



NAVAL
POSTGRADUATE
SCHOOL

Open Architecture as an Enabler for FORCEnet

Presented by:

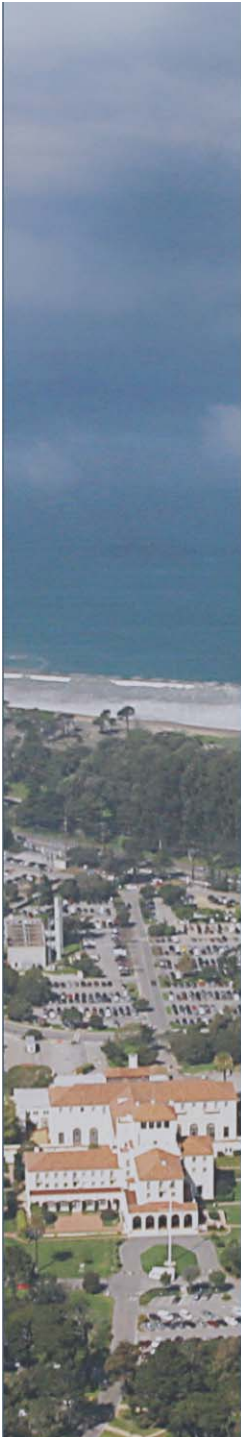
Tom Hedge

NSWC PHD San Diego

25 October 2006

The Nation's Premier Defense Research University

Monterey, California
WWW.NPS.EDU





NSWC PHD Project Team

- Viviane Deering
- Patrick Grates
- Tom Hedge
- Sein Kung
- Maria Martinez
- Percival MCarthy
- Kevin Pugh
- Sasha Radojkovic

Advisor - John M. Green, NPS



- Objectives
- Methodology
- Definitions and Models
- Battle Space
- Engagement Scenarios
- Design Principles
- Conceptual Design / Architecture
- Simulation Model
- Conclusions / Recommendations
- The Road From Here





Project Objective:

Evaluate and assess NAVSEA PEO IWS FORCEnet Open Architecture (OA) functional architecture against three (3) air defense engagement scenarios to either validate the model or identify recommended alternatives and / or improvements.

Presentation Objective:

Provide overview of project research methodology, including descriptions of models and architectural frameworks used to bound research, and present recommended model improvements.



- **Characterize the Problem / Battle Space** – identify operational environment, including actual engagement scenarios, to bound problem space
- **Formulate Design Principles** – consider operational environment & available FORCEnet / OA models and strategies in formulating principles for architecting OA system with Integrated Fire Control (IFC) capabilities
- **Develop Conceptual Design** – develop architectural framework for distributed system with automated decision aids for optimally managing warfare resources within the problem space
- **Functional Decomposition** – develop models and methods to express automated resource collaboration in the context of the FORCEnet/OA architecture domain
- **Simulation Modeling** – develop computer simulation model to assess proposed functional system architecture against the engagement scenarios
- **Analyze Simulation Results** – Assess results of simulation to determine validity of previously identified FORCEnet OA model



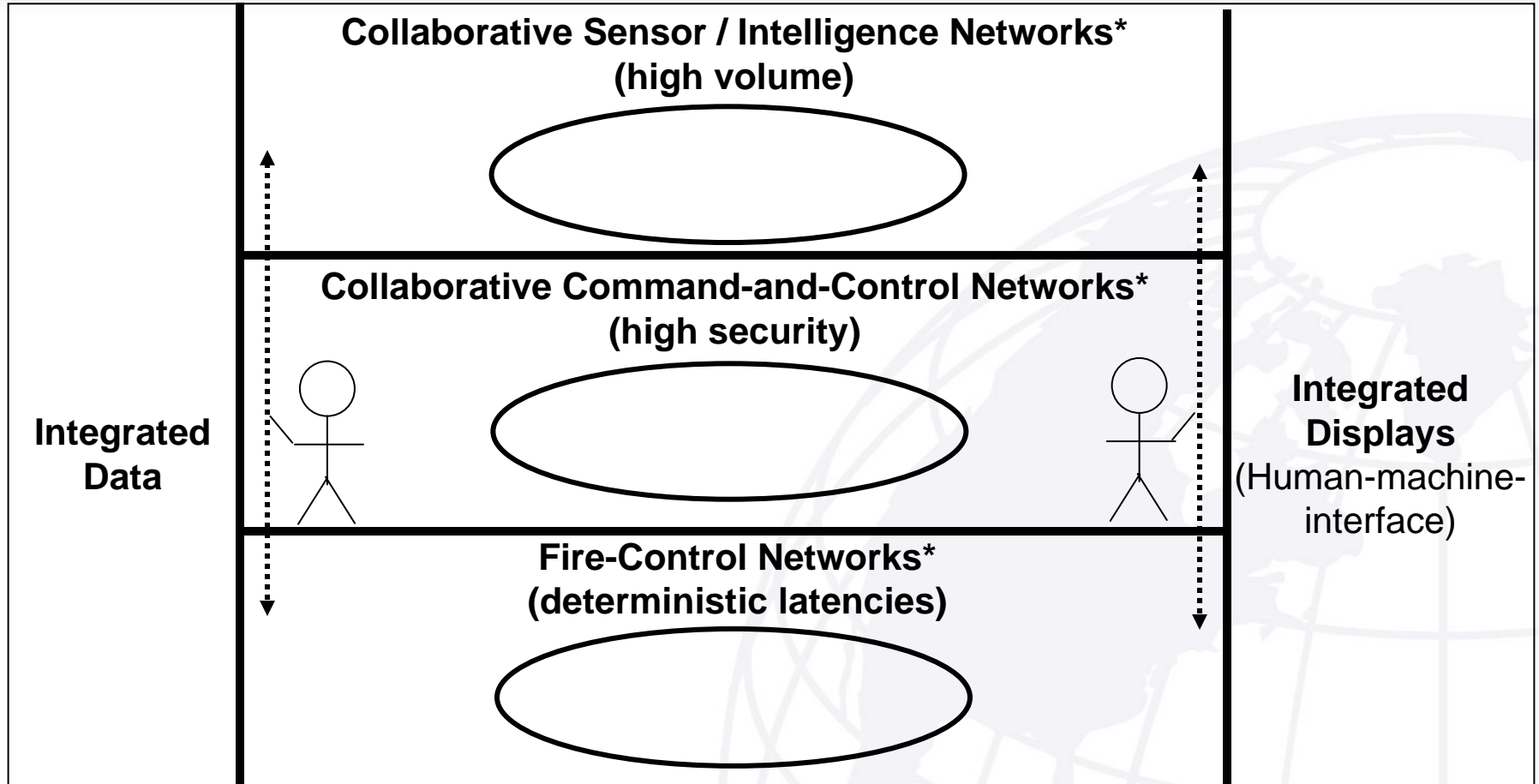
- FORCEnet: operational construct and architectural framework for naval warfare in the information age, integrating warriors, sensors, command and control, platforms, and weapons into a networked, distributed, combat force
- Open Architecture:
 - Technical and Functional Architectural
 - Interfaces at system boundaries must be described in detail using established commercial or DoD standards
 - Well-defined and easily understandable system boundaries at various levels
 - Subsystem descriptions and interface definitions capable of two or more layers of decomposition using established system engineering practices
 - *Foundation for 21st Century Combat System Designs*







- Time-Critical Targeting: ability to detect, track, engage, and assess threats having extremely limited windows of vulnerability or opportunity for detection
- Integrated Fire Control: ability of a weapon system to develop fire control solutions from information provided by one or more non-organic sensor sources, conduct engagements based on these solutions, and either provide mid-course guidance or allow this guidance to be provided by another warfare unit



