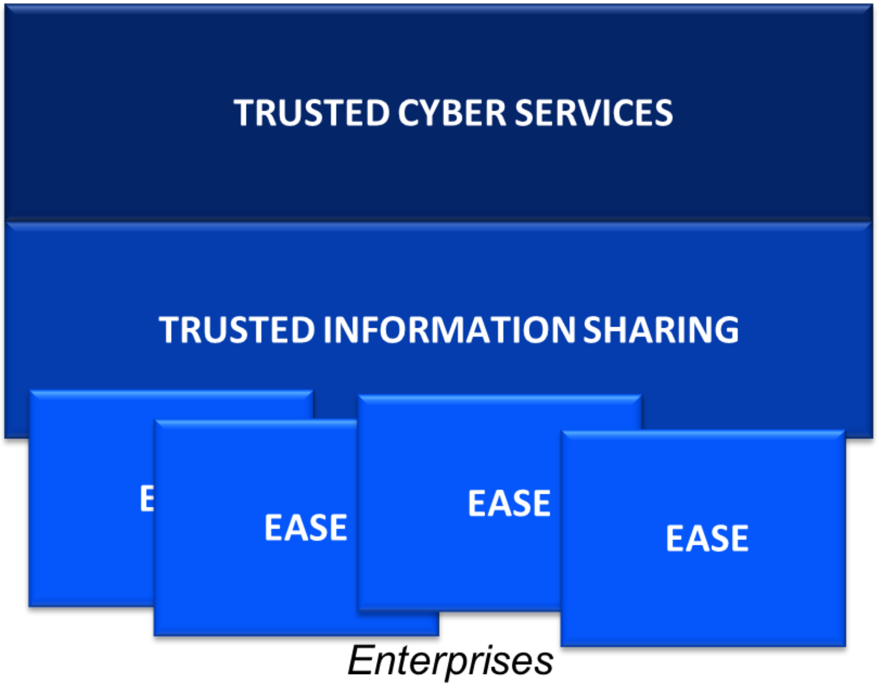
An active cyber defense ecosystem enabling near real-time network defense at the enterprise level.

Trusted information sharing and cyber services across enterprises.

Goals

- **Use human capital for cyber operations more effectively within the community through automation.**
  - **Respond to cyber events as they occur through automated sensing, sense making, decision making, and response**
  - **Increase the number of cyber events in an enterprise that can be analyzed, thereby detecting intrusions earlier in the kill chain.**
- **Degrade the attacker's ability to re-use their wares across the community through enhanced information sharing.**
  - **Rapidly share and ingest threat information, analytics, and effective cyber event responses within the defender community.**
  - **Force attackers to develop new tools and techniques for each new target.**
- **Remove barriers to adoption for the community through interoperability.**
  - **Create a market for security tools that emphasize machine-to-machine information exchange and interoperability.**
  - **Enable diverse but interoperable implementations of IACD, supporting a "bring your own enterprise" approach to integration.**

IACD Constituent Capabilities



- **Trusted Cyber Services**
  - **Trust Services**
  - **Information/Data Management Services**
  - **Analytics, Reputation, and Enrichment Services**
  - **Shared Situational Awareness Services**
  - **Integrated Operational Action Services**
- **Trusted Information Services**
  - **Indicators**
  - **Analytics**
  - **Courses of Action**
- **Enterprise Automated Security Environment (EASE)**
  - **Enterprise Automation**
  - **Interoperability**
  - **Information Sharing**

Reference Architecture Objectives

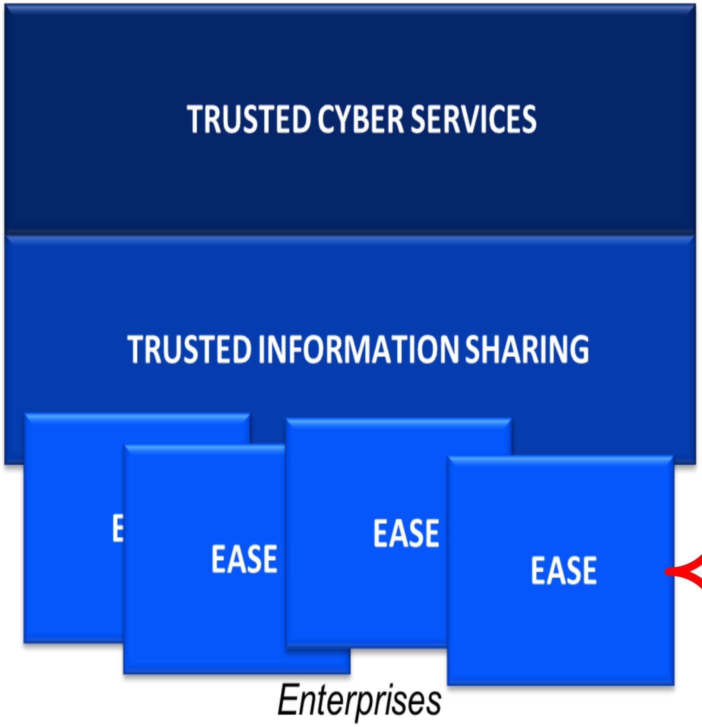
1. Encourage and provide guidelines for implementing security automation and information sharing in enterprises with diverse legacy architectures
2. Promote commercial adoption of standardized machine-to-machine interfaces by communicating IACD needs and requirements to vendors

