OpenC2

AN UPDATE FOR THE IACD COMMUNITY

David Lemire

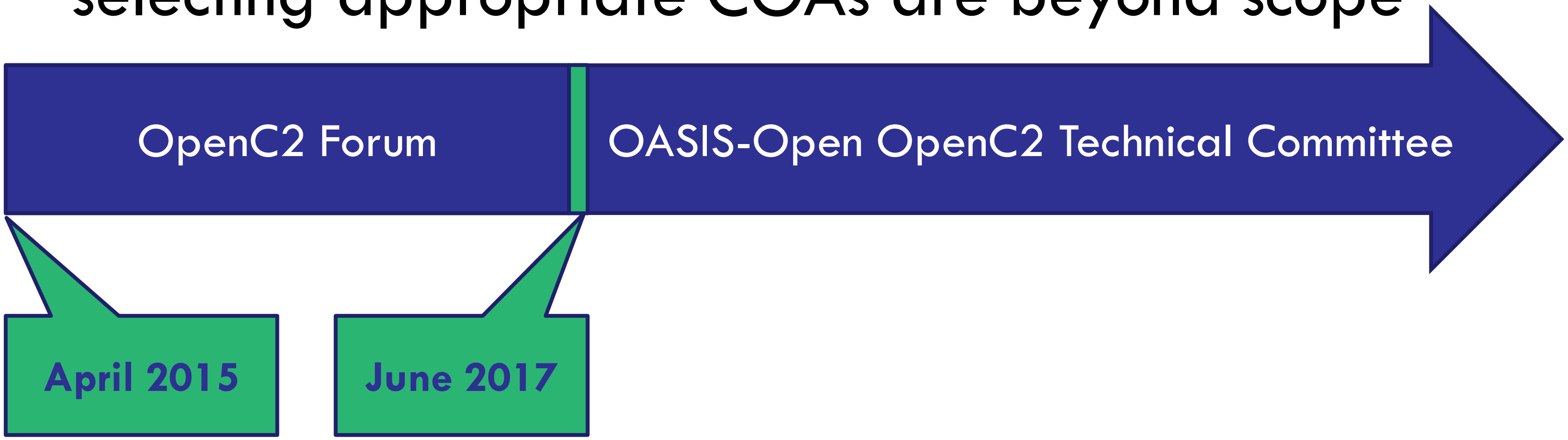
Secretary,

OASIS OpenC2 TC

October 3, 2018

OpenC2: A Quick Summary

- □ Concise extensible language to enable C2 cyber defense components, subsystems and/or systems
- □ Agnostic of the underlying products, technologies, transport mechanisms
- □ Other aspects such as sensing, analytics, and selecting appropriate COAs are beyond scope



OpenC2 Forum

OASIS-Open OpenC2 Technical Committee

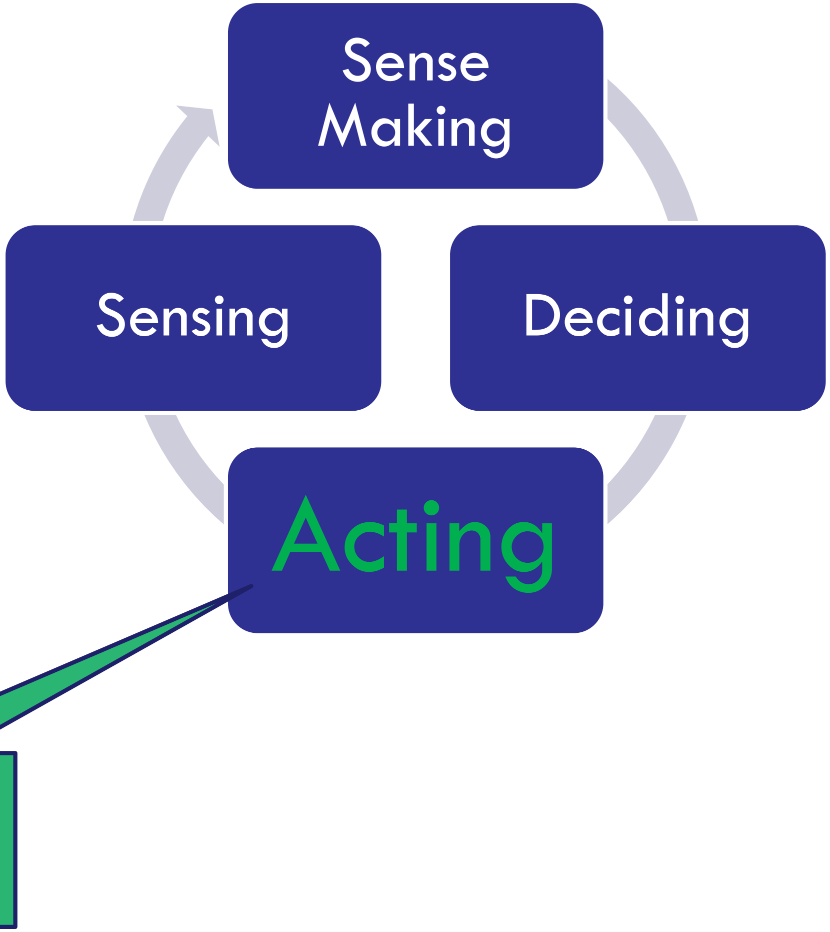
April 2015

June 2017

Clarifying Our Focus …

- OpenC2 does not:
  - Define Event or Alerts (Sensing)
  - Define sharing of indicators or threat Intelligence (Sensing)
  - Directly support conditional logic (Sense Making & decision)
  - Initiate Action based on conditional Logic (Policy Enforcement)
  - Define Courses of Action (Decision)
  - Specify protocols, Key management, etc. (Message Fabric)
- So what is OpenC2 doing?
  - Converging on a common language for C2
  - Defining Abstract Commands
    - AKA 'atomic actions', 'generic steps', 'Schema' …