FORCEnet Information Architecture



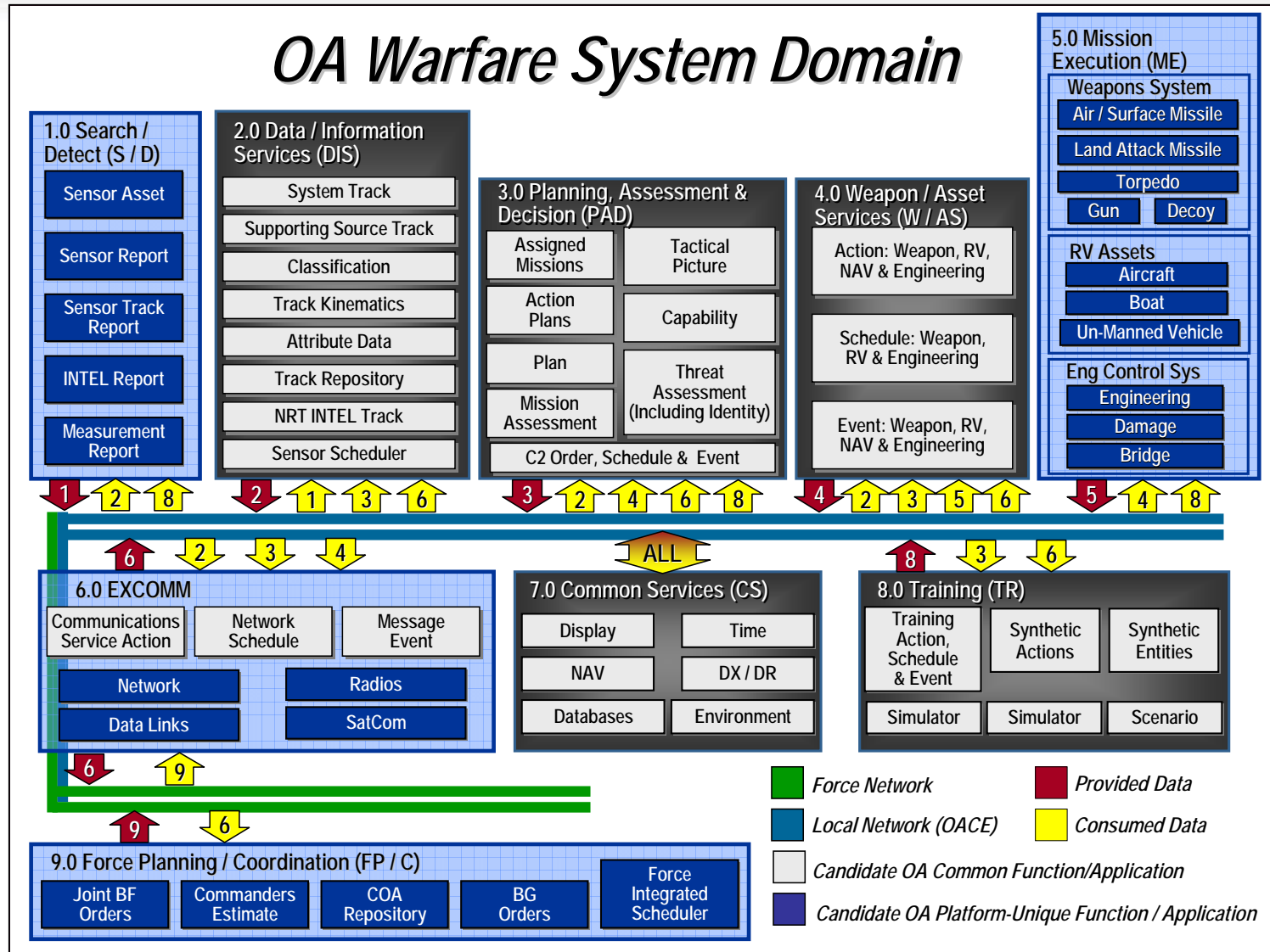
Legend:

-  Invariant architectural boundaries with network control system “throttles” to assure the metrics
-  Kill chains
-  Networks trace to communities of interest
-  Networks

Source: FORCEnet Implementation Strategy, National Research Council, 2006



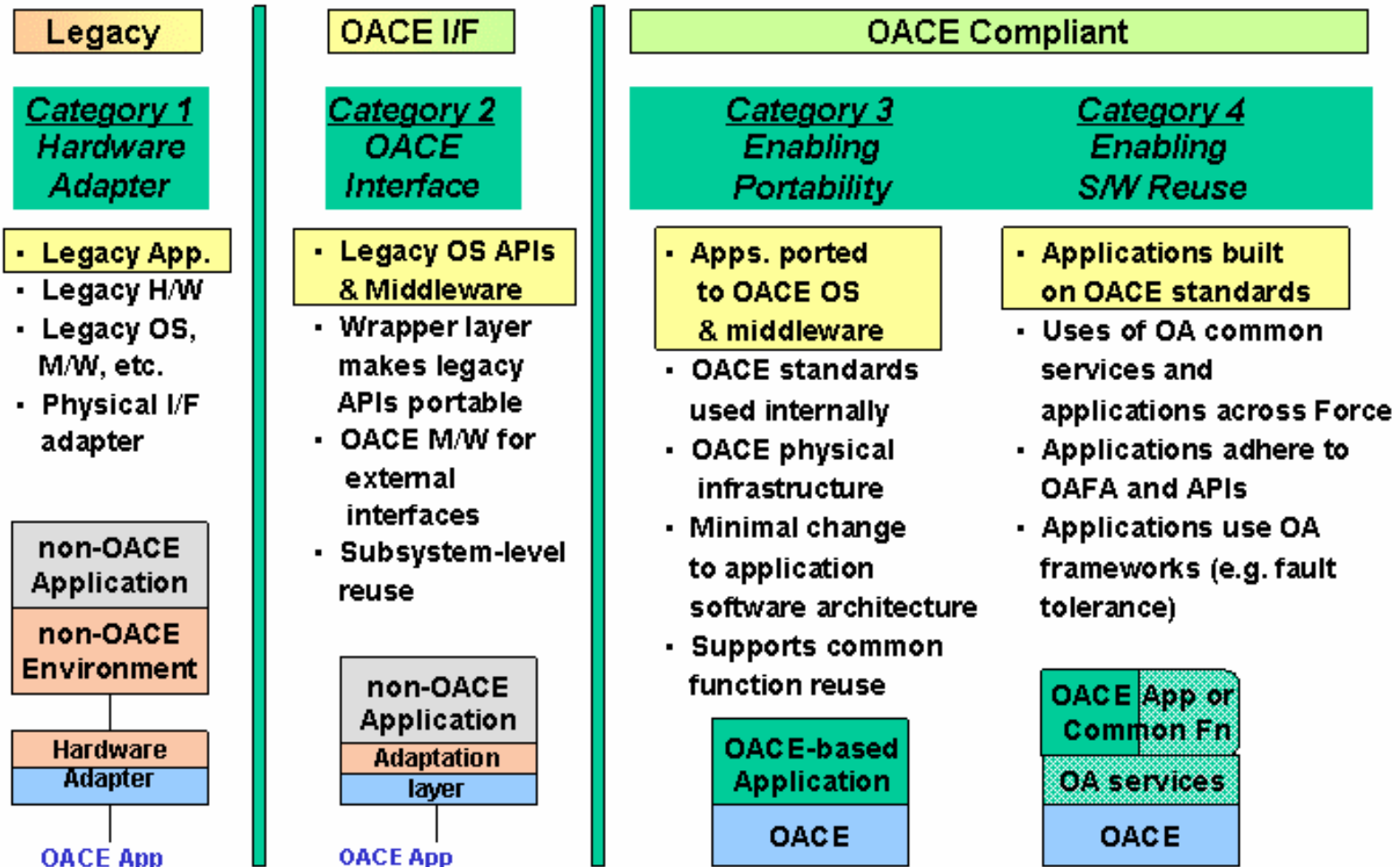
OA Warfare System Domain



Source: Combat Identification for Naval Systems in an Open Architecture, Young, 2006



Compliance Categories

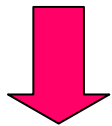
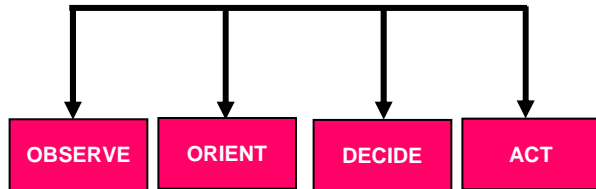