Approach to the Reference Architecture

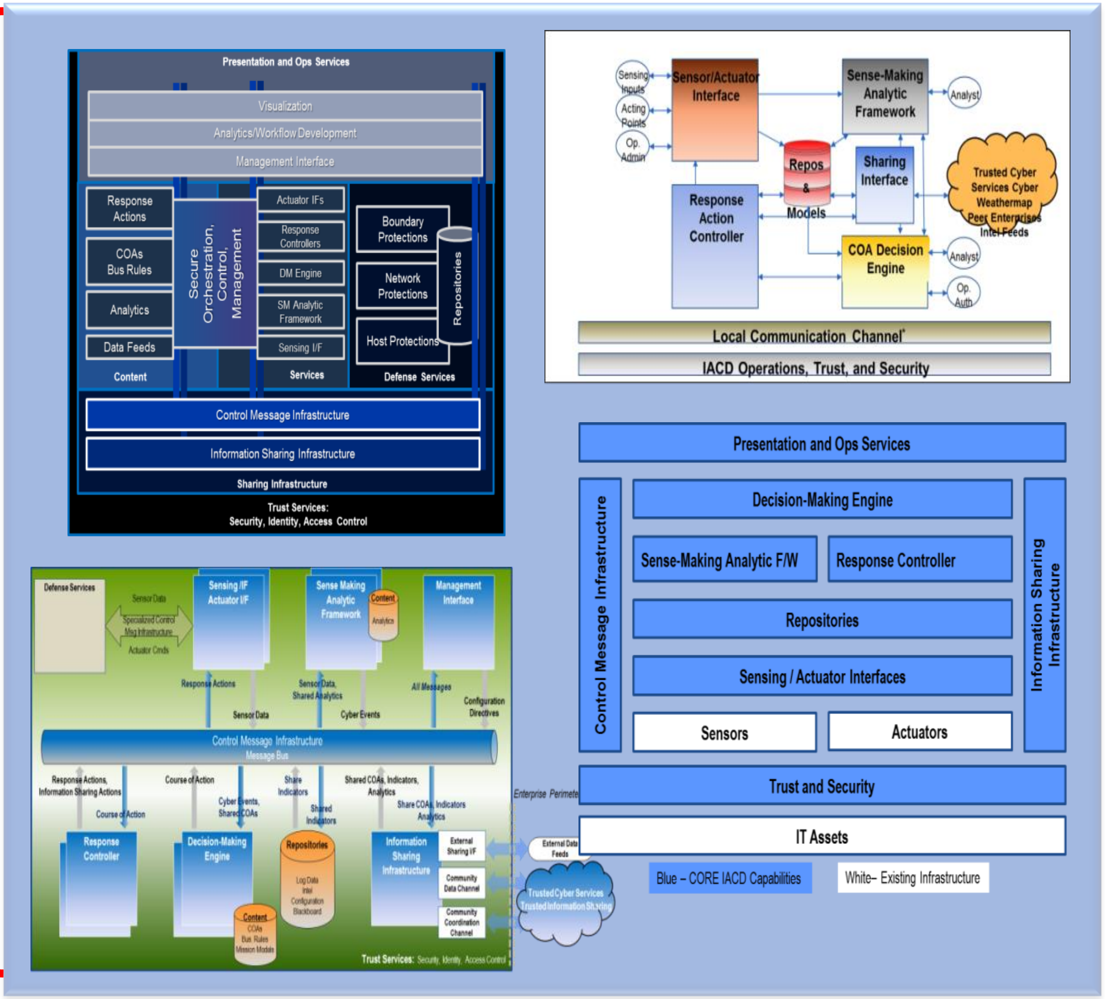
- Capability-based approach
  - Focus on the required capabilities and interactions between them
  - Support many different vendor solutions
- Acknowledge and support a “bring your own enterprise” model
  - Product-agnostic, plug-and-play architecture
- Allow vendors to innovate
  - For each capability, specify the minimum functionality necessary to ensure the capability meets the functional objectives, including interoperability
  - Only specify the essential functions
- Avoid tight coupling between components
  - Support multi-vendor solutions and simplify integration
- Be as stateless as possible within a capability
  - Increase robustness of the solution and prevent resource exhaustion

Enterprise Automated Security Environment (*EASE*)

