Australian Government

Department of Defence

Guided Weapons and
Explosive Ordnance Group

parari 2024 AUSTRALIAN EXPLOSIVE ORDNANCE SAFETY SYMPOSIUM

Interoperability and Interchangeability

Software Aspects of Weapon System Interoperability and Interchangeability

Mr Warren Miller
Software Assurance
Desk Officer

Directorate of Engineering
GWEO Systems Division

Defending Australia and its National Interests
www.defence.gov.au

Interoperability and Interchangeability

- Software is an enabler.
- How do we ensure software suitably enables interoperability and interchangeability?
- Doesn’t happen by accident
- Therefore must be “*Baked into the cake.*”

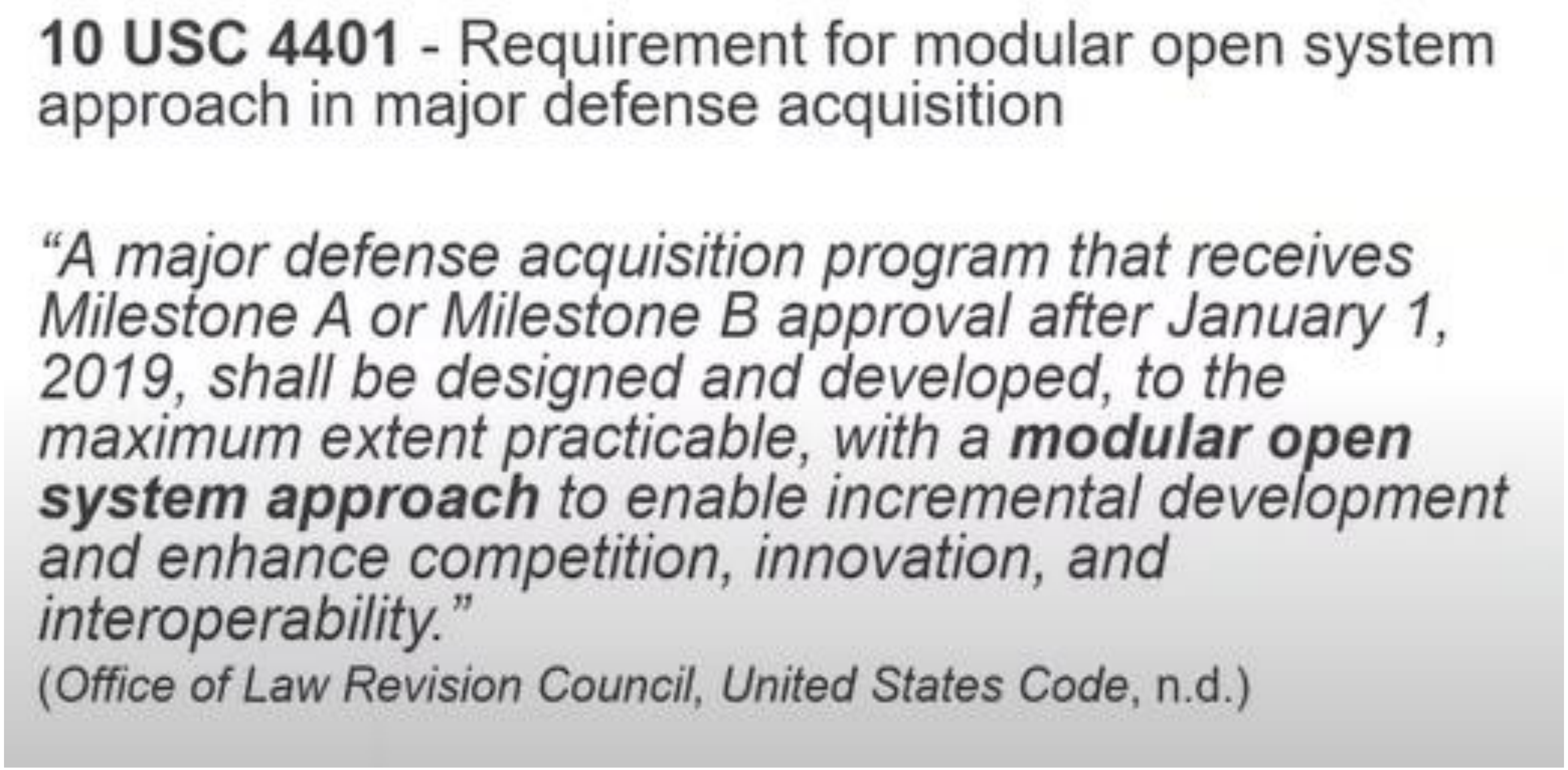
Interoperability and Interchangeability

- Let’s look at some different facets
  - Weapon Open System Architecture (WOSA)
  - Tactical Data Link (TDL) Link-16
  - Weapon System Safety and
  - Weapon System Security

WOSA employs Modular Open Systems Architecture Approach (MOSA)

- The US Department of Defense’s (DoD) modular open systems approach (MOSA) is to design systems with **highly cohesive**, **loosely coupled**, and **severable modules** that can be competed separately and **acquired from independent vendors**. This approach allows the Department to acquire warfighting capabilities, including systems, subsystems, software components, and services, with more flexibility and competition. MOSA implies the use of modular open systems architecture, a structure in which **system interfaces share common**, **widely accepted standards**, with which **conformance can be verified**.