In the IACD Context


Sense Making

Deciding

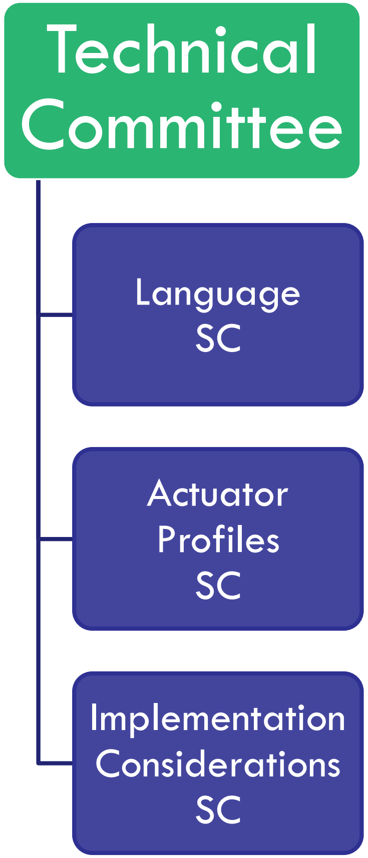
Acting

Sensing

OpenC2 Focus

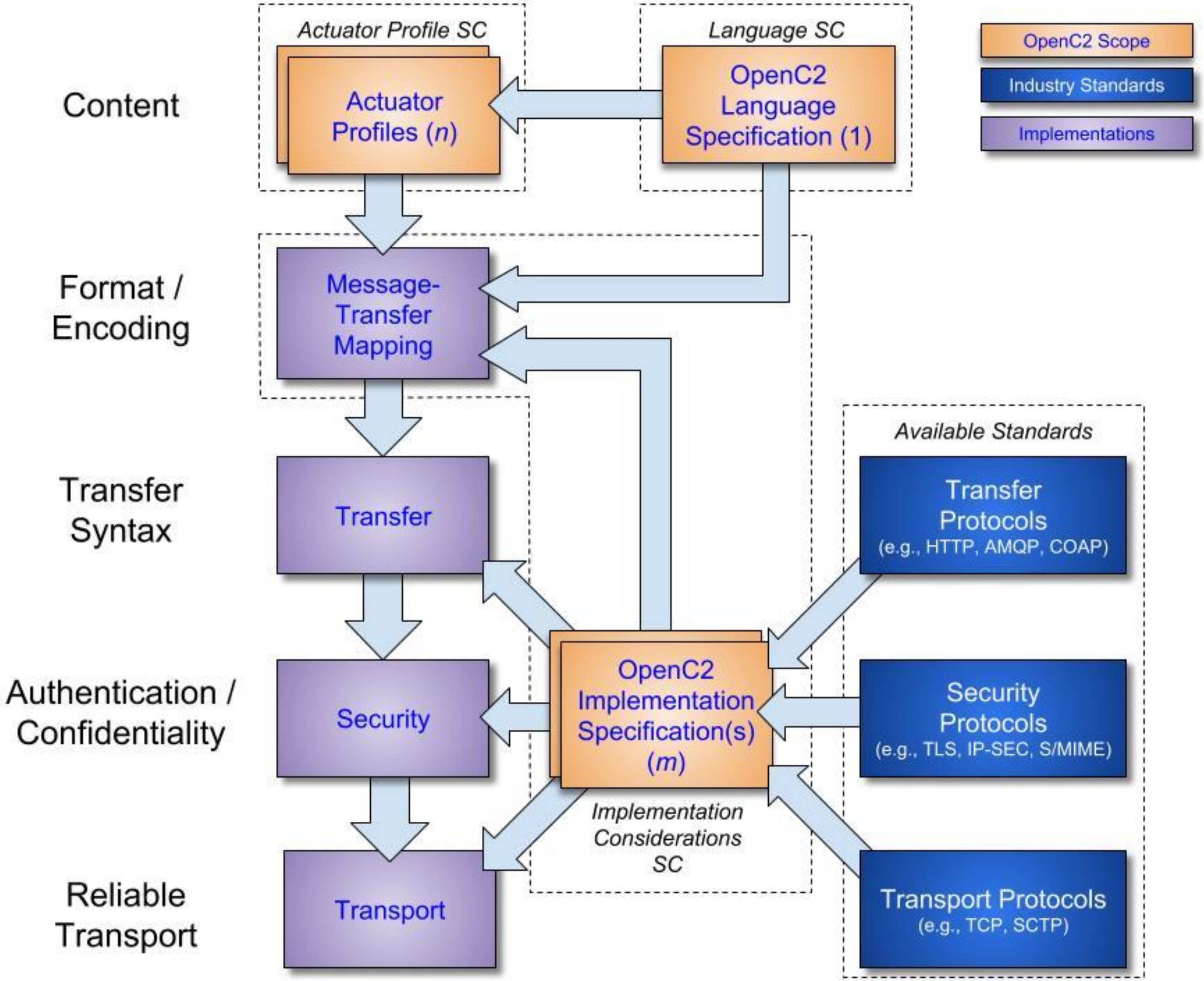
OpenC2 Subcommittee Foci

- Language Specification
  - Actions
  - Default Target namespace
  - Semantics, syntax
  - Minimum to implement
- Actuator Profiles
  - Scope and applicability
  - Required and optional Action/Target Pairs in the context of the specific Actuator
  - Specifiers and options for a class of actuators
- Implementation Guides
  - All other integration aspects (e.g., Transfer Specs)
  - Use of other standards to address 'External Dependencies'