Source: OACE Technologies and Standards, NSWC, Dahlgren Division, 4 Sep 2003

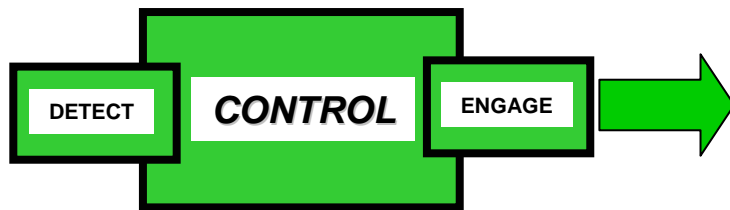


Legacy Models Considered

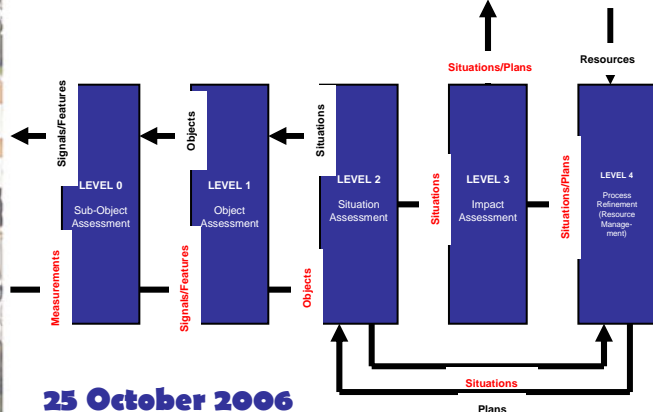
OODA Loop



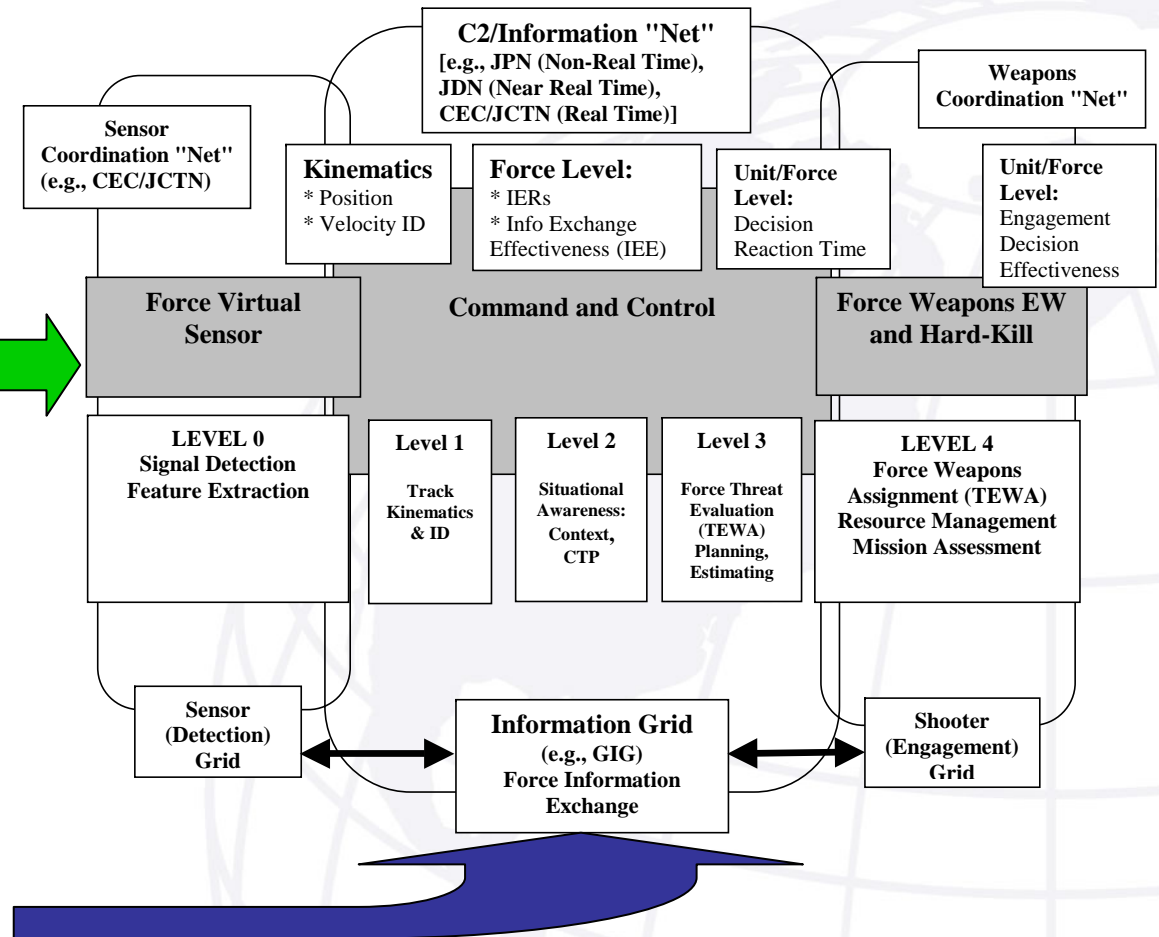
DCE Sequence



Data Fusion Model



25 October 2006



Source: A Self-Consistent Context for Unit and Force Level Tactical Decision-Making, Luessen, 2003



- Fundamental IFC System Characteristics
 - Dynamically updateable doctrine
 - Decentralized architecture and synchronized information
 - Doctrine and decision aids
- Key IFC Capability Requirements
 - Shared Situational Awareness (SA)
 - Determining best Course of Action (COA)
 - Distributed Resource Management (DRM)
 - Embedded IFC planning

Source: Integrated Fire Control for Future Aerospace Warfare, Young, 2004



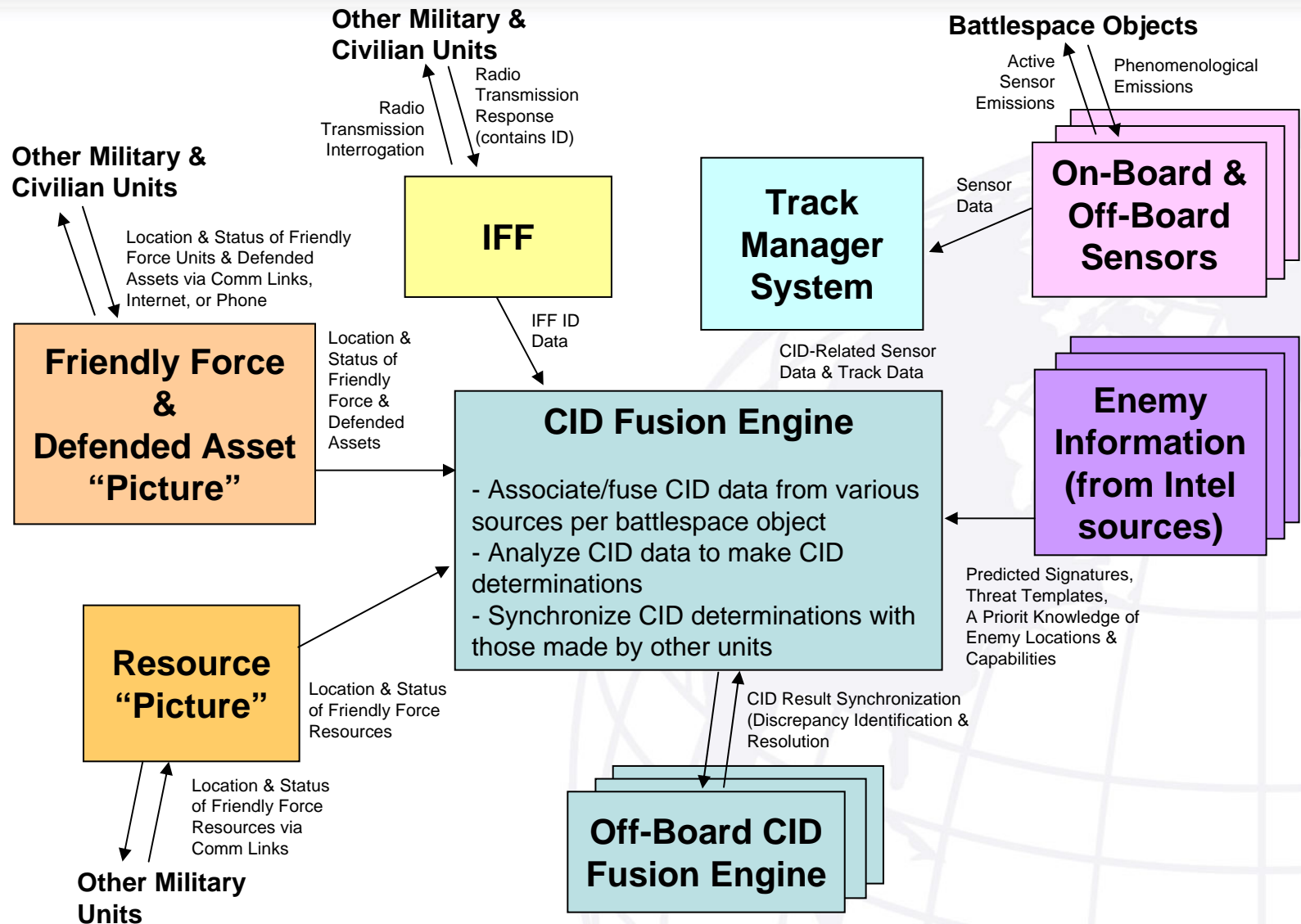
Common Identification (ID)

- **Objective:** accurate, timely, and sustainable characterization and classification of tracks to facilitate early threat and resource awareness, and enable optimal weapon engagement planning
- **Current methods:** Identification Friend or Foe (IFF), Local sensor data Intelligence, Surveillance, and Reconnaissance (ISR)
- **Future Capability Requirements**
 - Centralized geographical database
 - Shared resource picture
 - Common CID deterministic results
 - Common CID functionality
 - Support Joint Warfare operating environment
 - Effective CID data strategy
 - Span Warfare areas
 - Increased level of automation
 - Isolate CID processes (OA design)