Modular Open Systems Architecture Approach (MOSA)

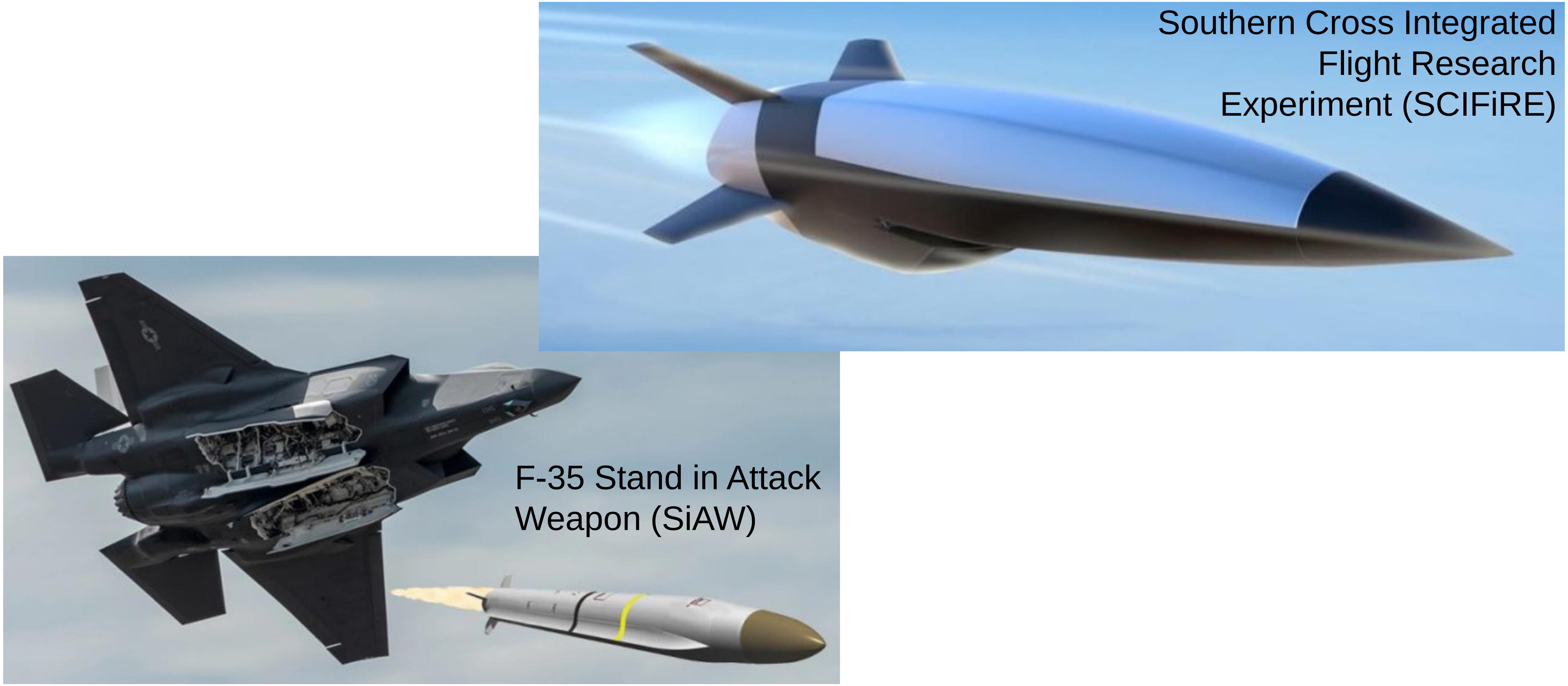


10 USC 4401 - Requirement for modular open system approach in major defense acquisition

*"A major defense acquisition program that receives Milestone A or Milestone B approval after January 1, 2019, shall be designed and developed, to the maximum extent practicable, with a **modular open system approach** to enable incremental development and enhance competition, innovation, and interoperability."*

(*Office of Law Revision Council, United States Code*, n.d.)

Weapon Open Systems Architecture (WOSA) Examples in Development



Southern Cross Integrated Flight Research Experiment (SCIFiRE)

F-35 Stand in Attack Weapon (SiAW)

Weapon Open System Architecture (WOSA)

- Comprised of – WOSA Reference Architecture (logical), WOSA Implementation Architecture and WOSA Verification Plan.
- WOSA is a reference standard which encompasses hardware and software represented as logical synergy between components. The **Reference Architecture** details a logical message construct (header and payload formatting for messages) to which all WOSA functional domains within a munition must conform, i.e., interface requirements. This WOSA Reference Architecture will then be utilized, to inform the munitions physical design, in developing the WOSA **Implementation Architecture**. The WOSA Reference Architecture would be the same across the weapon portfolio but the WOSA Implementation Architecture would be unique to each weapon system. The munitions physical design can be verified against the Reference Architecture using the WOSA **Verification Plan**.

Weapons Open System Architecture (WOSA) Goals

- Non proprietary architectural standards for all munitions
  - developed and maintained with industry consensus
  - open key interfaces, modularity and composition requirements
- Goal to improve acquisition efficiency
  - reduce integration cost/risk
  - reduce Lifecycle Cost
  - enable adaptability and reuse
  - decouple software/subsystem from hardware
  - decrease development and integration time
  - reduce obsolescence impacts via competition & rapid tech insertion