IACD Constituent Capabilities

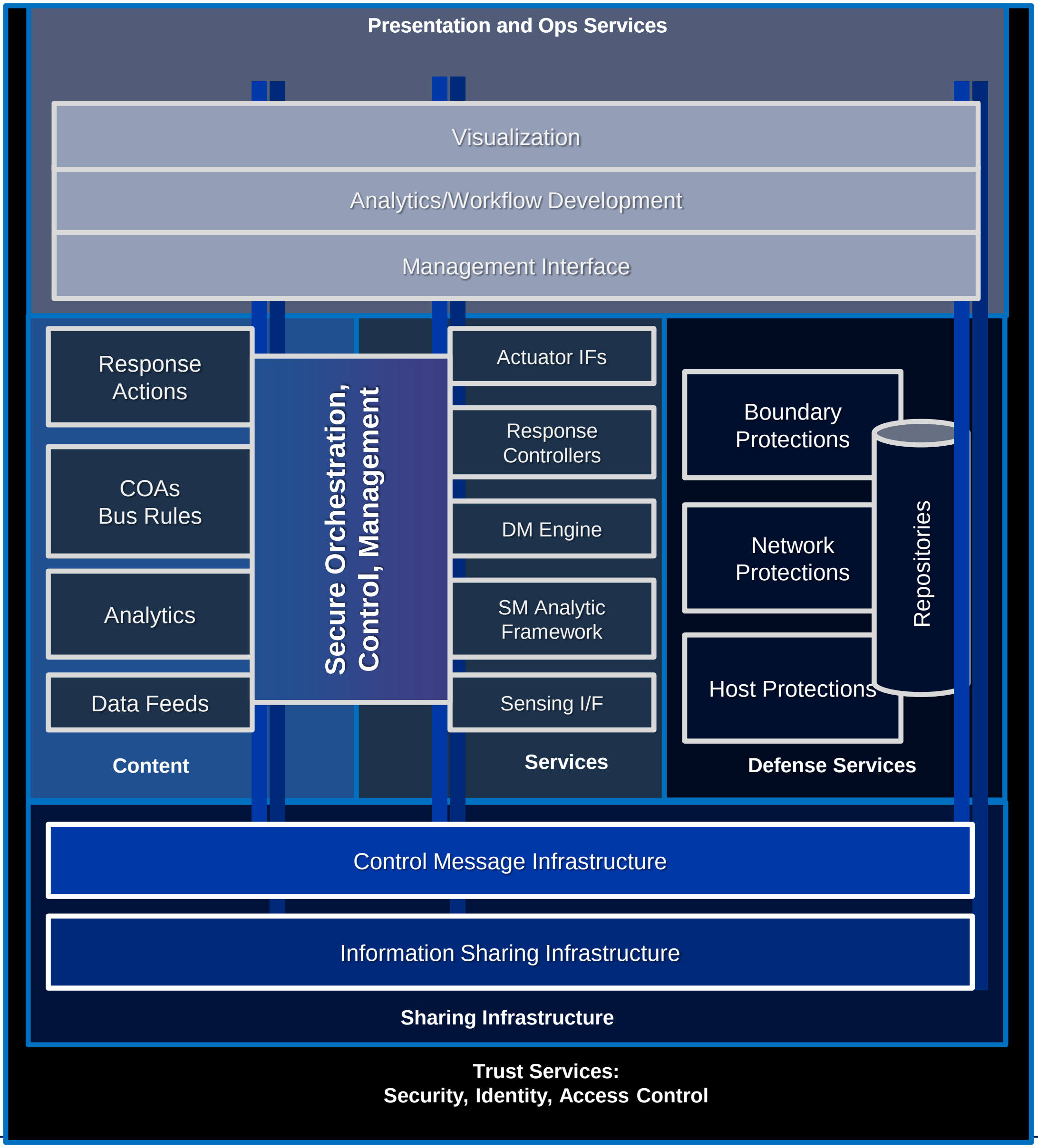


EASE Architectural Views

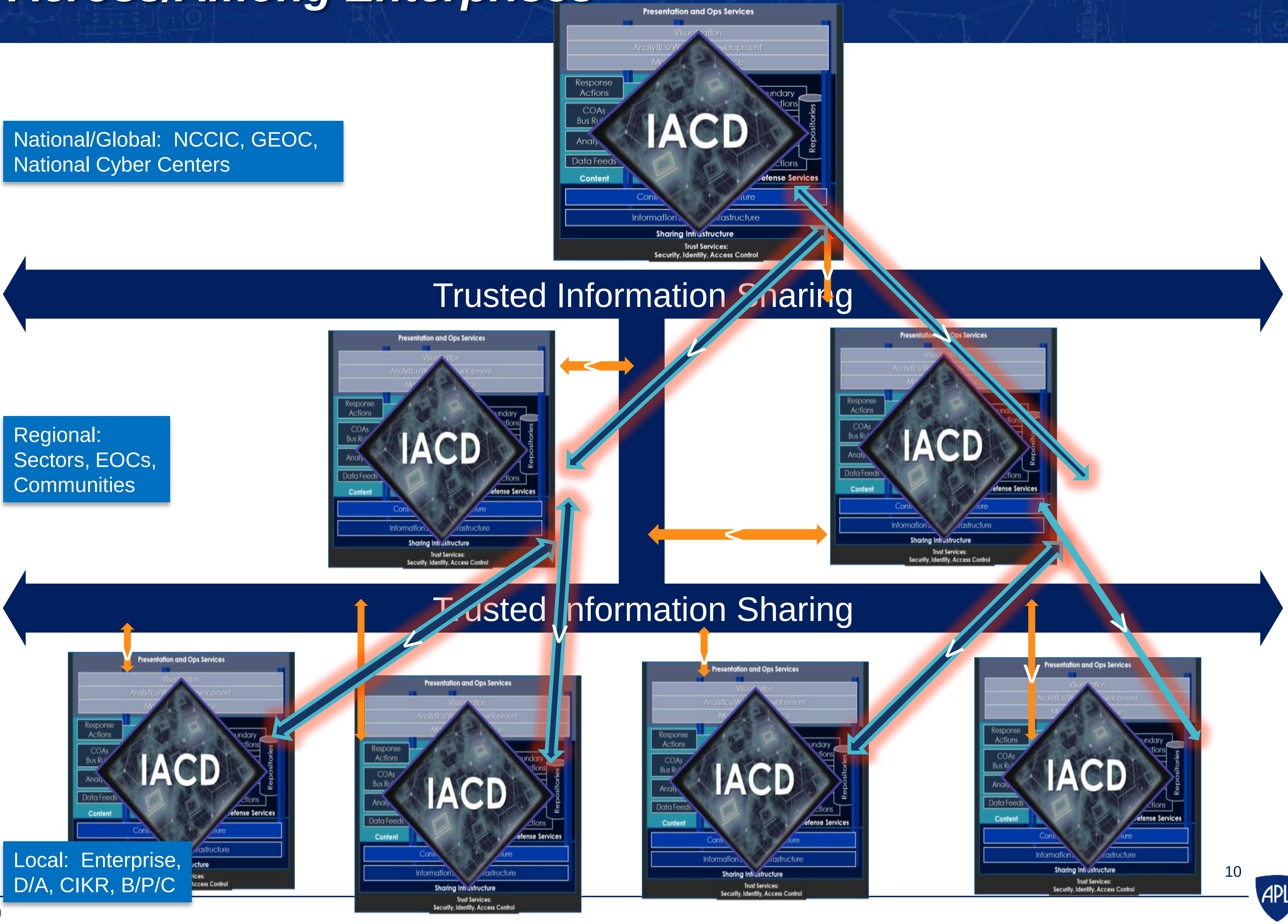

Presentation and Ops Services
Visualization
Analytics/Workflow Development
Management Interface
Response Actions
COAs Bus Rules
Analytics
Data Feeds
Content
Secure Orchestration, Control, Management
Actuator IFs
Response Controllers
DM Engine
SM Analytic Framework
Sensing I/F
Services
Boundary Protections
Network Protections
Host Protections
Repositories
Defense Services
Control Message Infrastructure
Information Sharing Infrastructure
Sharing Infrastructure
Trust Services:
Security, Identity, Access Control
Sensing Inputs
Acting Points
Op. Admin
Sensor/Actuator Interface
Sense-Making Analytic Framework
Analyst
Repos & Models
Sharing Interface
Trusted Cyber Services Cyber Weathermap Peer Enterprises Intel Feeds
Response Action Controller
COA Decision Engine
Analyst
Op. Auth
Local Communication Channel*
IACD Operations, Trust, and Security
Defense Services
Sensor Data
Specialized Control Msg Infrastructure
Actuator Cmds
Sensing /IF Actuator I/F
Sense Making Analytic Framework
Content
Analytics
Management Interface
Response Actions
Sensor Data
Sensor Data, Shared Analytics
Cyber Events
All Messages
Configuration Directives
Control Message Infrastructure
Message Bus
Response Actions, Information Sharing Actions
Course of Action
Course of Action
Cyber Events, Shared COAs
Share Indicators
Shared Indicators
Shared COAs, Indicators, Analytics
Share COAs, Indicators Analytics
Response Controller
Decision-Making Engine
Content
COAs
Bus Rules
Mission Models
Repositories
Log Data
Intel
Configuration
Blackboard
Information Sharing Infrastructure
External Sharing I/F
Community Data Channel
Community Coordination Channel
Trust Services: Security, Identity, Access Control
Enterprise Perimeter
External Data Feeds
Trusted Cyber Services
Trusted Information Sharing
Presentation and Ops Services
Control Message Infrastructure
Decision-Making Engine
Sense-Making Analytic F/W
Response Controller
Repositories
Sensing / Actuator Interfaces
Sensors
Actuators
Information Sharing Infrastructure
Trust and Security
IT Assets
Blue – CORE IACD Capabilities
White– Existing Infrastructure

Focus of briefing

Conceptual View
Functionality Inside the Enterprise



Conceptual View
Across/Among Enterprises


Presentation and Ops Services
Visualization
Analytics/Workflow Development
Response Actions
COAs Bus Rules
Analytics
Data Feeds
Content
Boundary Actions
Repositories
Defense Services
Information Sharing Infrastructure
Sharing Infrastructure
Trust Services: Security, Identity, Access Control
IACD
Trusted Information Sharing
Trusted Information Sharing