Source: Combat Identification for Naval Systems in and Open Architecture, Young, 2006



Future Common ID Capability

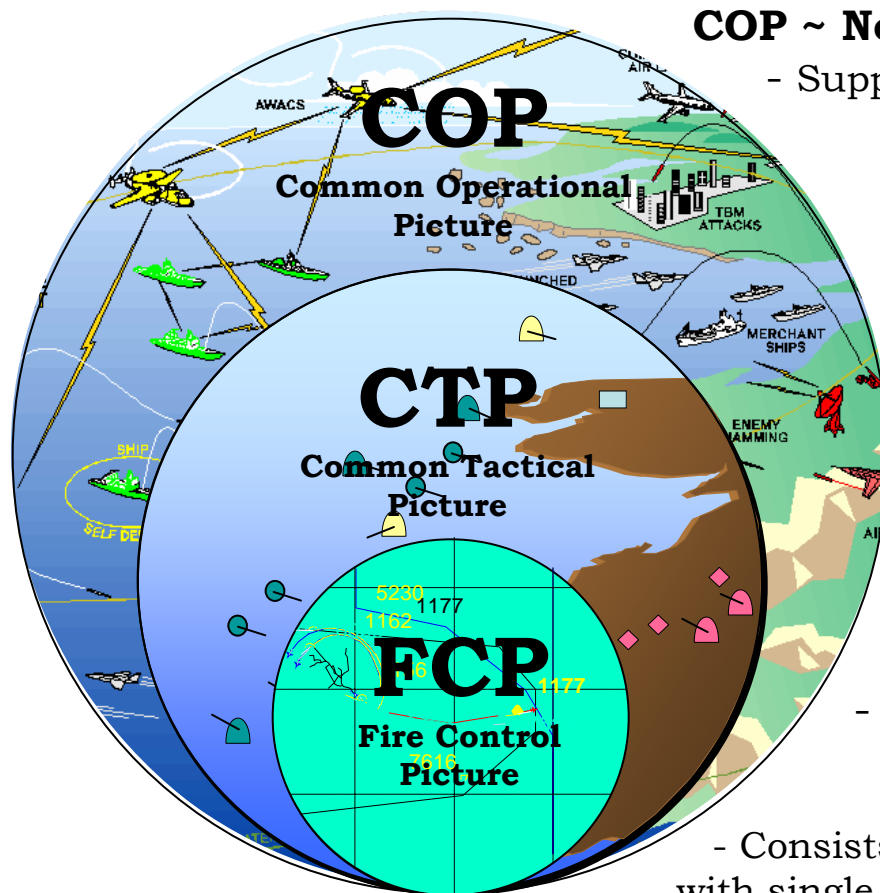


Source: Future CID Capability, Young, 2006



Battle Space Information Realms

The FORCEnet OA operational concept will enable ideal threat/weapon pairings by maintaining BF-wide shared situational awareness across the three information realms



COP ~ Non-Real Time (minutes)

- Supports Planning/Force Mgt:
 - Deployment
 - Movement
- Consists of: tactical info, courses of action, enemy order of battle info

CTP ~ Near-Real Time (seconds)

- Supports Cueing/Force Mgt:
 - Maneuver
 - Asset Control
 - Weapon/Sensor Cueing
 - Target Weapon Pairing
- Consists of: tactical information

FCP ~ Real Time (sub-seconds)

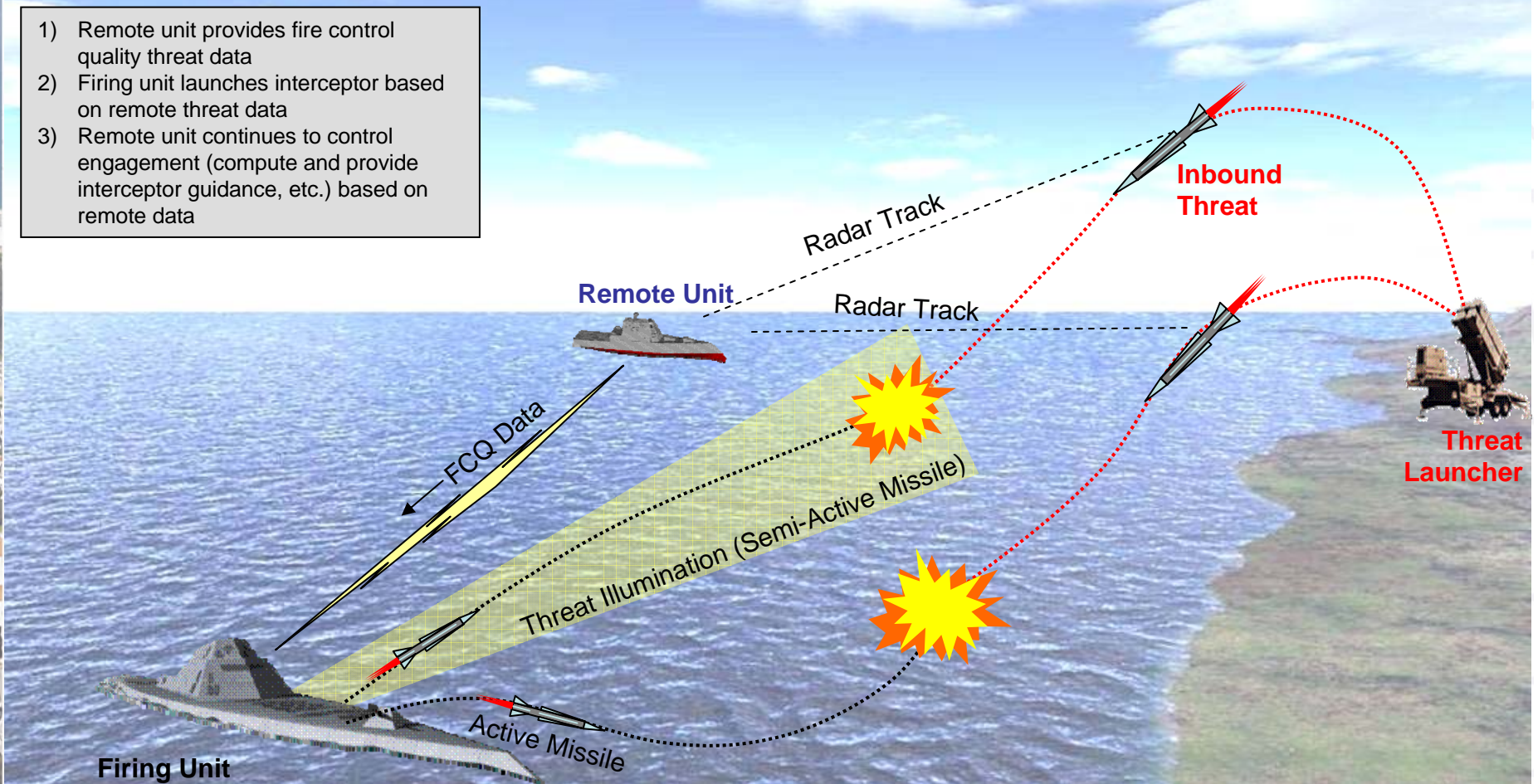
- Supports Fire Control:
 - Launch & In-Flight Fire Support
 - Engage on Remote
- Consists of: fire control quality measurements with single threat focus