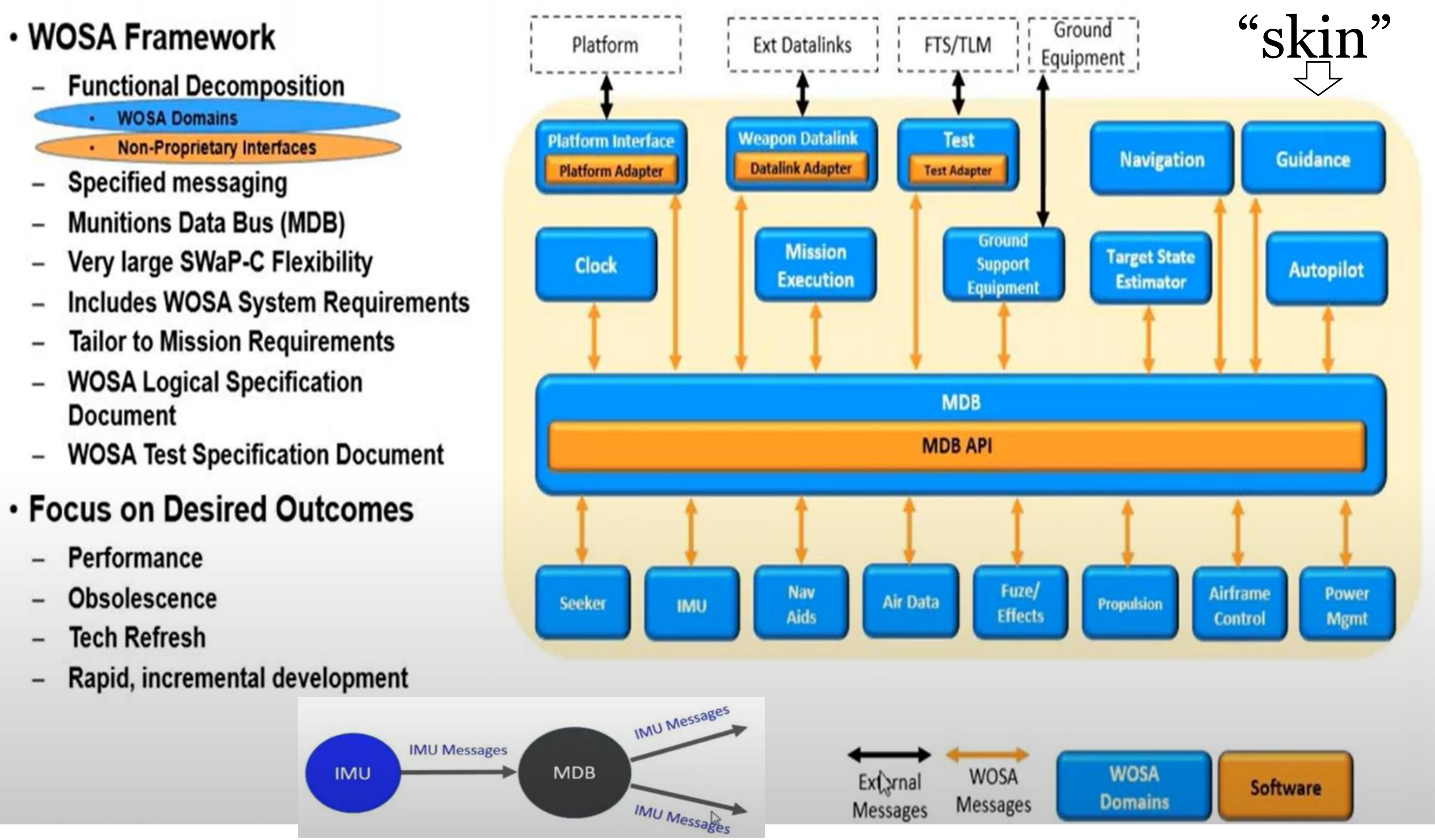
Weapons Open System Architecture (WOSA) Beneficial Properties

- Good Abstraction. A component implements a function or concept that enables re-use.
- High Cohesion. High relationship between chunked artifacts/functions into components.
- Low Coupling. Low interdependence between components.
- Data Reduction. Reduces extraneous data between components.
- Encapsulation. Components hide their internals and do not permit other components to bypass their visible interfaces.
- Well-Documented Interfaces. All interfaces are documented in sufficient detail to support the substitution of one variant of the associated component with another by an organization other than its original developer.
- Open Standards. All interfaces conform to open (non-proprietary) standards.
- Verified. The conformance of interfaces to their associated open standards can be readily verified via testing.

Weapons Open System Architecture (WOSA) Acquisition Strategy Use Cases

- Weapon designed for technology refresh.
  - e.g. Seeker can be simply swapped out for one with improved performance
- Common component used across multiple weapons.
  - e.g. New weapon has a requirement for a component common with existing weapon(s)
- Common weapon with two functionally different sub components.
  - e.g. Short and long range variants where front ends are common and rocket motors are different. Weapon integrator will “tune” software to accommodate both rocket motors.
- Weapon has four major components and three breakpoints (interfaces).
  - e.g. Each of the four major architectural components (i.e. propulsion, guidance-and-control, warhead, seeker) competed separately. As technology improves for each component, it can be quickly integrated into the weapon.