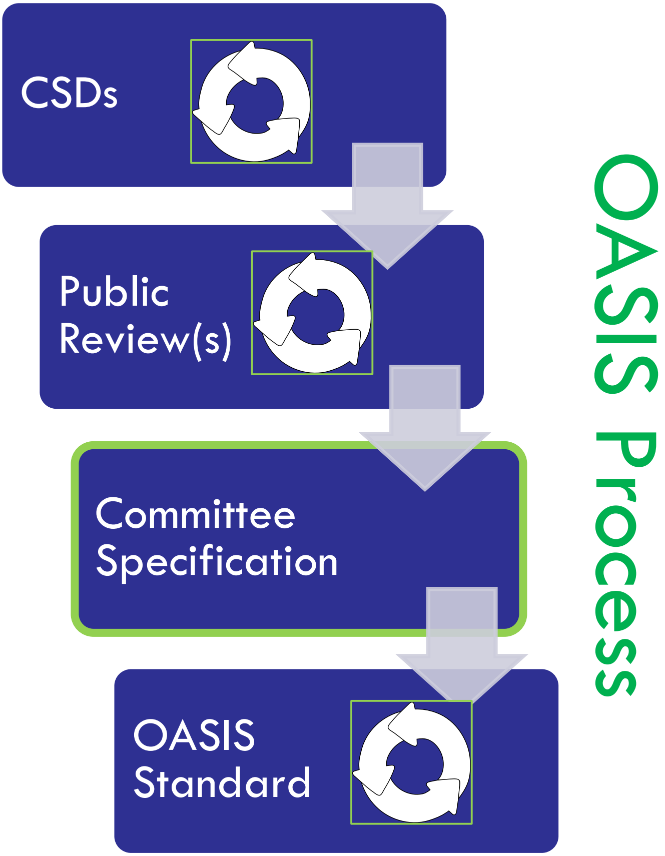
OpenC2 is not 'A' specification; It is a Suite

Connecting All Of The Pieces


Actuator Profile SC
Language SC
OpenC2 Scope
Industry Standards
Implementations
Content
Actuator Profiles (*n*)
OpenC2 Language Specification (1)
Format / Encoding
Message-Transfer Mapping
Transfer Syntax
Transfer
Available Standards
Transfer Protocols (e.g., HTTP, AMQP, COAP)
Authentication / Confidentiality
Security
OpenC2 Implementation Specification(s) (*m*)
Security Protocols (e.g., TLS, IP-SEC, S/MIME)
Implementation Considerations SC
Reliable Transport
Transport
Transport Protocols (e.g., TCP, SCTP)