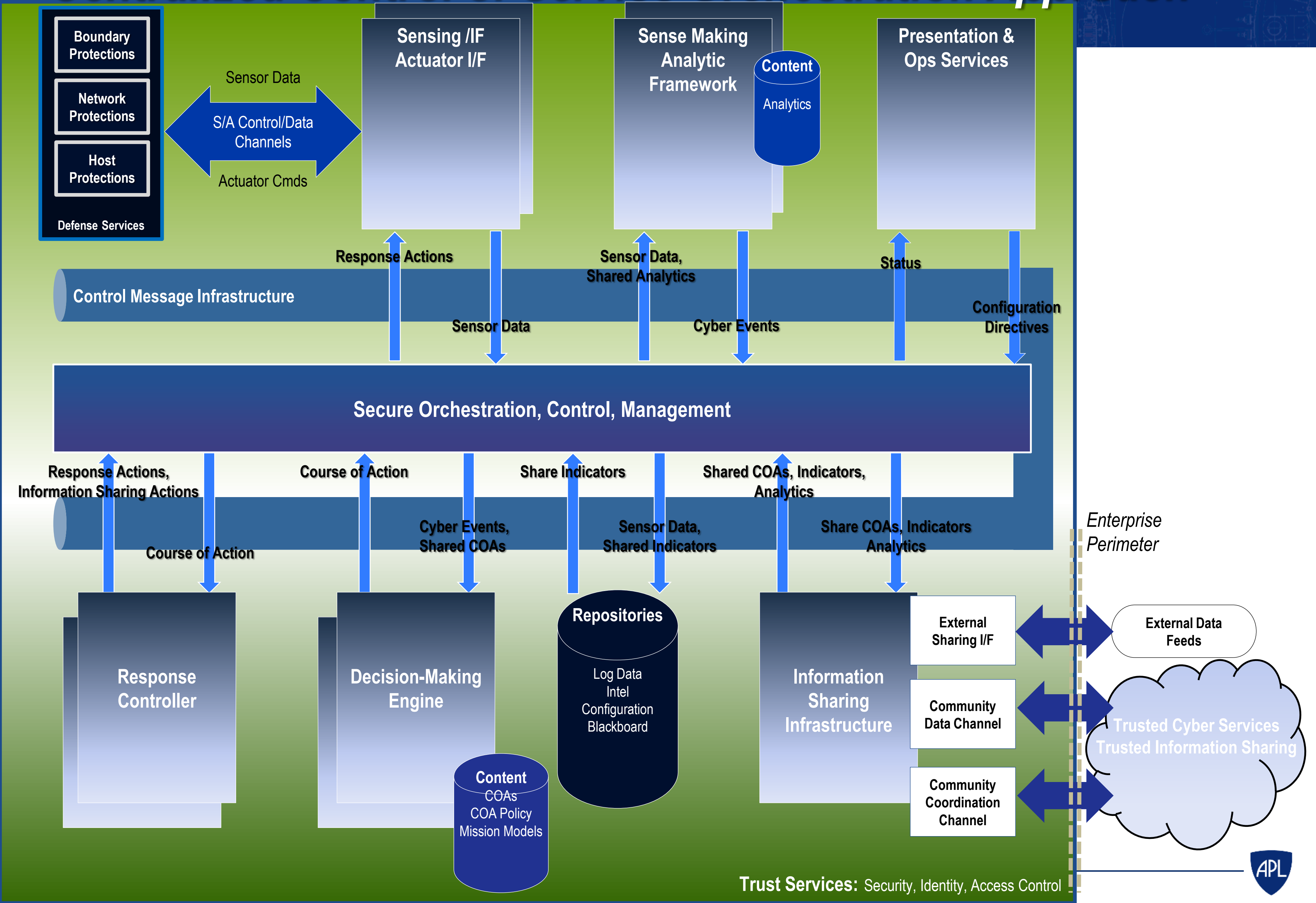
National/Global: NCCIC, GEOC, National Cyber Centers