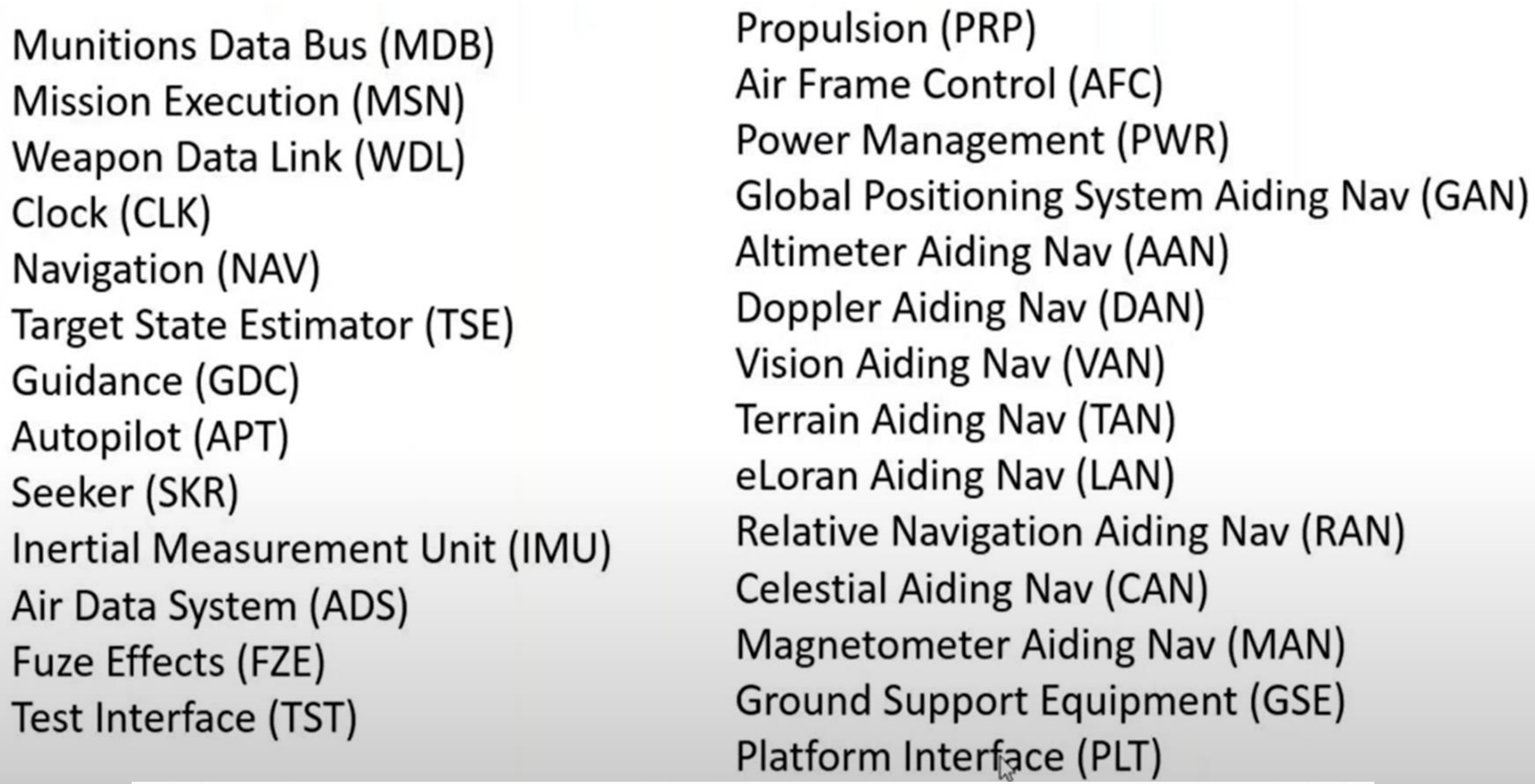
WOSA Framework (Functional)



- **WOSA Framework**
  - Functional Decomposition
    - WOSA Domains
    - Non-Proprietary Interfaces
  - Specified messaging
  - Munitions Data Bus (MDB)
  - Very large SWaP-C Flexibility
  - Includes WOSA System Requirements
  - Tailor to Mission Requirements
  - WOSA Logical Specification Document
  - WOSA Test Specification Document
- **Focus on Desired Outcomes**
  - Performance
  - Obsolescence
  - Tech Refresh
  - Rapid, incremental development

Weapons Open System Architecture (WOSA)

WOSA Domains

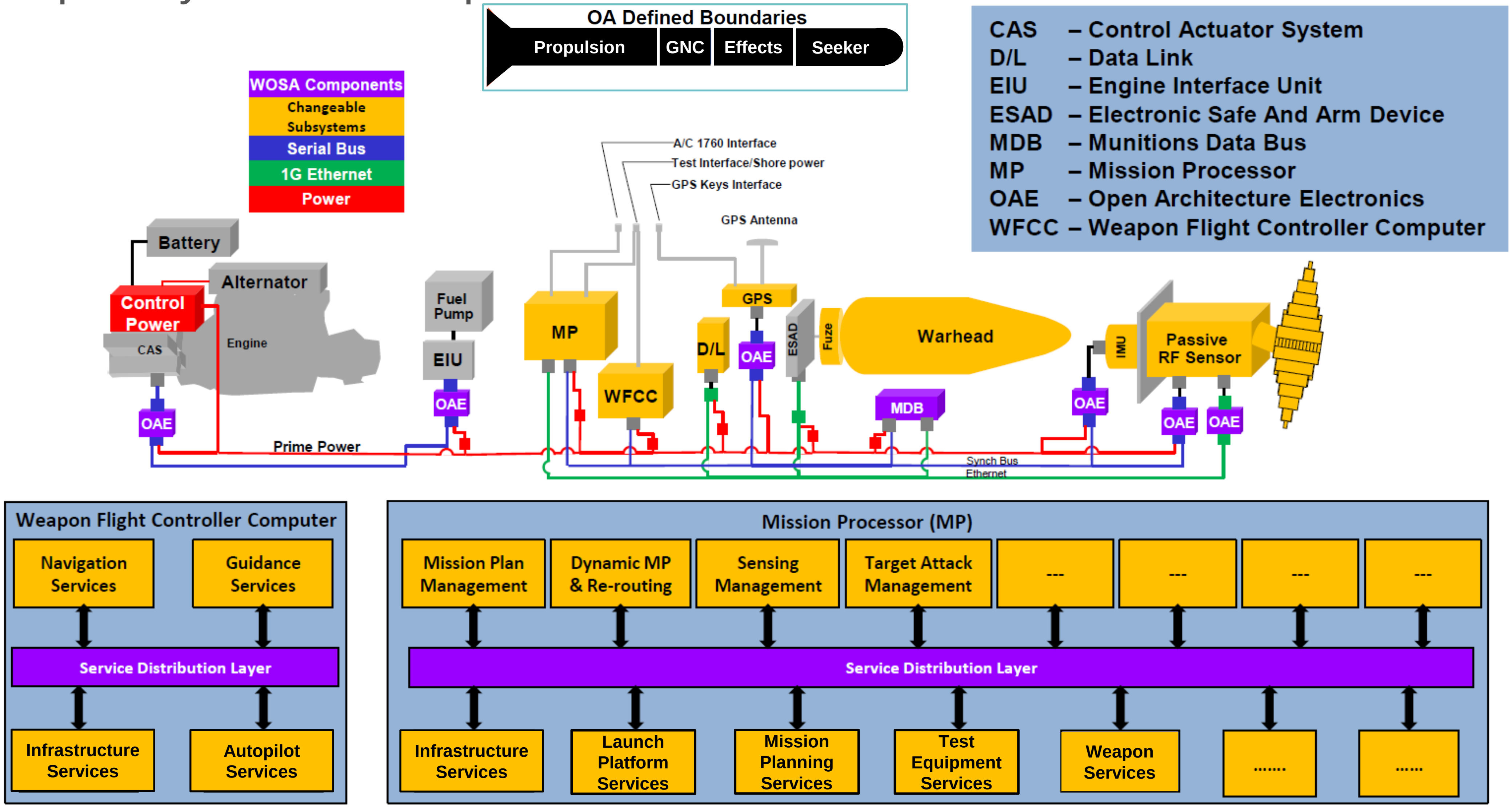


Munitions Data Bus (MDB)
Mission Execution (MSN)
Weapon Data Link (WDL)
Clock (CLK)
Navigation (NAV)
Target State Estimator (TSE)
Guidance (GDC)
Autopilot (APT)
Seeker (SKR)
Inertial Measurement Unit (IMU)
Air Data System (ADS)
Fuze Effects (FZE)
Test Interface (TST)

