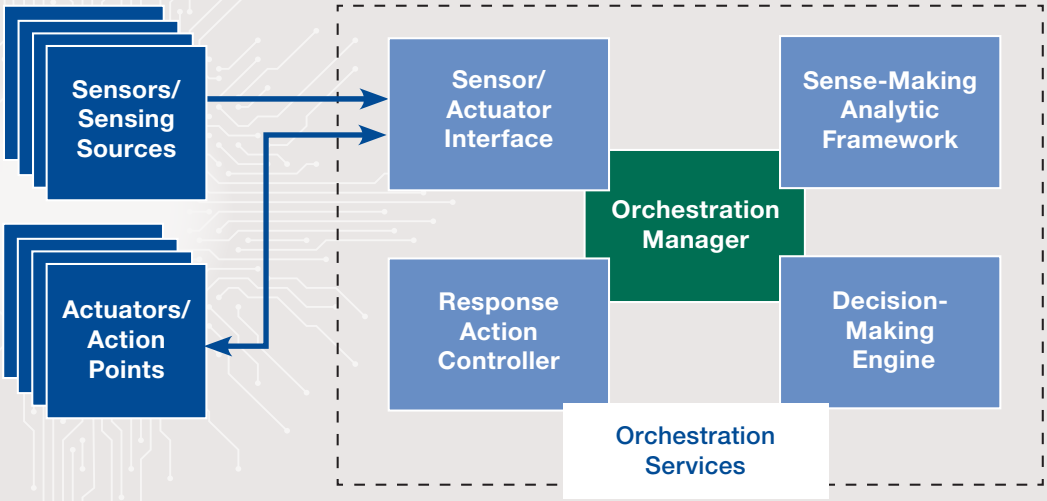
IACD Baseline Architecture

Derived from the OODA (Observe–Orient–Decide–Act) Loop, the IACD architecture has evolved into a framework that is composed of sensors bringing in shared and trusted information to trigger the Orchestration Services to act in response to cyber events.



Components Definitions

Sensors/Sensing Sources – The sensors receive and send data to the Orchestration Service.

Actuators/Action Points – The actuators perform the actions in response to a cyber event.

Sensor/Actuator Interface (S/A Interface) – The S/A interface enables communication with heterogeneous collections of sensors and actuators within an enterprise.

Sense-Making Analytic Framework (SMAF) – The SMAF further enriches the information.

Decision-Making Engine (DME) – The DME will determine what course of action (COA) is appropriate.

Response Action Controller (RAC) – The RAC will translate the COA into a sequence of response actions.

Orchestration Manager (OM) – The OM coordinates the flow of information and control across the Orchestration Services.

Orchestration Services – Orchestration Services are the collection of the five components: S/A Interface, SMAF, DME, RAC, and OM.

http:// https://secwww.jhuapl.edu/iacd @IACD_automate https://www.linkedin.com/groups/8608114 icd@jhuapl.edu