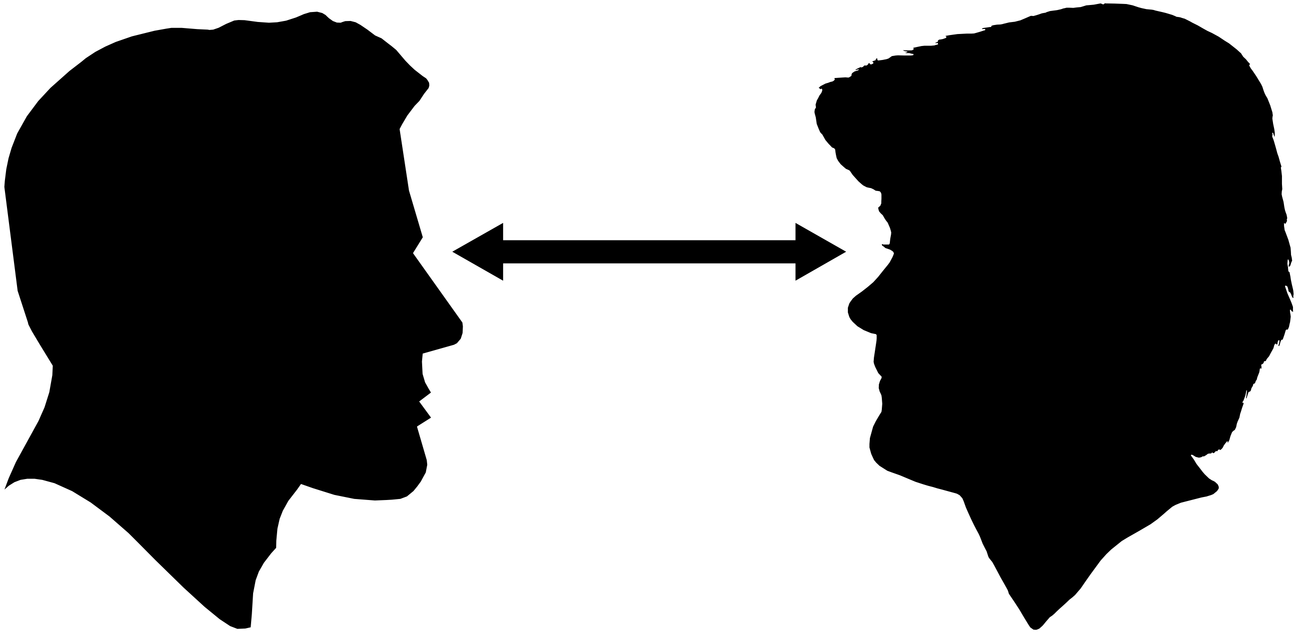
Specifications Progress

- Language SC
  - Technical Committee has accepted the Language Specification as CSD 5.0
  - Ballot for next CSD imminent
- Actuator Profile SC
  - Technical Committee has accepted the Stateless Packet Filter Profile as CSD 2.0
  - Ballet for next CSD underway
- Implementation Considerations
  - Technical Committee has accepted the HTTPS Transfer Specification as CSD 1.0
  - Ballot for next CSD underway



Goal: Release for Public Review by late October

Just This Week



OpenC2 Face-to-Face Meeting

End State: OpenC2 Enabled Enterprise

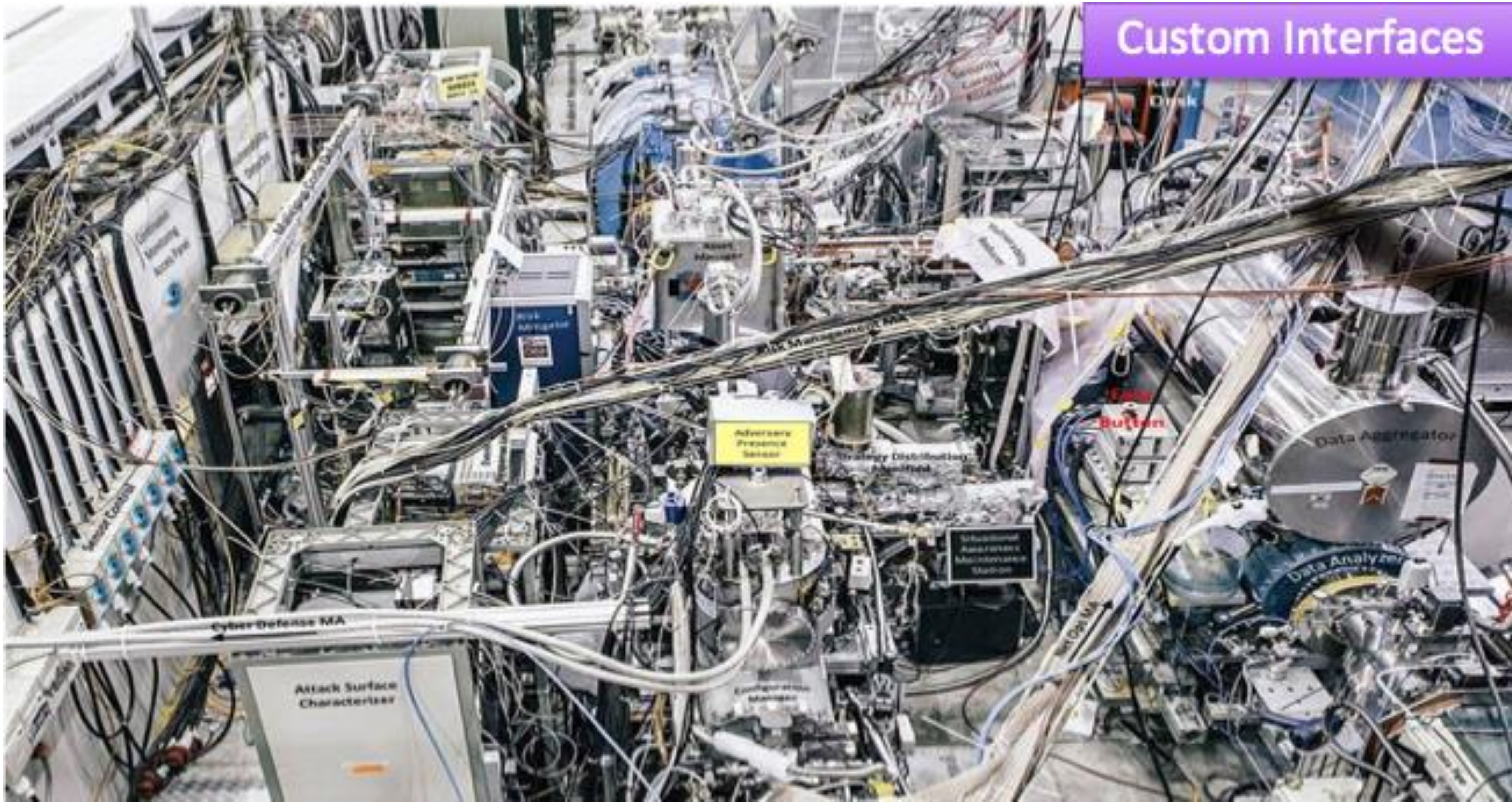
- Enterprise Owner: RFP language:
  - …'Complies with OpenC2 specifications'
  - … 'micro-satellite formation fliers utilizing COAP'
  - … 'ground segment logically separates…'
- Vendors: Implement one or more 'Actuator Profiles'
- Integrators: Select appropriate Implementation Specification and cyber defense components.