Propulsion (PRP)
Air Frame Control (AFC)
Power Management (PWR)
Global Positioning System Aiding Nav (GAN)
Altimeter Aiding Nav (AAN)
Doppler Aiding Nav (DAN)
Vision Aiding Nav (VAN)
Terrain Aiding Nav (TAN)
eLoran Aiding Nav (LAN)
Relative Navigation Aiding Nav (RAN)
Celestial Aiding Nav (CAN)
Magnetometer Aiding Nav (MAN)
Ground Support Equipment (GSE)
Platform Interface (PLT)

WOSA Version 3.4 released Oct 2023 (v1.0 released January 2018)

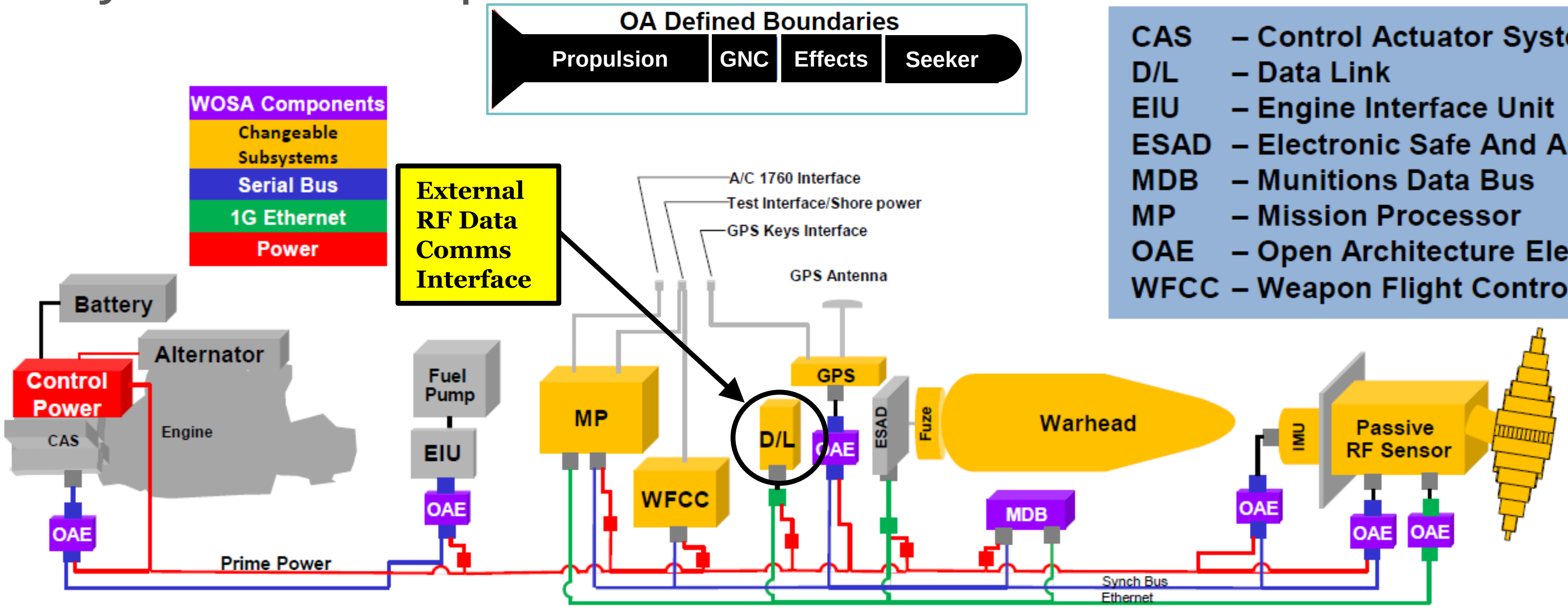
Weapon System Decomposition

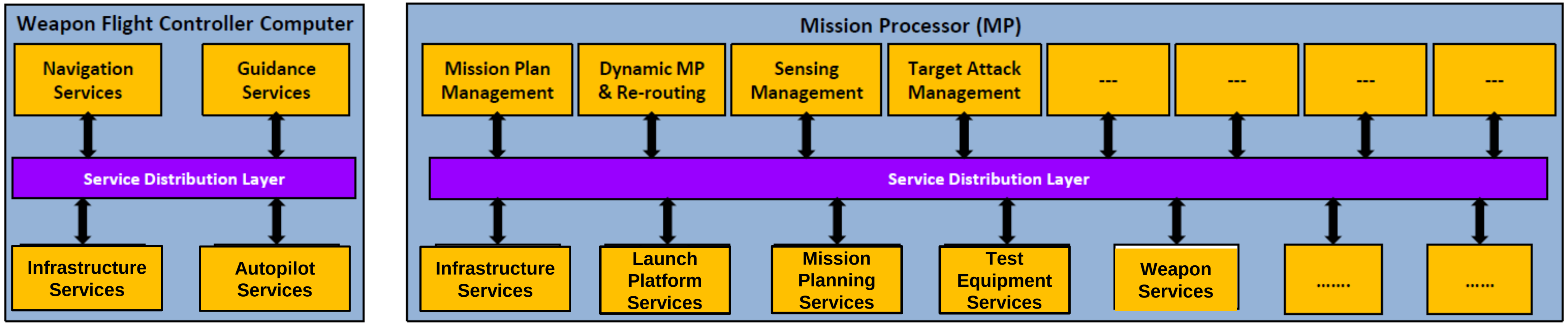


CAS	– Control Actuator System
D/L	– Data Link
EIU	– Engine Interface Unit
ESAD	– Electronic Safe And Arm Device
MDB	– Munitions Data Bus
MP	– Mission Processor
OAE	– Open Architecture Electronics
WFCC	– Weapon Flight Controller Computer