Source: Naval Network-Centric Sensor Resource Management, Worth/Green, 2006



Engage on Remote OV-1

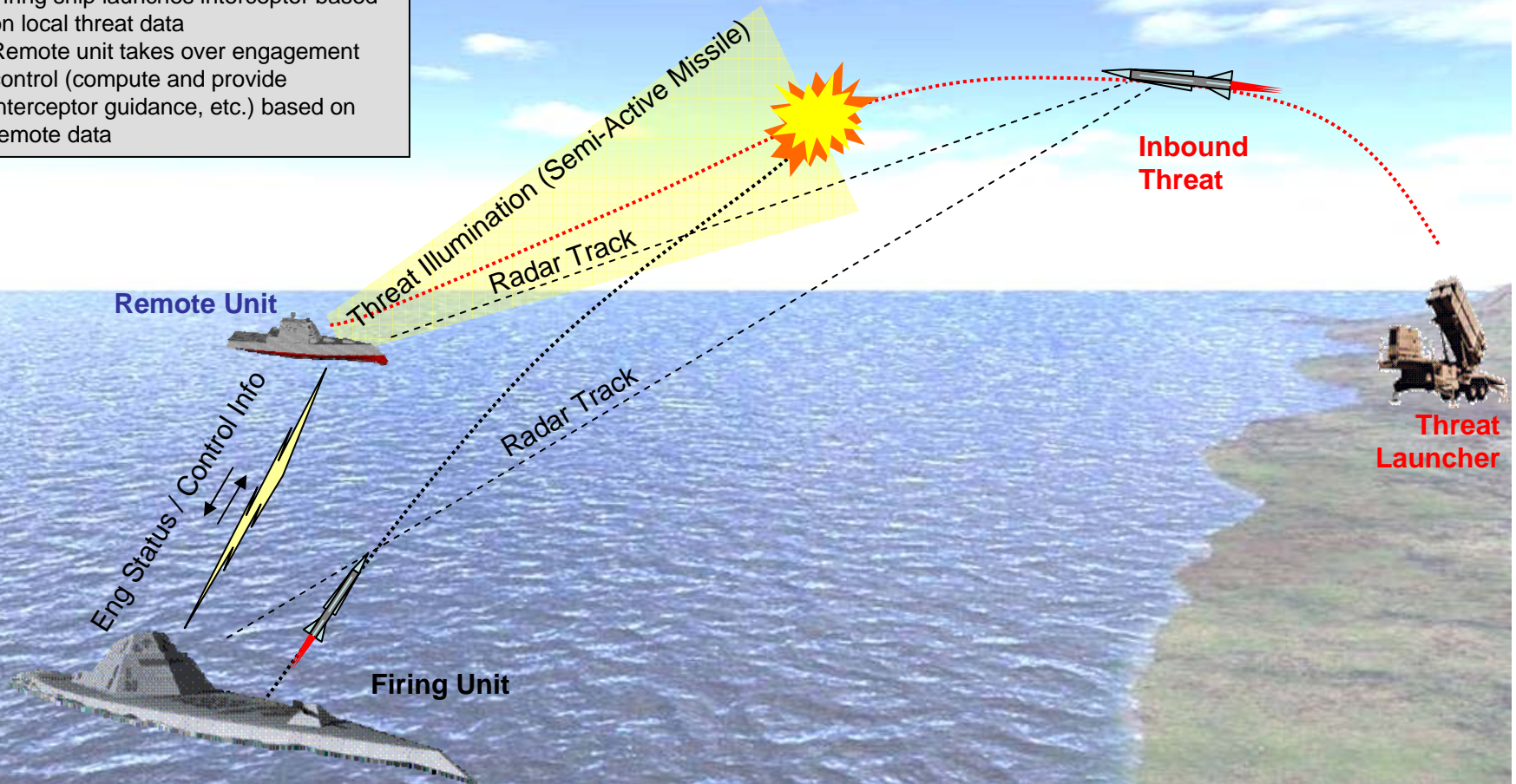
- 1) Remote unit provides fire control quality threat data
- 2) Firing unit launches interceptor based on remote threat data
- 3) Remote unit continues to control engagement (compute and provide interceptor guidance, etc.) based on remote data





Forward Pass OV-1

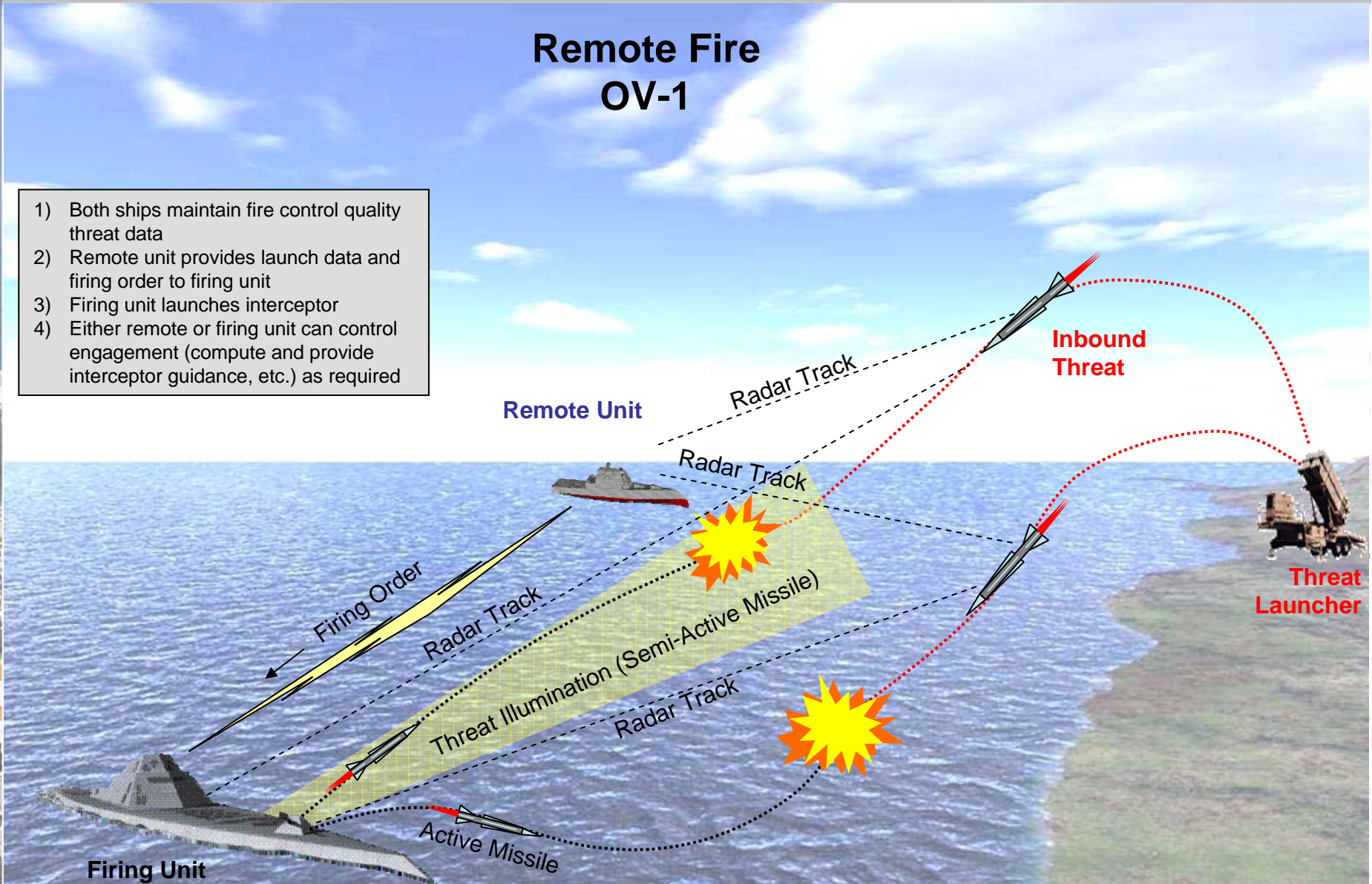
- 1) Firing ship launches interceptor based on local threat data
- 2) Remote unit takes over engagement control (compute and provide interceptor guidance, etc.) based on remote data





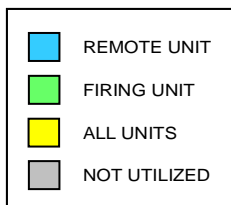
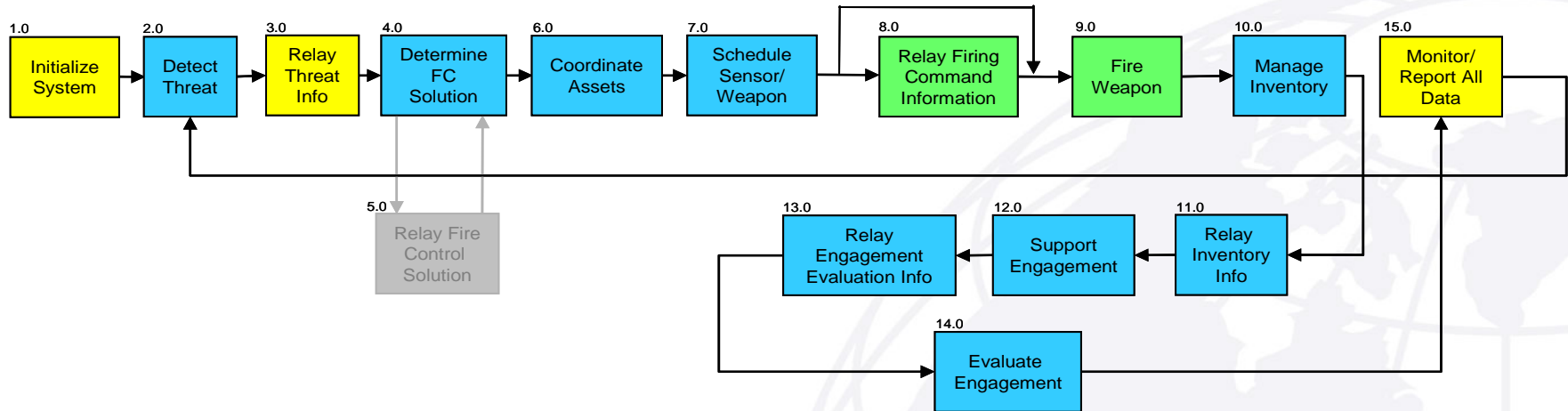
Remote Fire OV-1