Regional: Sectors, EOCs, Communities

Local: Enterprise, D/A, CIKR, B/P/C

Messaging View

Centralized Control of Service Orchestration Approach



Boundary Protections

Network Protections

Host Protections

Defense Services

Sensor Data

S/A Control/Data Channels

Actuator Cmds

Sensing /IF Actuator I/F

Sense Making Analytic Framework

Content

Analytics

Presentation & Ops Services

Response Actions

Sensor Data

Sensor Data, Shared Analytics

Cyber Events

Status

Configuration Directives

Control Message Infrastructure

Secure Orchestration, Control, Management

Response Actions, Information Sharing Actions

Course of Action

Course of Action

Cyber Events, Shared COAs

Share Indicators

Sensor Data, Shared Indicators

Shared COAs, Indicators, Analytics

Share COAs, Indicators Analytics

Response Controller

Decision-Making Engine

Content

COAs

COA Policy

Mission Models

Repositories

Log Data

Intel

Configuration

Blackboard

Information Sharing Infrastructure

External Sharing I/F

Community Data Channel

Community Coordination Channel

Enterprise Perimeter

External Data Feeds

Trusted Cyber Services

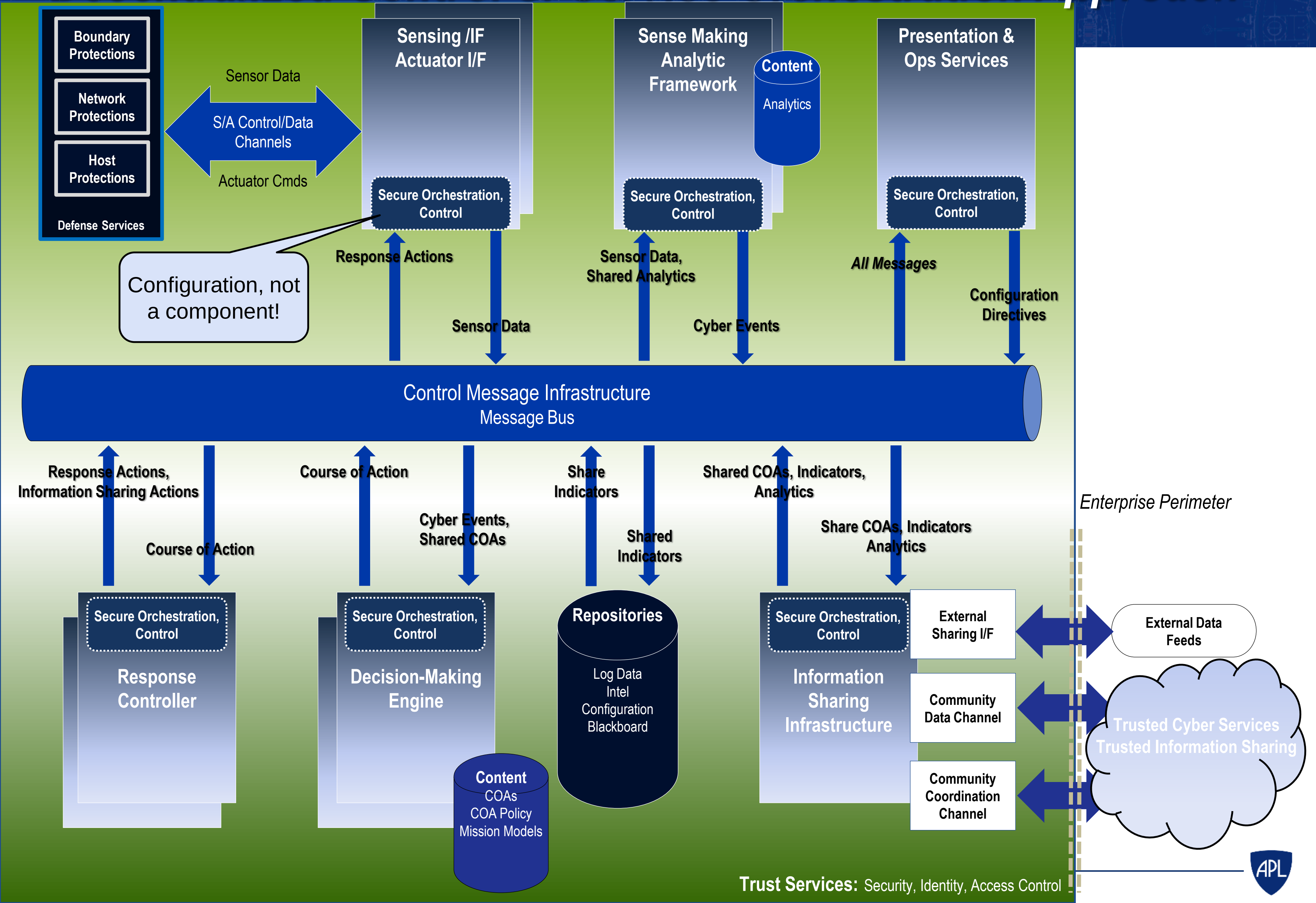
Trusted Information Sharing

Trust Services: Security, Identity, Access Control

APL

Messaging View

Decentralized Control of Service Orchestration Approach



Boundary Protections

Network Protections

Host Protections

Defense Services

Sensor Data

S/A Control/Data Channels

Actuator Cmds

Sensing /IF Actuator I/F

Secure Orchestration, Control

Sense Making Analytic Framework

Content

Analytics

Secure Orchestration, Control

Presentation & Ops Services

Secure Orchestration, Control

Configuration, not a component!

Response Actions

Sensor Data

Sensor Data, Shared Analytics

Cyber Events

All Messages

Configuration Directives

Control Message Infrastructure

Message Bus

Response Actions, Information Sharing Actions

Course of Action

Course of Action

Cyber Events, Shared COAs

Share Indicators

Shared Indicators

Shared COAs, Indicators, Analytics

Share COAs, Indicators Analytics

Enterprise Perimeter

Secure Orchestration, Control

Response Controller

Secure Orchestration, Control

Decision-Making Engine

Content

COAs

COA Policy

Mission Models

Repositories

Log Data

Intel

Configuration

Blackboard

Secure Orchestration, Control

Information Sharing Infrastructure

External Sharing I/F

Community Data Channel

Community Coordination Channel

External Data Feeds

Trusted Cyber Services

Trusted Information Sharing

Trust Services: Security, Identity, Access Control

Centralized vs. Decentralized (Hypotheses)

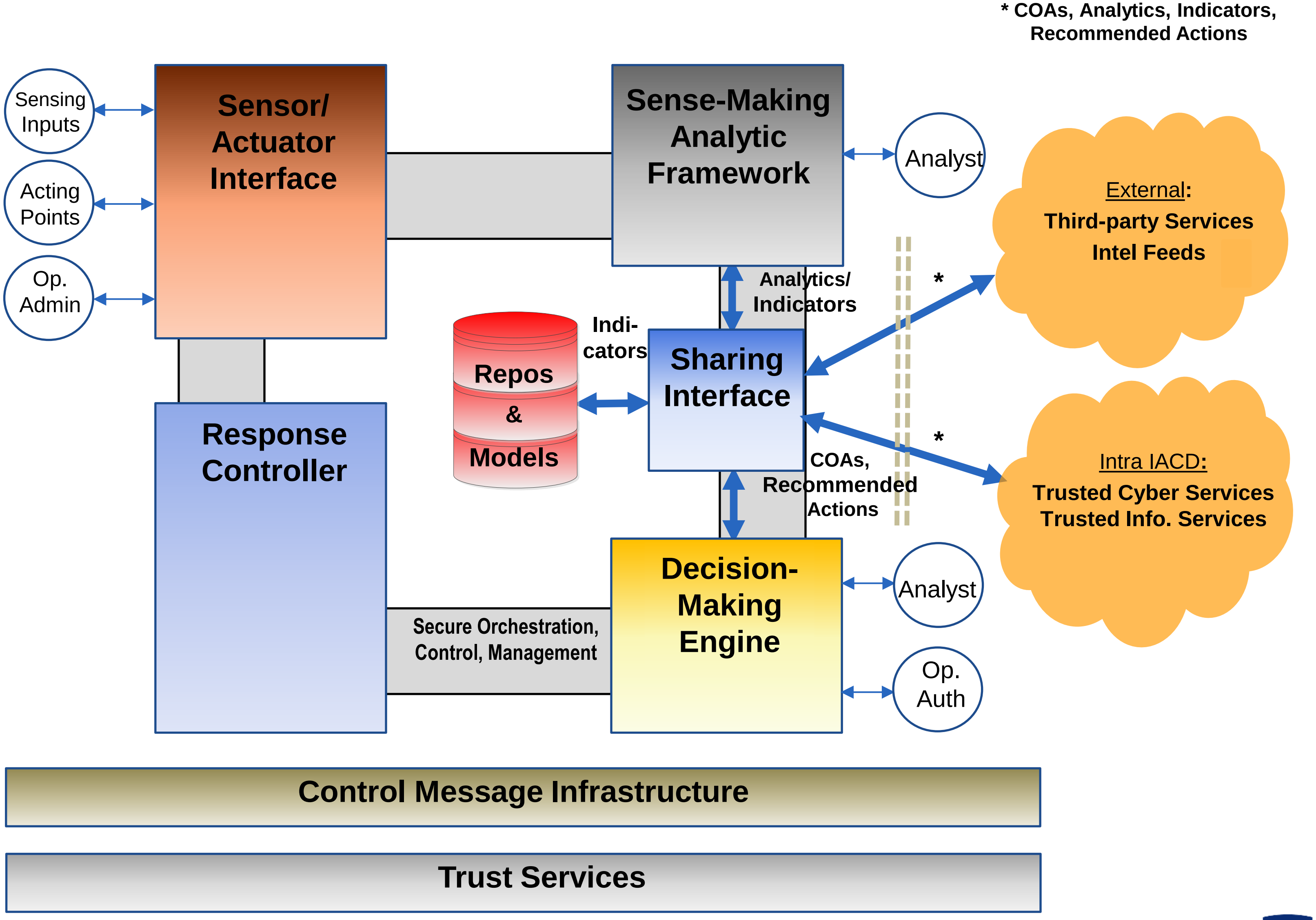
Centralized

- **Advantages**
  - Control logic easily managed in one component
  - Existing Orchestrator products satisfy functionality
  - Central point of management
- **Disadvantages**
  - Potential bottleneck or resource exhaustion at centralized coordinator
  - New services require additional logic in centralized coordinator