Weapon System Decomposition

CAS	– Control Actuator System
D/L	– Data Link
EIU	– Engine Interface Unit
ESAD	– Electronic Safe And Arm Device
MDB	– Munitions Data Bus
MP	– Mission Processor
OAE	– Open Architecture Electronics
WFCC	– Weapon Flight Controller Computer





Weapon Flight Controller Computer

Navigation Services | Guidance Services

Service Distribution Layer

Infrastructure Services | Autopilot Services

Mission Processor (MP)

Mission Plan Management | Dynamic MP & Re-routing | Sensing Management | Target Attack Management | --- | --- | --- | ---

Service Distribution Layer

Infrastructure Services | Launch Platform Services | Mission Planning Services | Test Equipment Services | Weapon Services | .... | ......

Tactical Data Link (TDL) – Link 16

- Adherence to a common data link standard assures interoperability over RF
- MIL-STD-6016, aka Link 16, is a TDL interoperability standard.
  - 11,410 pages in total.
  - A compliant participant on the network will implement the relevant subset of messages based on its role.
- Link 16 was expanded to accommodate Network Enabled Weapons (NEW) thus allowing them to join the network as a participant.

Network Enabled Weapon (NEW)

Tactical Data Link (TDL) – Link 16 NEW

- Positive weapons control, pre and post weapons launch
- The network obtains weapon status and location information throughout the weapon’s flight.
- The weapon controller may update the weapon impact point or retarget during flight, enhancing targeting accuracy.
- Effective against rapidly deployable and mobile enemy weapon systems.
- In addition, the weapon controller can terminate (abort) an engagement by redirecting the weapon to a safe area or alter fusing to reduce effects.

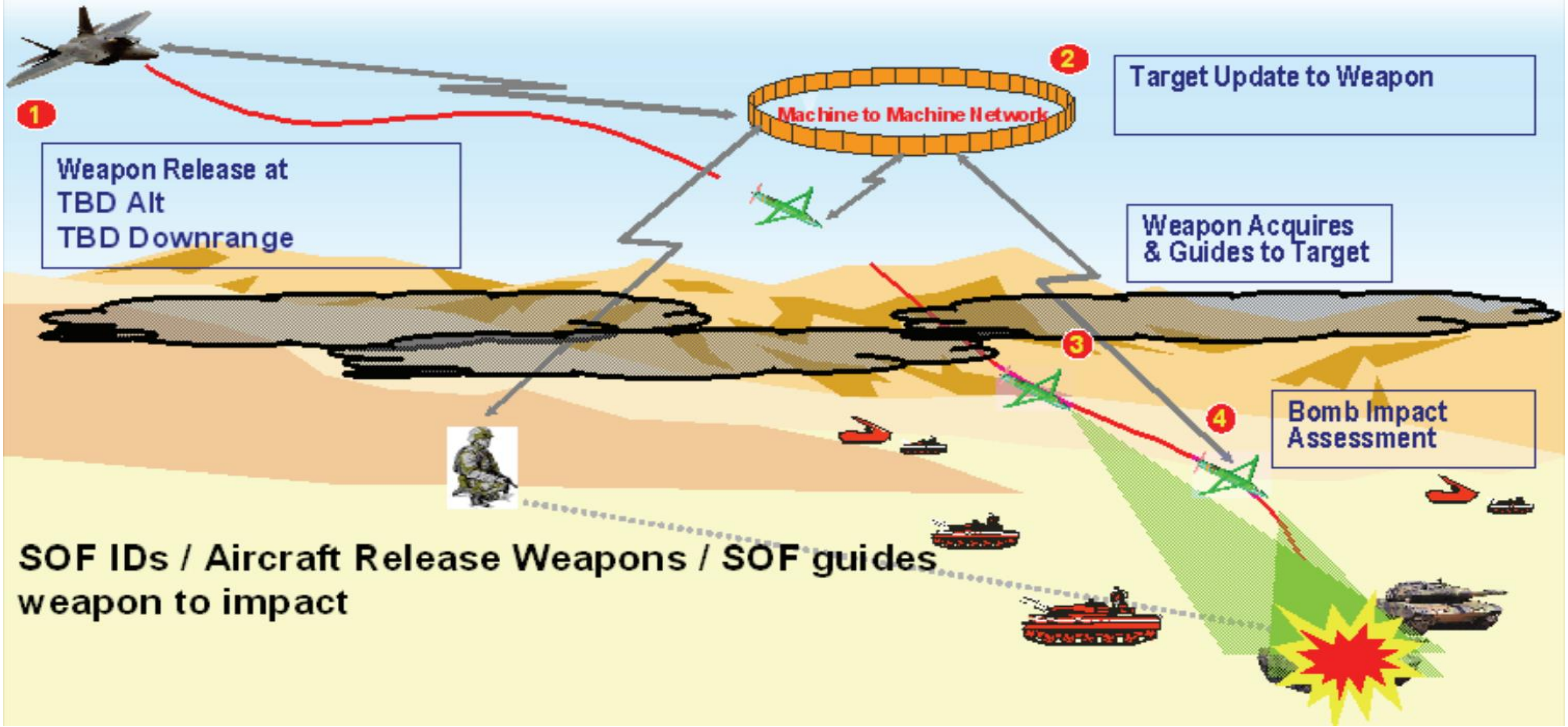
Tactical Data Link (TDL) – Link 16 NEW

- For NEW, not just the launching platform involved. A NEW may be handed off to another compliant controlling unit which may or may not have launching platform capabilities. For example a strike aircraft could hand off a launched weapon to ground forces in a Close Air Support scenario.
- NEW generally join an established network and may access, from the network, the location and identity of known forces, friendly and otherwise, in the target area – are somewhat “aware” of their surroundings – just not in a Machine Learning (ML) / Artificial Intelligence (AI) context.