- 1) Both ships maintain fire control quality threat data
- 2) Remote unit provides launch data and firing order to firing unit
- 3) Firing unit launches interceptor
- 4) Either remote or firing unit can control engagement (compute and provide interceptor guidance, etc.) as required



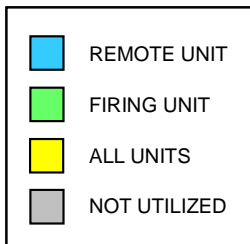
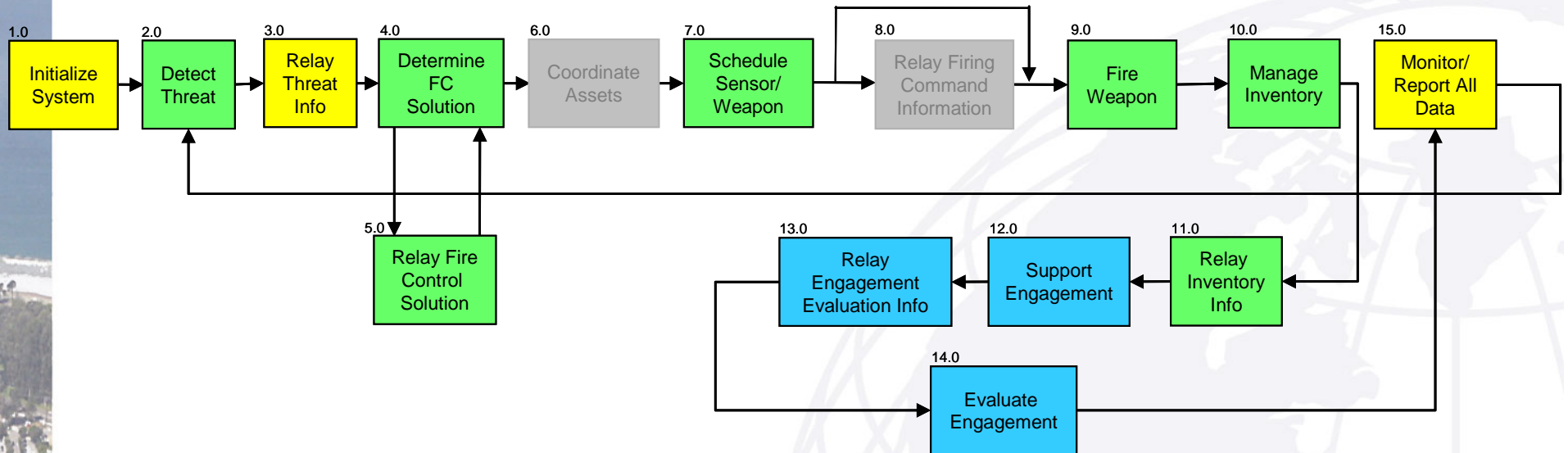