Decentralized

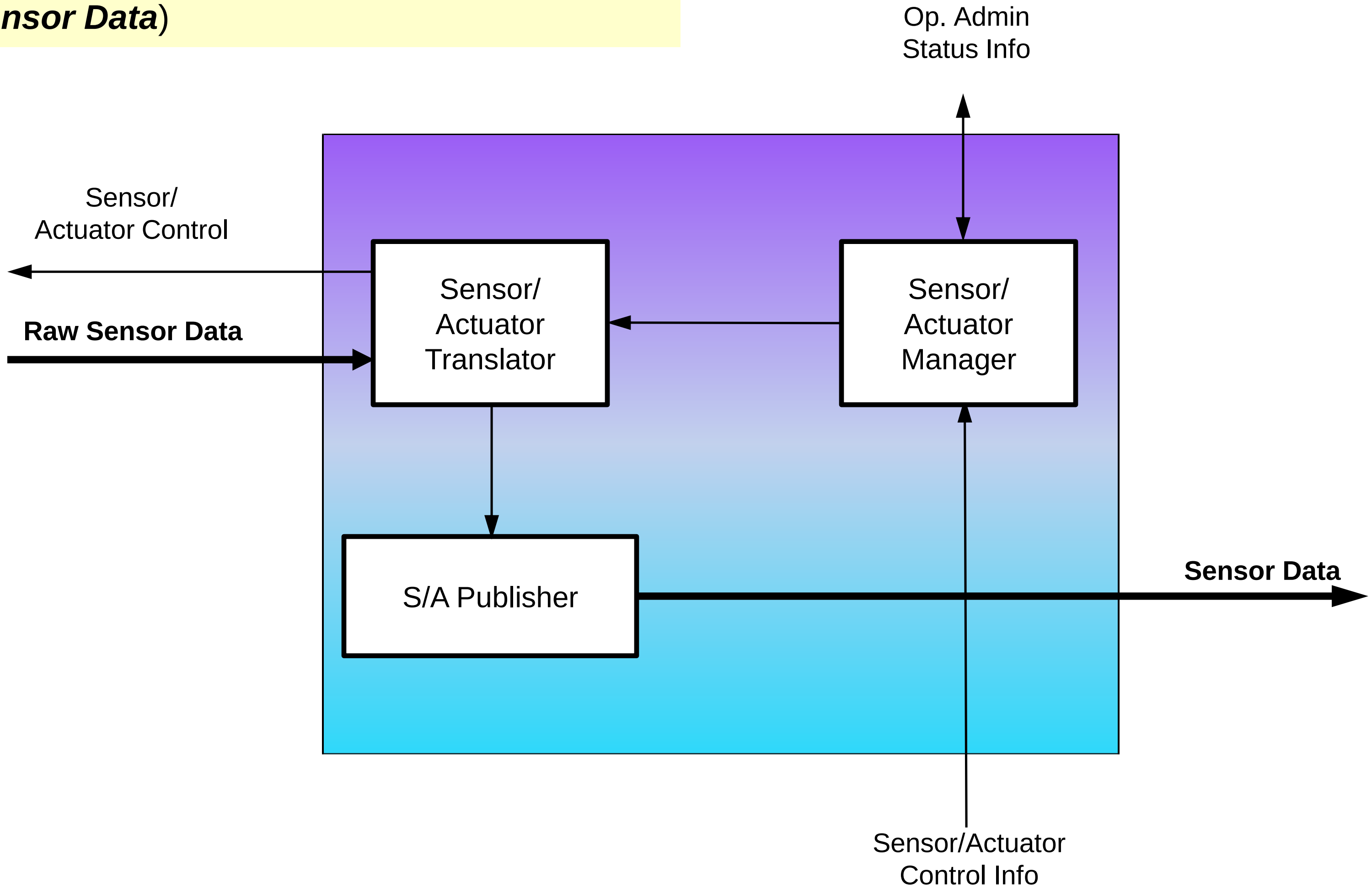
- **Advantages**
  - Scalability – replicate stateless components to increase capacity
  - Extensibility – add new components as data producers or consumers
- **Disadvantage**
  - Management, debugging challenges
  - Control Message Infrastructure must be high performance – all logic at the data consumers

Functional View
Information Sharing


* COAs, Analytics, Indicators, Recommended Actions
Sensing Inputs
Acting Points
Op. Admin
Sensor/ Actuator Interface
Sense-Making Analytic Framework
Analyst
External: Third-party Services Intel Feeds
Analytics/ Indicators
*
Indi- cators
Repos & Models
Sharing Interface
*
COAs, Recommended Actions
Intra IACD: Trusted Cyber Services Trusted Info. Services
Response Controller
Secure Orchestration, Control, Management
Decision-Making Engine
Analyst
Op. Auth
Control Message Infrastructure
Trust Services

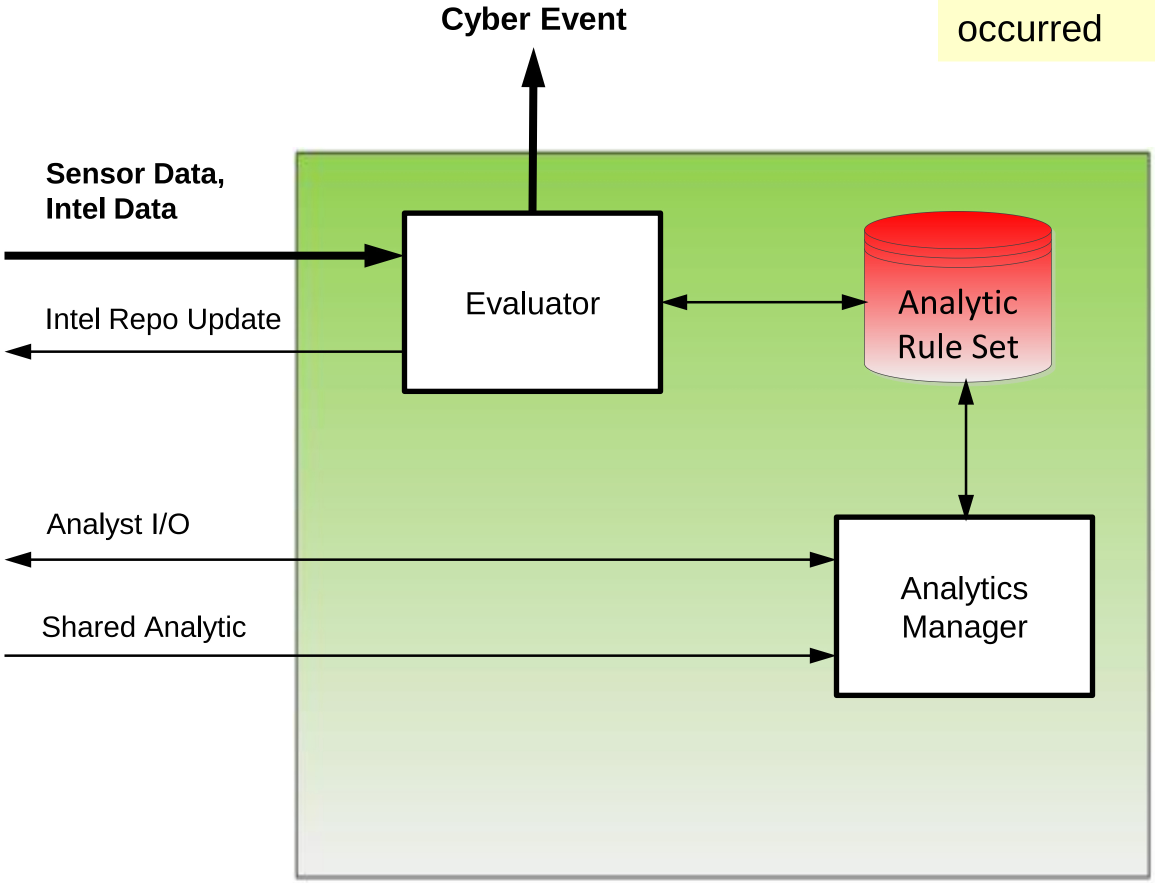
Functional View
Sensor Actuator Interface