Tactical Data Link (TDL) – Link 16 NEW

- Elements on board the missile
  - TDL Software
    - May be hosted in the Mission Processor
    - Constructs messages for transmission
    - Processes received messages
  - Data Link Terminal (DLT)
    - Interfaces with TDL Software
    - Encrypts outgoing / decrypts incoming data
    - Transmits / receives RF waveform
  - Antenna

Close Air Support Scenario



Network Enabled Weapon (NEW)

Key Benefits

- Increased standoff range
- Moving target engagement
- Avoids blue force and no strike targets
- In-flight target update
- In-flight retargeting
- In-flight controller hand-off
- In-flight abort
- Increased weapon accuracy
- Bomb Hit Indication (BHI)
- Real-time situational awareness

TDL Interoperability Testing

- Conformance to Standard Testing (CTS)
  - Full CTS test covering all areas implemented by TDL platform
  - Test procedures and scenarios adapted for each platform implementation
- Joint Interoperability Testing (JIT)
  - Focus is testing interoperability between ADF platforms
  - Particular focus on new or modified platforms
- Combined Interoperability Testing (CIT)
  - Focus is testing interoperability between US and ADF platforms
  - Involves multiple platforms both real and simulated

Safety Engineering

OUR MISSILE PROGRAM IS THE PRIDE OF ELBONIA!
Dilbert.com DilbertCartoonist@gmail.com
YESTERDAY WE LAUNCHED A TEST MISSILE THAT WENT A HUNDRED YARDS BEFORE RIPPING THE ROOF OFF AN ORPHANAGE.
6-19-12 ©2012 Scott Adams, Inc./Dist. by Universal Uclick
YOU TEST YOUR MISSILES NEAR ORPHANS?
WHAT ARE THE ODDS THEY'D BE UNLUCKY THREE TIMES?

Minimising Software Contribution

- Many EO software functions have the potential to cause or contribute to hazardous conditions.
- Given this is the case, safety must be designed-in i.e. hazards designed-out, and any residual risk minimised.
- To do so requires a systematic and rigorous approach to software system development and system safety.
- Systematic and rigorous approach:
  - Adopt a set of industry standards and guide books.
  - Apply level of rigour commensurate with software contribution to system safety risk.
  - Ensure the Principles of Software Safety Assurance are satisfied.

Software Safety Engineering

- Safety Engineering, Systems Safety Engineering, Software Safety Engineering and Software Engineering processes are present and integrated
- The contribution of software to system level hazards is considered
- Hazards associated with software functions are identified and controls/mitigations implemented
- Software single point failures identified and eliminated/controlled/mitigated
- The intended role and environment are consistent with the role and environment for which the EO was designed
- Software risk is eliminated or minimised So Far As Reasonably Practicable (SFARP)

Lifecycle Standards

- System Lifecycle Standard
  - ISO/IEC/IEEE 15288:2015(E) Systems and software engineering — System life cycle processes
    - Plus ISO/IEC/IEEE 15289:2015 Systems and software engineering — Content of life-cycle information products (documentation – systems engineering)
- Software Lifecycle Standard
  - Legacy Standard:
    - MIL-STD-498 Military Standard: Software Development and Documentation
  - Modern Standards:
    - ISO/IEC/IEEE 12207:2017 Systems and software engineering — Software life cycle processes
      - Plus ISO/IEC/IEEE 15289:2015 Systems and software engineering — Content of life-cycle information products (documentation – software engineering)

Safety Standards and Guides

- System Safety Standard
  - MIL-STD-882E System Safety Standard 11 May 2012

- Domain Specific Software Safety Engineering and Assurance Guides
  - AOP-52 (STANAG 4452) Guidance on Software Safety Design and Assessment of Munition-related Computing Systems, Edition B Version 1 – 29 November 2016
  - Range Commanders Council (RCC) 319 Flight Termination Systems Commonality Standard

Hazard List and Analysis Considerations – Open Systems Architecture

- Standardised weapon open systems architecture lends itself to the creation of a common generic set of hazards for fully featured PGMs and common standardized acceptable methods to control those hazards.
- Among other benefits, addressing hazards in a standardised way will streamline the certification process and introduction into service of new and upgraded weapons or weapon components
- New hazards then become a small delta to address
- Better understood residual risk
- Readily determine if risk profile changes when a weapon or weapon component is changed for another

Security Engineering

THIS SHADOWY GUY IS FROM AN UNNAMED GOVERNMENT AGENCY!!!
HE WANTS US TO CREATE A COMPUTER VIRUS TO ATTACK ELBONIAN MISSILE FACTORIES!!!
IS HE FROM OUR GOVERNMENT, LOUD HOWARD?
IS THAT IMPORTANT?
Dilbert.com DilbertCartoonist@gmail.com
8-1-12 ©2012 Scott Adams, Inc./Dist. by Universal Uclick