Backups

Making it Real:

- JCAUS Prototype Effort
  - ~ 200 unmanned platforms on a star
  - KMIP Transport Specification
  - Joint NSA and Draper Laboratories
- Lycan Series
  - Translation of OpenC2 JSON to objects and back
  - Python, Java and BEAM
  - Maintained by AT&T and s-fractal
- OCAS
  - Simulator to validate and verify OpenC2 interface
  - Maintained by S-fractal

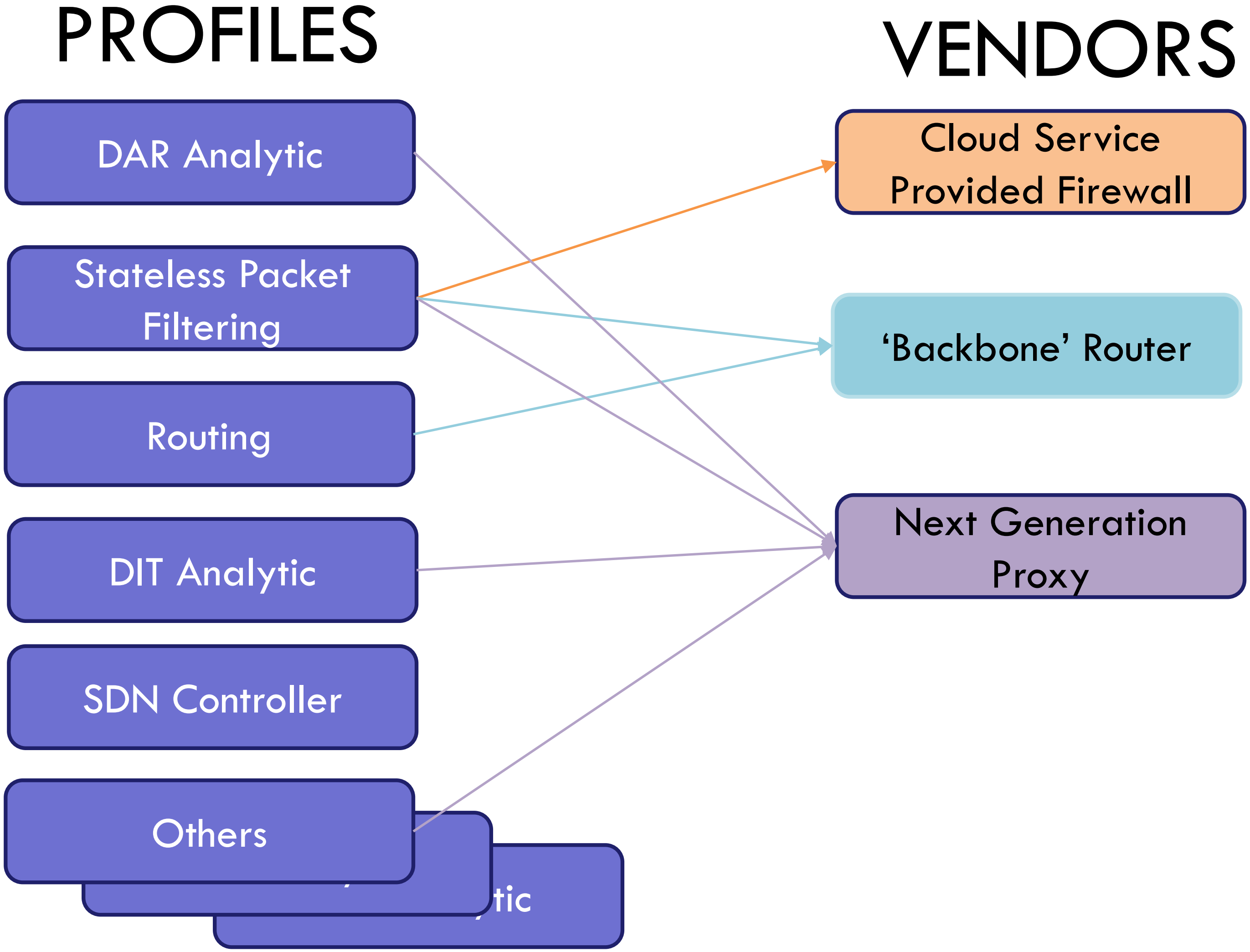
Integration in the Absence of Standards



Custom Interfaces

Risk Mitigator
Risk Management MA
Adversary Presence Sensor
Strategy Distribution Manifold
Situational Awareness Maintenance Station
Button
Data Aggregator
Data Analyzer
Cyber Defense MA
Attack Surface Characterizer
Configuration Manager