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



Functional View
Sense Making Analytic Framework

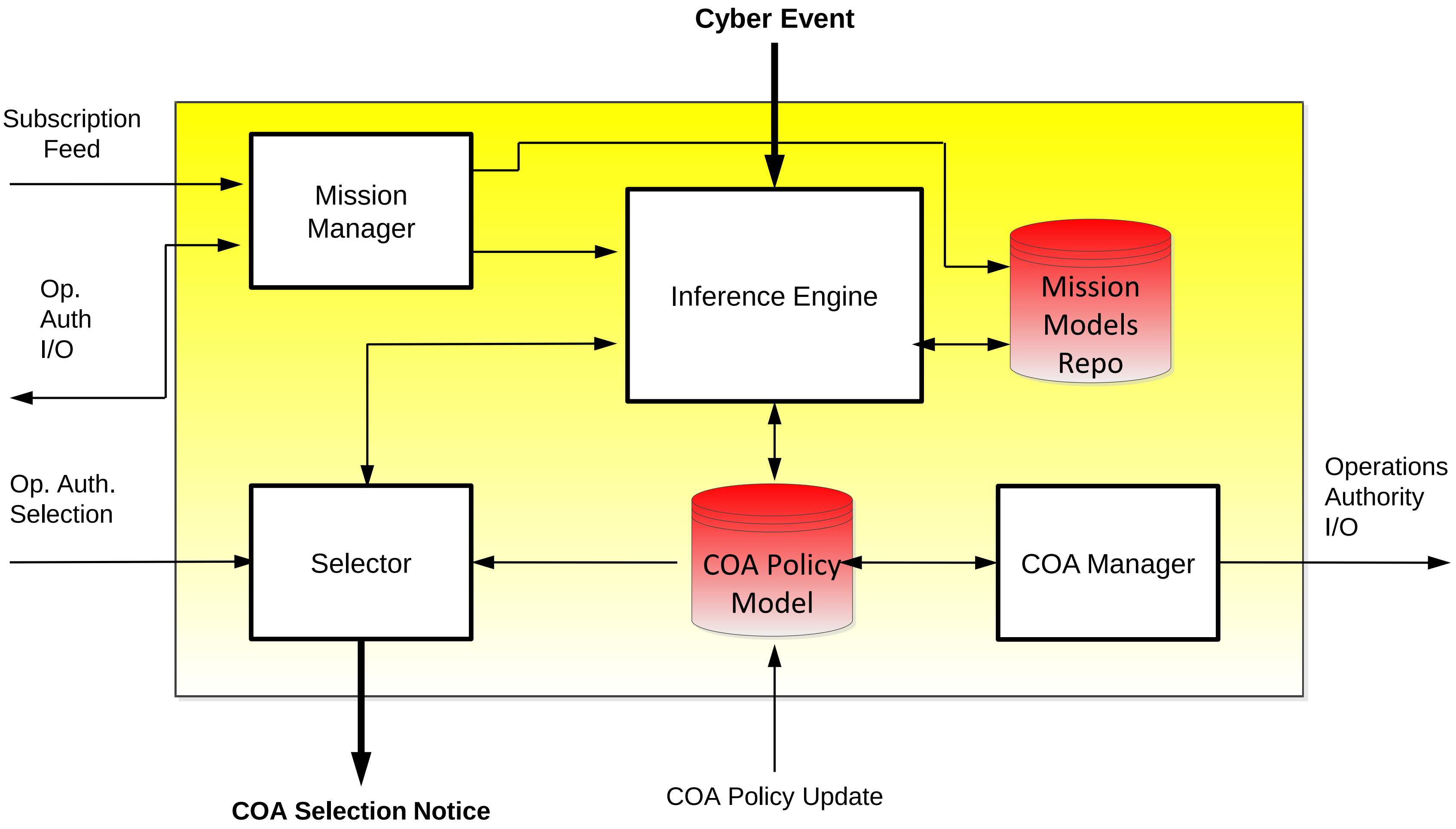
Evaluators use analytics to assess ***Sensor Data*** against ***Intel Data***, determine if a ***Cyber Event*** has occurred



