Open Standards and the Defense Industrial Base

Dr. Ben Calloni, P.E., CISSP, OCRES-AP

- OMG System Assurance Task Force – Chair
- OMG BoD – Member
- The Open Group – Member: OTTF, Security, & RTES Forums, Former Member and VP of Governing Board
- FACE Consortia – Member: Technical Standards WG & Business Conformance WG
- AIAA Associate Fellow – Member of Computer Systems and SOF TC's
- OSD Software Assurance Forum (now DHS SwA Forum)

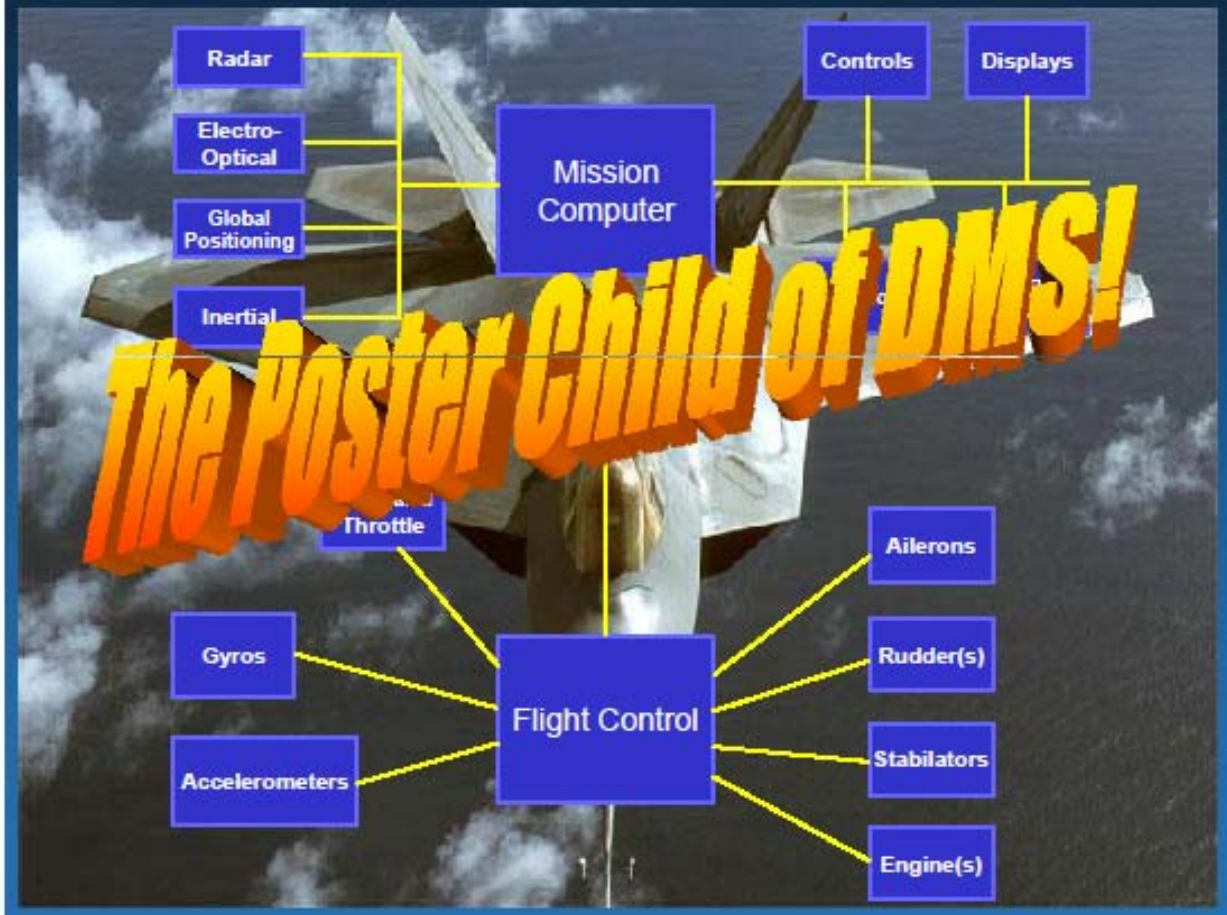
Note

- Opinions expressed in this presentation are not necessarily those of the Object Management Group
- Some data presented from Lockheed Martin Aeronautics Projects funded by AFRL
  - Weapon Systems Software Technology Support (WSSTS), Delivery Order #5 project, and the
  - Embedded Information Systems Technology Support (EISTS), Delivery Order #4 project
    - PM Agent, Jahn Luke, USAF AFRL/RYWC
    - Funding Agent, Lt Col Glenn Palmer, Director, USAF Computer Resources Support Improvement Program (CRSIP), **CRSIP previous Director Lt Col Joe Jarzombek**.
  - "Interoperability and Interchangeability: COTS Middleware Holds the Key", 2003 Joint Advanced Weapons Systems Sensors, Simulation and Support Symposium, 14 – 17 July 2003, Naval Postgraduate School, Monterey, CA
  - "COTS, MIL-SPEC, and MILS: A Necessary Harmony for Affordable Multilevel Secure Architectures", Military Technologies Conference, March 14-15, 2006, Boston, MA