Scope (Vendors point of view)



PROFILES

VENDORS

DAR Analytic

Stateless Packet Filtering

Routing

DIT Analytic

SDN Controller

Others

tic

Cloud Service Provided Firewall

'Backbone' Router

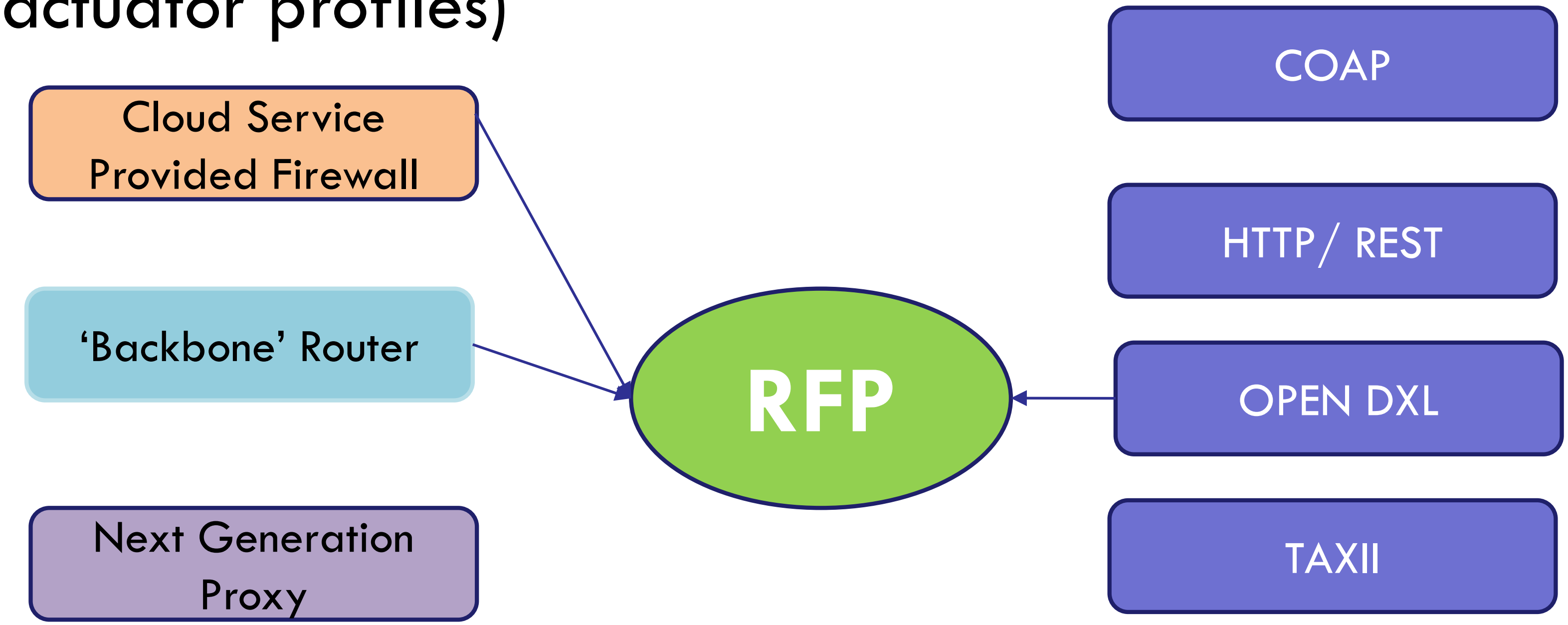
Next Generation Proxy

Scope (Integrators point of view)

PRODUCTS

(defined in terms of actuator profiles)

IMPLEMENTATION SPECIFICATIONS



Cloud Service Provided Firewall

'Backbone' Router

Next Generation Proxy

RFP

COAP

HTTP/ REST

OPEN DXL

TAXII

And more…

- Python API's
  - OpenC2 API to accept & Convert OpenC2 commands to Python
  - Yuuki and Orchid are codebase
  - Reactor Master and Reactor Relay are Deployed
  - Maintained by ElecticIQ and University of Maryland
- JADN
  - Provides abstraction that is independent of serialization
  - Unit testing, validation and serialization

Interoperability Focused

- OpenC2 Compatibility
  - Provide ‘feedback’ mechanism to Technical Committee
  - Identify ‘incompatibilities’ between implementations
  - Created by University of Maryland
- OpenC2 Serializations
  - JSON (mandatory to implement)
  - CBOR
  - Protobuf
  - XML