Engage on Remote FFBD



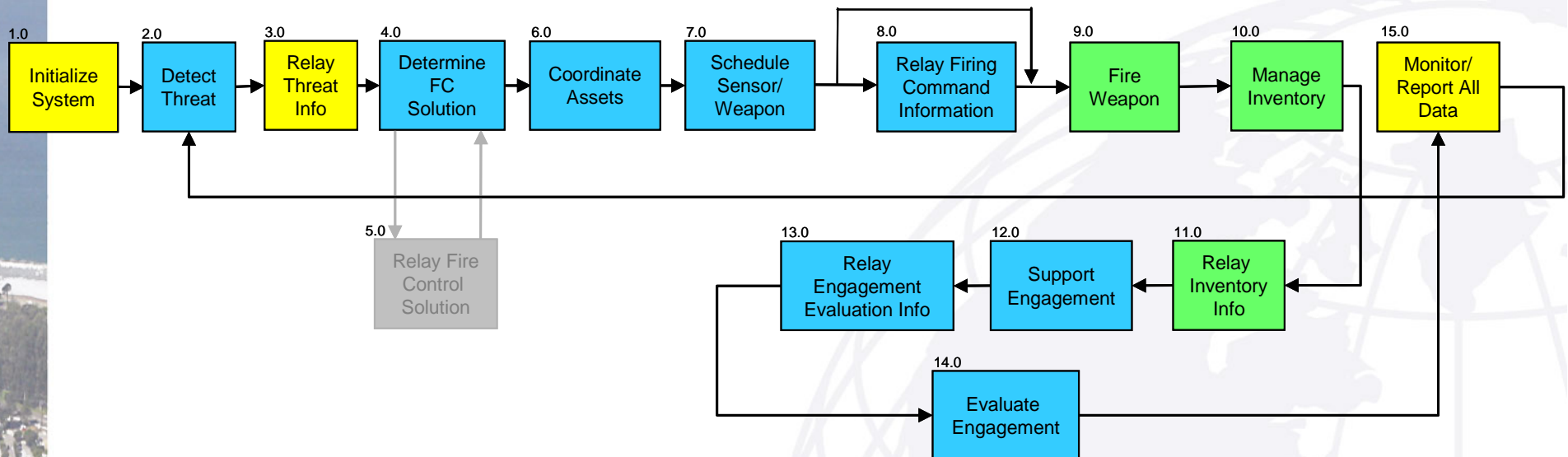


Forward Pass FFBD





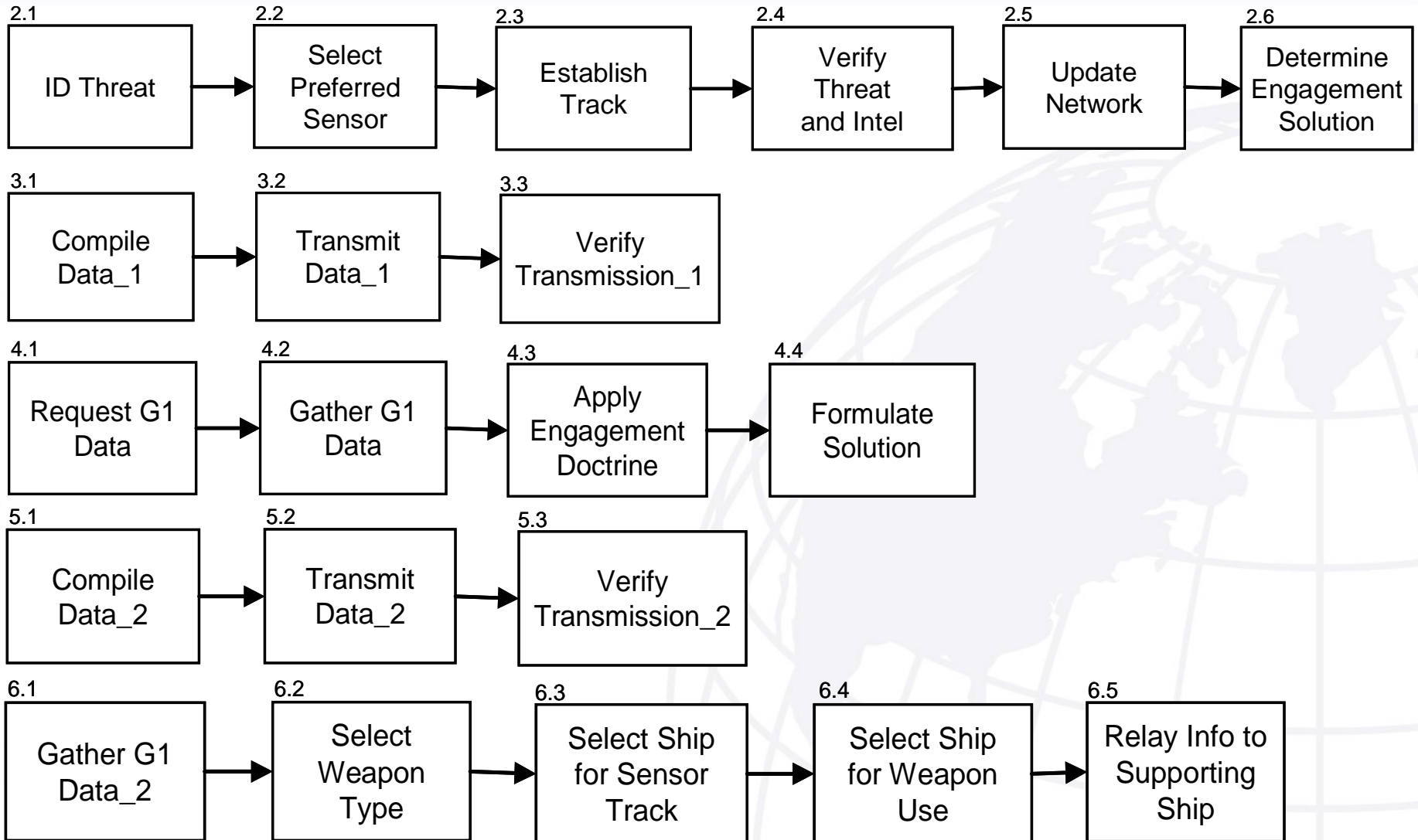
Remote Fire FFBD



- REMOTE UNIT
- FIRING UNIT
- ALL UNITS
- NOT UTILIZED

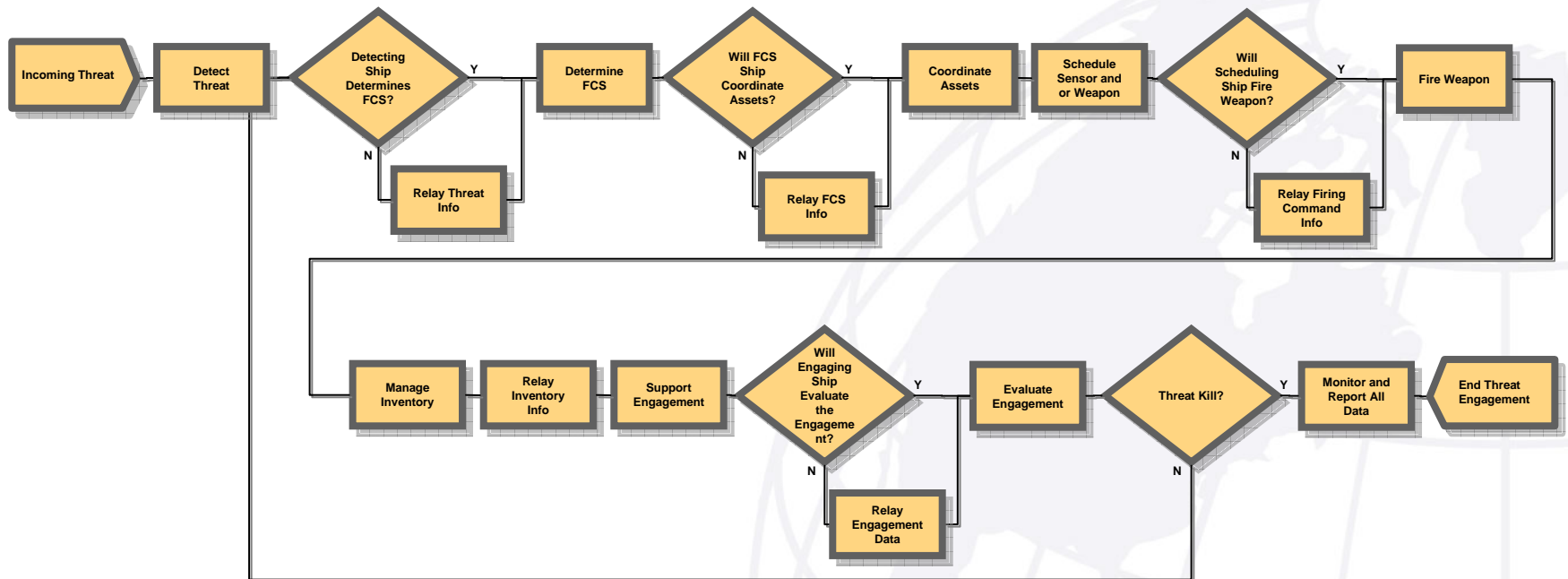


Representative Sub-Function FFBDs





Simulation Model





Simulation Model Results

# of Incoming Threats	Threat Interval (seconds)	% of Successful First-time Engagements	WIP [Saturation] (seconds)	Average Total Time (seconds)	Limiting Process #1	Limiting Process #1 Time (seconds)	Limiting Process #2	Limiting Process #2 Time (seconds)
1	60	90	0.5166	25.1135	"ID the Threat"	0.3694	"Establish a Track"	0.2561
1	60	100	0.4974	23.4344	"ID the Threat"	0.3551	"Establish a Track"	0.2648
1	30	90	1.2893	34.8877	"ID the Threat"	0.872	"Determine an Engagement Solution"	0.5203
1	30	100	1.2033	32.1173	"ID the Threat"	0.8961	"Establish a Track"	0.4846
2	60	90	2.3242	63.4865	"Transmit All Data"	2.0821	"Compile Inventory Data"	1.7562
2	60	100	2.2656	59.8616	"Transmit All Data"	2.3936	"Compile Inventory Data"	1.9017
2	30	90	5.8229	120.15	"Transmit All Data"	3.3926	"Compile Inventory Data"	3.0117
2	30	100	5.7013	111.14	"Transmit All Data"	3.7807	"Compile Inventory Data"	3.271



Revised FORCEnet OA Model

PEO IWS OA Warfare System / Functional Domain

Revised FORCEnet OA System / Functional Domain

Detect

- Search / Detect
- Sensor Asset
- Sensor Report
- Sensor Track Report
- INTEL Report
- Measurement Report



- Search / Detect
- Sensor Asset
- Sensor Report
- Sensor Track Report
- INTEL Report
- Measurement Report



Revised FORCEnet OA Model (cont'd)

PEO IWS OA Warfare System / Functional Domain

- Data / Information Services
 - Sensor Track
 - Supporting Source Track
 - Classification
 - Track Kinematics
 - Attribute Data
 - Track Repository
 - NRT INTEL Track
 - **Sensor Scheduler**

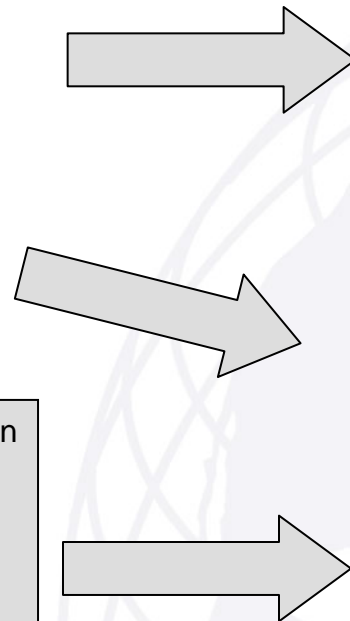
- Planning, Assessment & Decision
 - Assign Missions
 - Tactical Picture
 - Action Plans
 - Capability
 - Plan
 - Mission Assessment
 - Threat Assessment
 - C2 Order, Schedule, & Event

Revised FORCEnet OA System / Functional Domain

- Data / Information Services
 - Sensor Track
 - Supporting Source Track
 - Classification
 - Track Kinematics
 - Attribute Data
 - Track Repository
 - NRT INTEL Track

- Planning, Assessment & Decision
 - **Sensor Scheduler**
 - Assign Missions
 - Tactical Picture
 - Action Plans
 - Capability
 - Plan
 - Mission Assessment
 - Threat Assessment
 - C2 Order, Schedule, & Event
 - **Schedule: Weapon, RV, NAV & Engineering**
 - **Action: Weapon, RV, NAV & Engineering**

Control

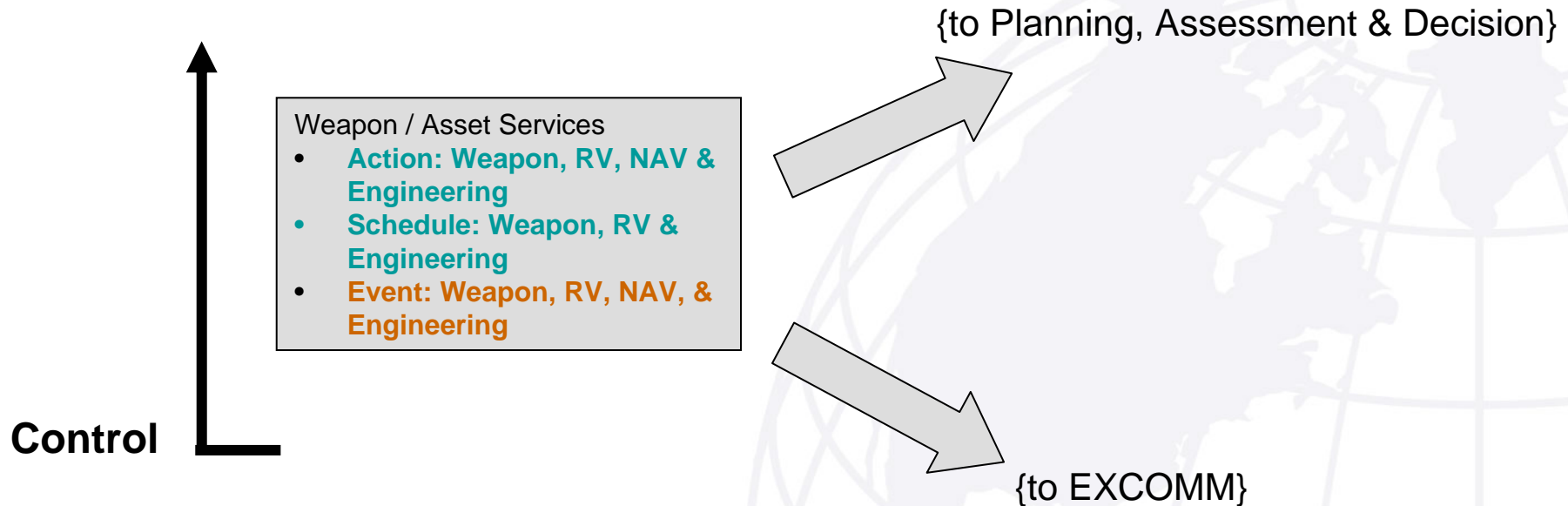




Revised FORCEnet OA Model (cont'd)