Security Engineering

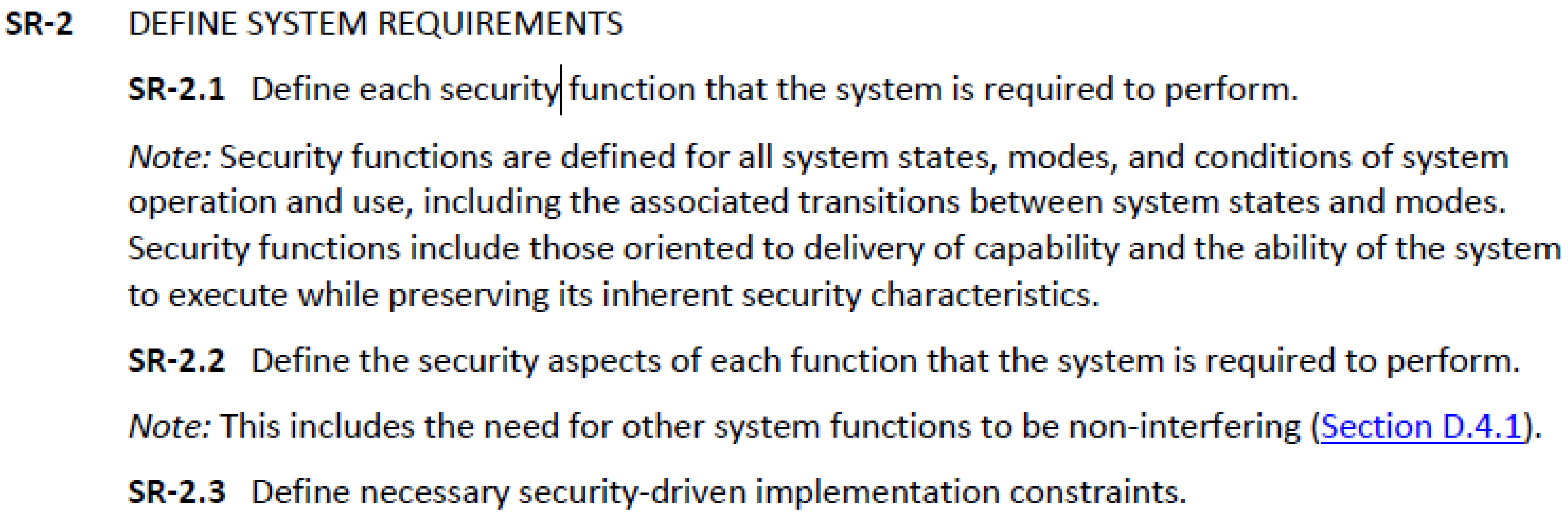
- Now that everything’s acquiring connectivity, you can’t have safety without security
- Certification and Accreditation are backward looking
- Engineering systems to be secure
- Security Engineering process parallels Safety Engineering
  - Identify vulnerabilities,
  - do analysis,
  - select and apply generic design requirements,
  - control vulnerabilities,
  - mitigate impact of breaches

Security Engineering – Standards

- Similar to Safety Engineering, Industry Standards and Guides are there to help
- NIST Special Publication NIST SP 800-160v1r1 Engineering Trustworthy Secure Systems
  - Systems Engineering Overview
  - System Security Concepts
  - Systems Security Engineering Framework
  - Trustworthy Secure Design

Security Engineering - NIST SP 800-160v1r1

- NIST SP 800-160v1r1 Conveniently embeds security activities and tasks within 15288/12207 System and Software Life Cycle Standards processes referenced earlier.



SR-2 DEFINE SYSTEM REQUIREMENTS

SR-2.1 Define each security function that the system is required to perform.

Note: Security functions are defined for all system states, modes, and conditions of system operation and use, including the associated transitions between system states and modes. Security functions include those oriented to delivery of capability and the ability of the system to execute while preserving its inherent security characteristics.

SR-2.2 Define the security aspects of each function that the system is required to perform.

Note: This includes the need for other system functions to be non-interfering (Section D.4.1).

SR-2.3 Define necessary security-driven implementation constraints.

Concluding Remarks

- We’ve had a look at open systems architecture, data links, safety and security.
- There are other aspects that may also be considered in the context of software such as:
  - Survivability
  - Training
  - Support
- Measures can be taken to design for interoperability and interchangeability at both the weapon component and weapon AUR levels.
- To derive greatest benefit, the desired level of interoperability and interchangeability must be considered early in the lifecycle, during requirement specification of weapon systems.

Questions

?

Spare Slides

Agenda

- Definitions and Context

- Open System Architecture
- Common Data Links
- Safety
- Security

Theme 2024

parari 2024

AUSTRALIAN
EXPLOSIVE
ORDNANCE
SAFETY SYMPOSIUM

Interoperability and Interchangeability

- Interoperability
  - – is the ability for forces of two or more nations to train, exercise and operate effectively together in the execution of assigned missions and tasks.
- Interchangeability
  - – is the ability to substitute one item for another of different composition or origin, between nations, without loss in effectiveness, accuracy and safety performance of weapons systems.

Interoperability Layers

- The definition of interoperability used by the Australian Defence Organisation is common to that used by NATO and the US DoD
- “It is defined as the ability of **systems, units or forces** to act together, to provide services to or accept services from, or exchange information with partner systems, units or forces.”
- For practical purposes, these relate to the DODAF technical, system and operational-level views.

- DODAF = Department of Defence Architecture Framework

Interoperability at Architectural Levels

- At the **technical level**, the issue is one of compatibility, i.e. the degree to which one electronic system can operate with another e.g. Inertial Measurement System
- For the **system level**, interconnectivity may be the main focus, i.e. the degree to which assets or units can connect with one another e.g. two platforms via an RF data link
- At the **operational level**, interoperability issues may concentrate on the organisational and doctrinal aspects (command and control arrangements) of the way in which forces (land, sea and air) can operate together in a joint environment, or the operation of a national force with other nations in a coalition

Interchangeability

- Interchangeability can then be thought of as the ability to replace a system (or part thereof), unit or force with another interoperable system (or part thereof), unit or force.
- Opportunity to swap current object out for an object that provides a better service – i.e. serviceable; equivalent function with improved performance, safer, more secure, better survivability (Susceptibility, Vulnerability and Recoverability)
- The context could be integration or operation
- Conceptually, the object could be a Weapon System component such as Inertial Reference System (IRS); an All Up Round (AUR); a weapon system; an entire weapon platform which may have multiple weapons systems; or another nation’s air/sea/ground force