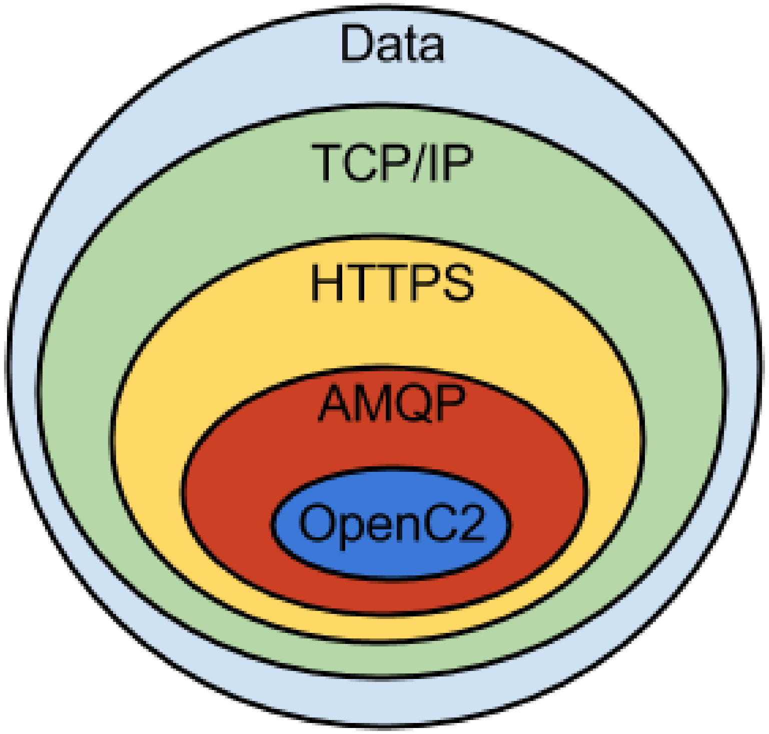
Scope of OpenC2

Defining the scope of OpenC2:

Directs assets command execution and acknowledges successes / failures.

Due to its vendor agnostic encapsulation, it can utilizes any messaging protocol over any transportation and encryption mechanisms.

It is important to note that this encapsulation method is not set in stone. Each layer can have a variety of implementations .

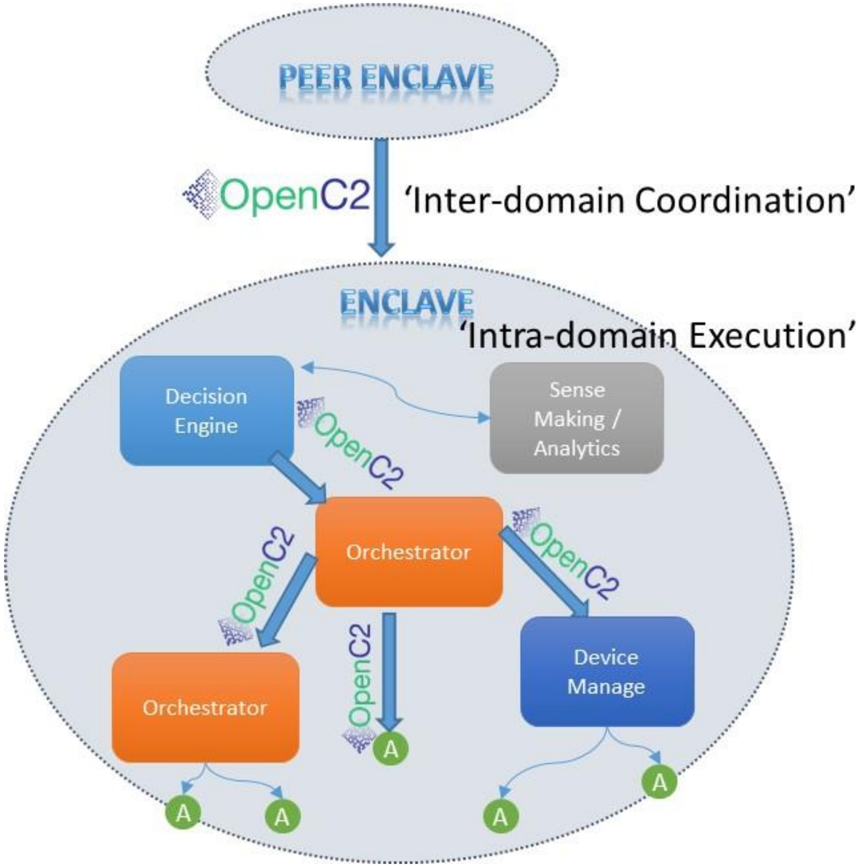


OpenC2 Considerations

- Topology
  - Star Topology with transient TLS sessions
  - Pub/sub environment
  - Ad-hoc/ mobile networks
- Transport considerations
  - REST API or Remote Procedure Calls?
  - Bandwidth rich or Low SNR RF environment?
  - Centrally managed or distributed Decision/ Analytics
- Scale? Trust Model? Actuator set?