Functional View

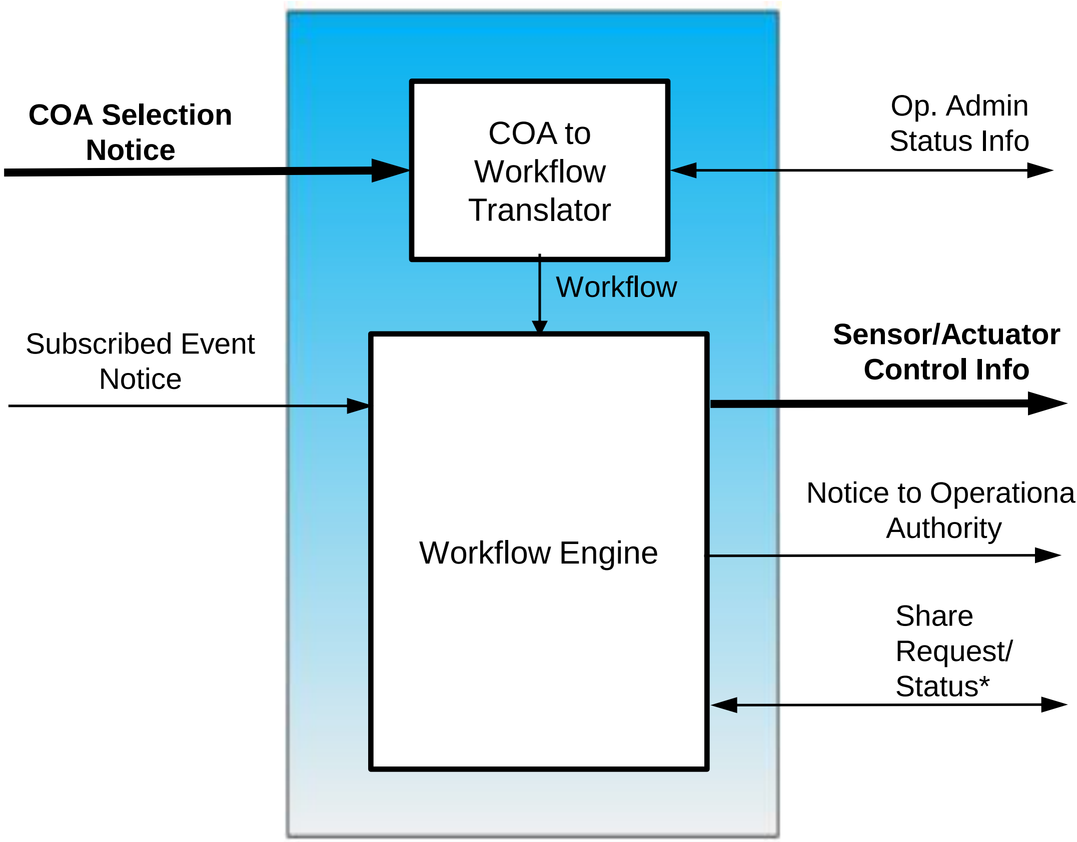
Decision-Making Engine

Given a ***Cyber Event***, DM-Engine determines a course of action (***COA***) to minimize risk while considering mission impact of the alternative COAs



Functional View
Response Action Controller

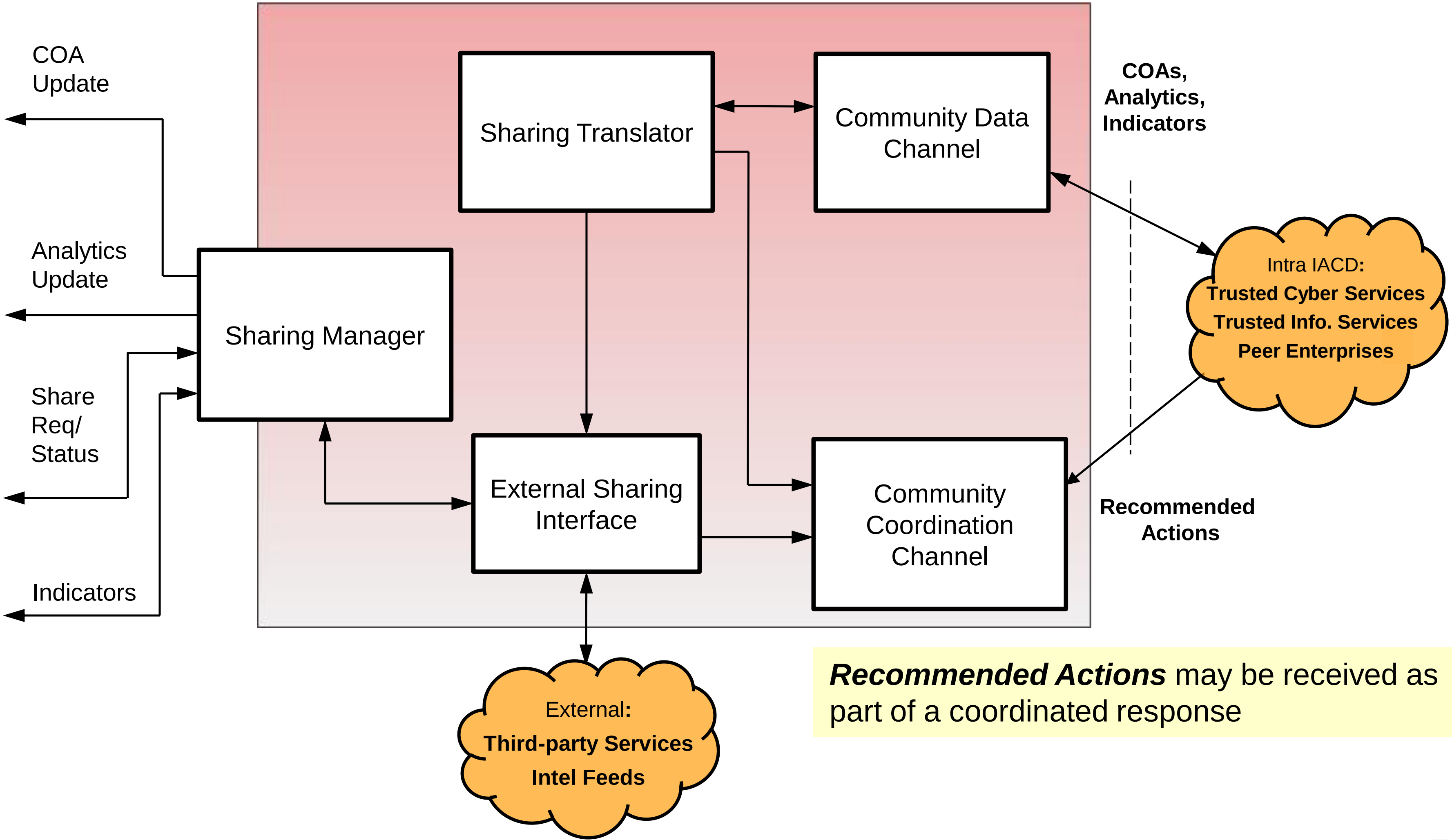
Selected COAs ***(COA Selection Notice*****),** with parameters for targets and other options, converted to specific ***Workflow***s containing ***Sensor/Actuator Control Info*** for execution



* Incoming status includes Tip/Event/COA sharing notice

Functional View
Sharing Interface

COAs, ***Analytics***, and ***Indicators*** may be received from the community or shared with the community



Recommended Actions may be received as part of a coordinated response

Work To Date

- **Partially completed the architecture views presented in this briefing**
- **Completed detailed Functional Decomposition**
- **Assessed the architecture against representative use cases**
- **Executed four spirals to demonstrate the concept feasibility by integrating commercial products:**
  - **Spiral 0: Auto-enrichment of troubleshooting and analyst activity; detection and mitigation of malware**
  - **Spiral 1: Generation of indicators and tips for sharing, and direction to other enterprises; indicators and tips received from external source and initiation of IACD response**
  - **Spiral 2: Indicators and tips received from external source and initiation of IACD response**
  - **Spiral 3: Sharing COAs between enterprises**

Next Steps

- **Product Vendors:**
  - We need your feedback on the reference architecture!
  - We need your help to develop the open interface and interoperability specifications

- **Potential Adopters:**
  - We need your feedback on the reference architecture!
  - Use cases for your environment, including mobility, managed service consumers, industrial control systems, and geographically distributed networks

- **The IACD Challenge:**
  - We are looking for vendors and integrators to instantiate some or all of the architecture and demonstrate the capabilities
  - Opportunity to demonstrate the results at a future Community Day event:

- https://secwww.jhuapl.edu/iacdcommunityday/

Conclusions

- IACD focuses on cyber defense information sharing, automation, and interoperability
- Reference Architecture serves as a framework for vendors and adopters to complete the interface definitions required for interoperable solutions
- Prior spiral demonstrations have shown the feasibility and benefits of security automation
- The next steps require support from industry to define the interfaces and messages that will enable interoperability

APL

JOHNS HOPKINS

APPLIED PHYSICS LABORATORY