**PEO IWS OA
Warfare System /
Functional Domain**

**Revised FORCEnet
OA System /
Functional Domain**





PEO IWS OA Warfare System / Functional Domain

- Mission Execution
- Air / Surface Missile
 - Land Attack Missile
 - Torpedo
 - Gun
 - Decoy
- RV Assets
- Aircraft
 - Boat
 - Un-manned Vehicle
- RV Assets
- Engineering
 - Damage
 - Bridge

Engage



Revised FORCEnet OA System / Functional Domain

- Mission Execution
- Air / Surface Missile
 - Land Attack Missile
 - Torpedo
 - Gun
 - Decoy
- RV Assets
- Aircraft
 - Boat
 - Un-manned Vehicle
- RV Assets
- Engineering
 - Damage
 - Bridge
- Kill Assessment**
- Midcourse Guidance**



Revised FORCEnet OA Model (cont'd)

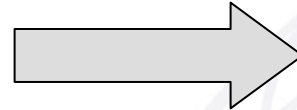
PEO IWS OA Warfare System / Functional Domain

Common Services

- Display
- NAV
- Database
- Time
- DX / DR
- Environment

EXCOMM

- Communications Service Action
- Network Schedule
- Message Event
- Network
- Radios
- Data Links
- SatComm



Revised FORCEnet OA System / Functional Domain

Common Services

- Display
- NAV
- Database
- Time
- DX / DR
- Environment

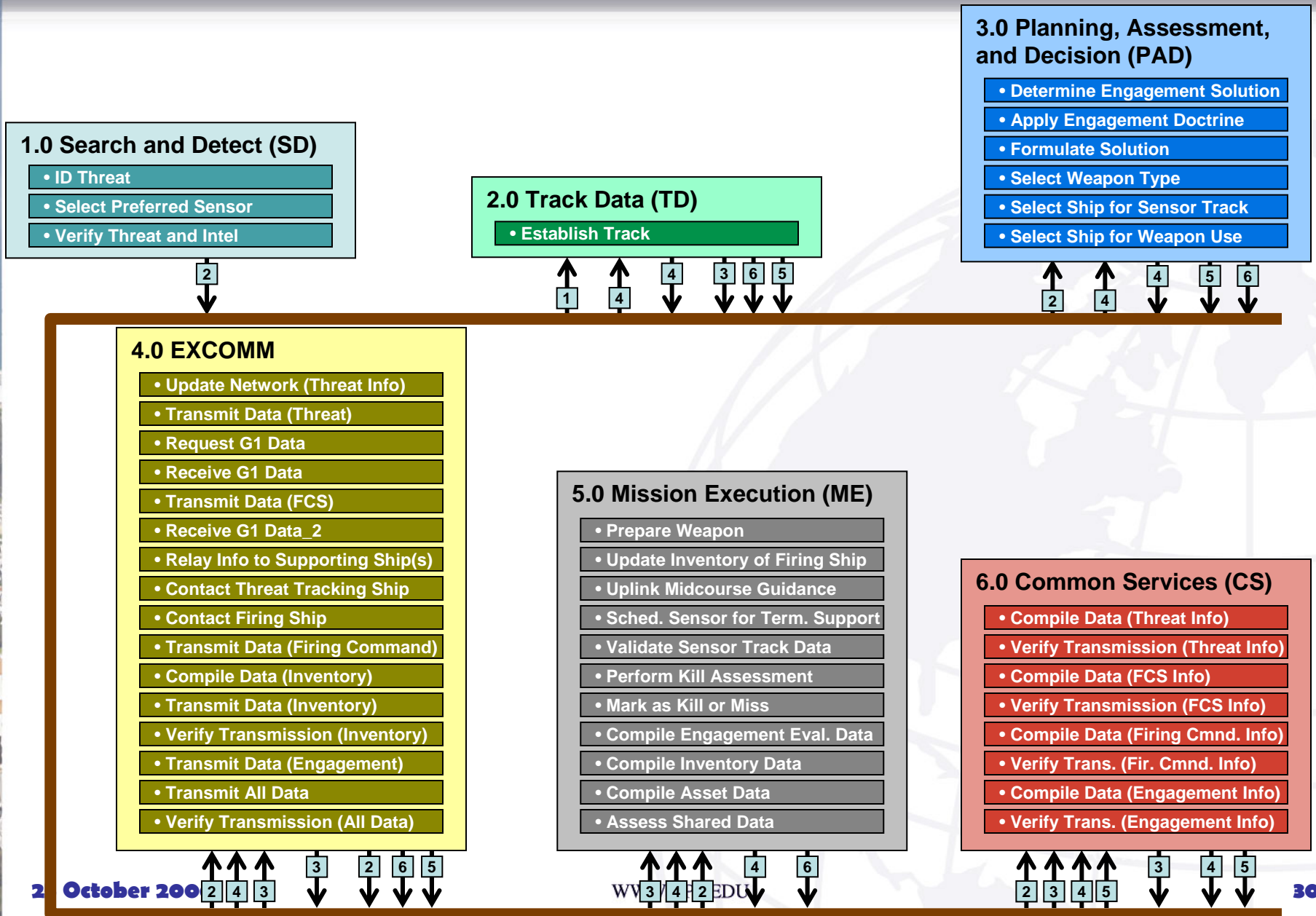


EXCOMM

- Communications Service Action
- Network Schedule
- Message Event
- Network
- Radios
- Data Links
- SatComm
- **BG /BF COA Orders**
- **Event: Weapon, RV, NAV & Engineering**



Revised FORCEnet OA Functional Model





Revised FORCEnet OA System Domain

1.0 Search and Detect (SD)

- Sensor Asset
- Sensor Report (Status)
- Sensor Track Report
- INTEL Report
- Measurement Report



2.0 Track Data (TD)

- Ship Track (System Track)
- Support Source Track
- Track Repository
- Track Kinematics
- Attribute Data



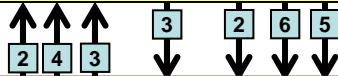
3.0 Planning, Assessment, and Decision (PAD)

- Threat Assessment
- Sensor Scheduler
- Assigned Missions
- Plan
- C2 Order, Schedule, Event
- Tactical Picture
- Capability
- Schedule: Weap., RV, NAV Engin.



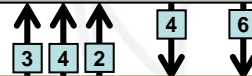
4.0 EXCOMM

- G1 Data
- G2 Data
- G3 Data
- Data Links
- Network
- SATCOM
- Radios
- BG/BF/COA Orders



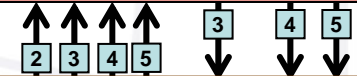
5.0 Mission Execution (ME)

- Weapon Systems
- RV Assets
- Asset Reports
- Mission Evaluation
- Midcourse Guidance



6.0 Common Services (CS)

- Display
- Time
- Navigation
- Environment
- Databases





Conclusions / Recommendations

- Functional analysis of PEO IWS OA Functional Domain model resulted in revised FORCEnet OA model
- Simulation validated logical functional flow of revised FORCEnet OA model
- Simulation validated system timing of revised FORCEnet OA model
- Revised FORCEnet OA model and Simulation used for model validation merit further scrutiny and refinement



Recommended Future Actions

- Incorporate real-world timing parameters of current/future combat systems
- Incorporate real-world threat characteristics and parameters into simulation model
- Use simulation model to determine threat “processing” time using
- Refine simulation model based on results from using real-world combat system and threat parameters
- Use refined simulation model to assess combat system network architectures for saturation nodes and choke points
- Assess simulation model against other likely engagement scenarios
- Continue to revise NAVSEA FORCEnet OA model for use in architecting future single ship and strike group systems and networks