OpenC2 External Dependencies

- OpenC2 is necessary but insufficient
- OpenC2 Assumes
  - Decision has been made
  - Action is warranted
  - The command can get there intact and securely.
  - Recipient is authenticated and authorized.
- OpenC2 Focuses on the ACTING portion of cyber Defense

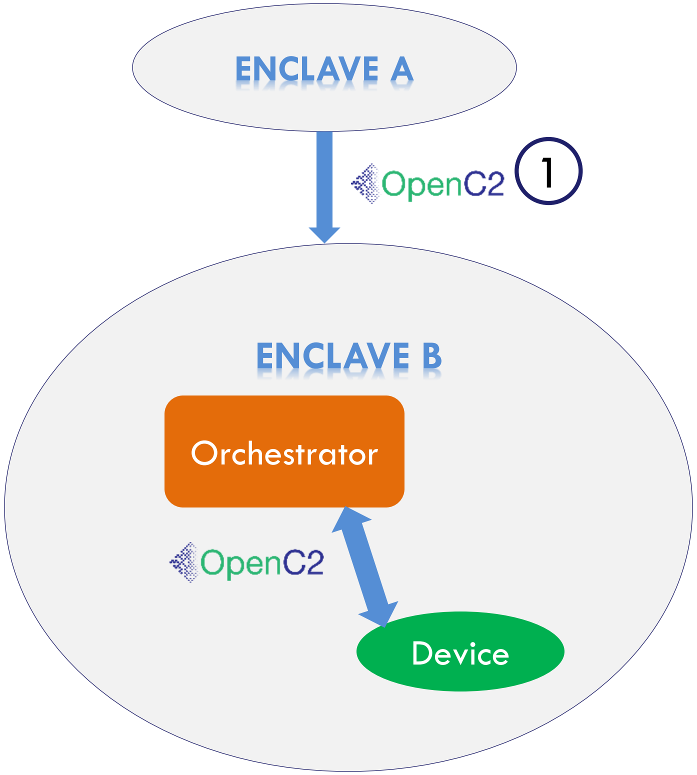


OpenC2 Implementations will FAIL without a robust means to convey commands!

OpenC2 Assurance Threats - 1

① Threats against Inter-enclave C2 – an actor may:

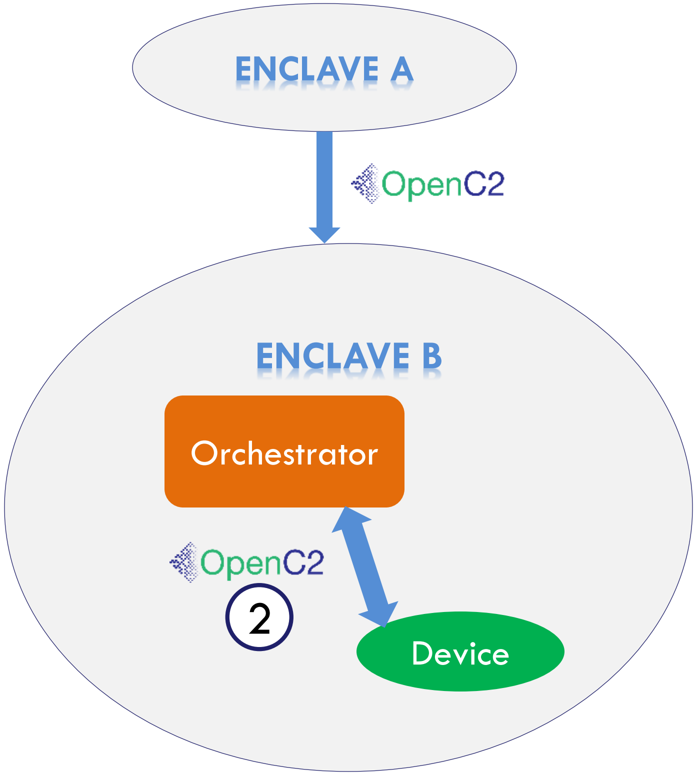
- alter C2 message to degrade or halt defensive responses,
- send spoofed commands to open up enclave B to attack,
- view C2 traffic to gain warning of defensive responses,
- Disrupt network services to prevent delivery of C2 messages.



OpenC2 Assurance Threats - 2

② Threats against intra-enclave C2 – an actor may:

- alter C2 messages to degrade or halt defensive responses,
- send false commands to open up an enclave for attack,
- Spoof C2 replies to disrupt defense or confuse defenders,
- Flood devices to prevent delivery of C2 messages.



What Can Go Wrong?

OpenC2 at a glance

- Focuses on ‘Response’ portion of cyber-defense
- OpenC2 assumes the following has been done:
  - Sensing; ‘What’ triggers the action
  - Analytics; ‘Why’
  - Decision; ‘Which’ action
  - Message Fabric; ‘Transport’ and ‘Assurance’
- Leverage pre-existing protocols and efforts
- Unambiguous Machine-to-Machine Communication
- Simplicity
  - Low overhead on sensor and actuator

Cyber Attacks & Defense

- Current State:
  - Global Attack Surface
  - Operating at Machine Speed
  - Statically Configured Point Defenses
- Challenge
  - Coordinated Defense in Cyber Relevant Time
- Strategy
  - Decouple Functional Blocks
  - Standardize Interfaces

OpenC2 Focuses on ‘Acting’

- STIX
  - Standard Threat INTEL object
  - Supports Analysis
- TAXII
  - Standard Transport protocol
  - Supports Secure Exchange
- OpenC2
  - Standard Command Language
  - Supports Acting/ Response

OpenC2 is part of a Suite of OASIS Standards