Outline

- Standards
  - OMG System Assurance Task Force
- Interoperability, Exchangeability
- COTS Vendor Support
- COTS Standards and the Defense Industrial Base

Challenge Problems - Context



Characteristics

- Complex, Large
- Decades Lifespan
- Frequent Software Updates
- Mix of Computation Types
  - Logic/State Machine
  - Computational
  - Signal Processing
  - Feedback Control

F-22 Diminished Manufacturing Sources

- Hardware
  - *Intel i960*
  - *Specialized ASICS*
  - *Mil Std 1750A*
  - *Mil Std 1553*
  - *PI Bus*
  - *JIAWG Architecture*
- Software
  - *Proprietary (non commercial)*
    - Operating System (Avionics Operating System – AOS)
    - Middleware (Avionics Management System – ASM)
  - *VAX/VMS data base systems*
  - *Ada83*
  - *Mid '80's Software Engineering Environments*
- …..

Mil-Spec

- An “Elephant” is what you get when you design a “Mouse” to MIL-Spec!

- $500 Toilet Seats
- $100 Hammers (vs. one from the “helpful hardware folks”!)
- $7000 Coffee Makers on C-5 Galaxy (plus other A/C)
  - Stainless Steel
  - Low Pressure Certified
  - Fire Rated
  - Rated to 50 G’s
  - Air Force Magazine - 1980’s!!!

- http://www.tsgc.utexas.edu/archive/general/ethics/galaxy.html

Military TECHNOLOGIES CONFERENCE

OBJEC

Software

- The truth about Geeks
  - *We like pizza and large quantities of caffeine, especially at 2 AM.*
  - *We prefer to always Build it ourselves!*
  - *We prefer to rewrite whenever possible!*
  - *We will spend (waste) dozens of hours squeezing 3% utilization from a CPU. (Be careful with requirements.)*
- Largest cost component in computer systems
  - *Why is it in Software Engineering we have a mind set that unused processor utilization is a waste?*
  - *c.f. Wing spars, bridge span structures, trusses, etc.*
  - *Ltc BJ -247# boarding weight.*
- We need to keep a broad view and accept COTS as a way of development life.
  - *DoD Contractor expertise should be expended on developing combat capabilities, not re-designing infrastructure elements!*
- We need to speak HUMAN and translate to computer-eze!!!!

The Wonderful World of Standards

"Standards are like toothbrushes, everyone agrees that they're a good idea but nobody wants to use anyone else's!"

MITRE ???

OMG System Assurance Task Force (SysA TF)

- Mission
  - Establish a common framework for analysis and exchange of information related to system assurance and trustworthiness. This trustworthiness will assist in facilitating systems that better support Security, Safety, Software and Information Assurance

- Immediate focus of SysA TF is to complete work related to
  - SwA Ecosystem - **common framework for presenting and analyzing properties of system trustworthiness**
    - leverages and connects existing OMG specifications and identifies new specifications that need to be develop to complete framework
    - provides integrated tooling environment for different tool types
    - architected to improve software system analysis and achieve higher automation of risk analysis

http://sysa.omg.org/
https://buildsecurityin.us-cert.gov/swa/ecosystem.html

Software Assurance Ecosystem: The Formal Framework for System Assessments with Focus on Automation

Tools Interoperability and Unified Reporting Environment

Process Docs & Artifacts

Requirements/Design Docs & Artifacts

Reports, Risk Analysis, etc

Process, People & Documentation Evaluation Environment

- Some point tools to assist evaluators but mainly manual work
- Claims in Formal SBVR vocabulary
- Evidence in Formal SBVR vocabulary
- Large scope requires large effort
- Supported by The Open Group's UDEF*

Process, People, documentation Evidence

Formalized Specifications

Assurance Case Repository

- Formalized in SBVR vocabulary
- Automated verification of claims against evidence
- Highly automated and sophisticated risk assessments using transitive inter-evidence point relationships

Supported by the following standards:
- ISO/IEC 15026
- ISO/TC 37 / OMG SBVR
- OMG Structured Assurance Case Metamodel
- Software Fault Patterns (Target late 2012)
- UML Security Policy Extensions (planned)
- Risk Assessment Metamodel (late 2012)
- Information Exchange Framework (MARS TF)
- Data Tagging and Labeling (MARS TF)

Software System / Architecture Evaluation

- Many integrated & highly automated tools to assist evaluators
- Claims and Evidence in Formal vocabulary
- Combination of tools and ISO/OMG standards
- Standardized SW System Representation In KDM
- Large scope capable (system of systems)
- Iterative extraction and analysis for rules

Supported by ISO/IEC 19506

Software system Technical Evidence

Executable Specifications

Software System Artifacts

Hardware Environment

Data Structures

SFP(CWE)

IA Controls

Protection Profiles

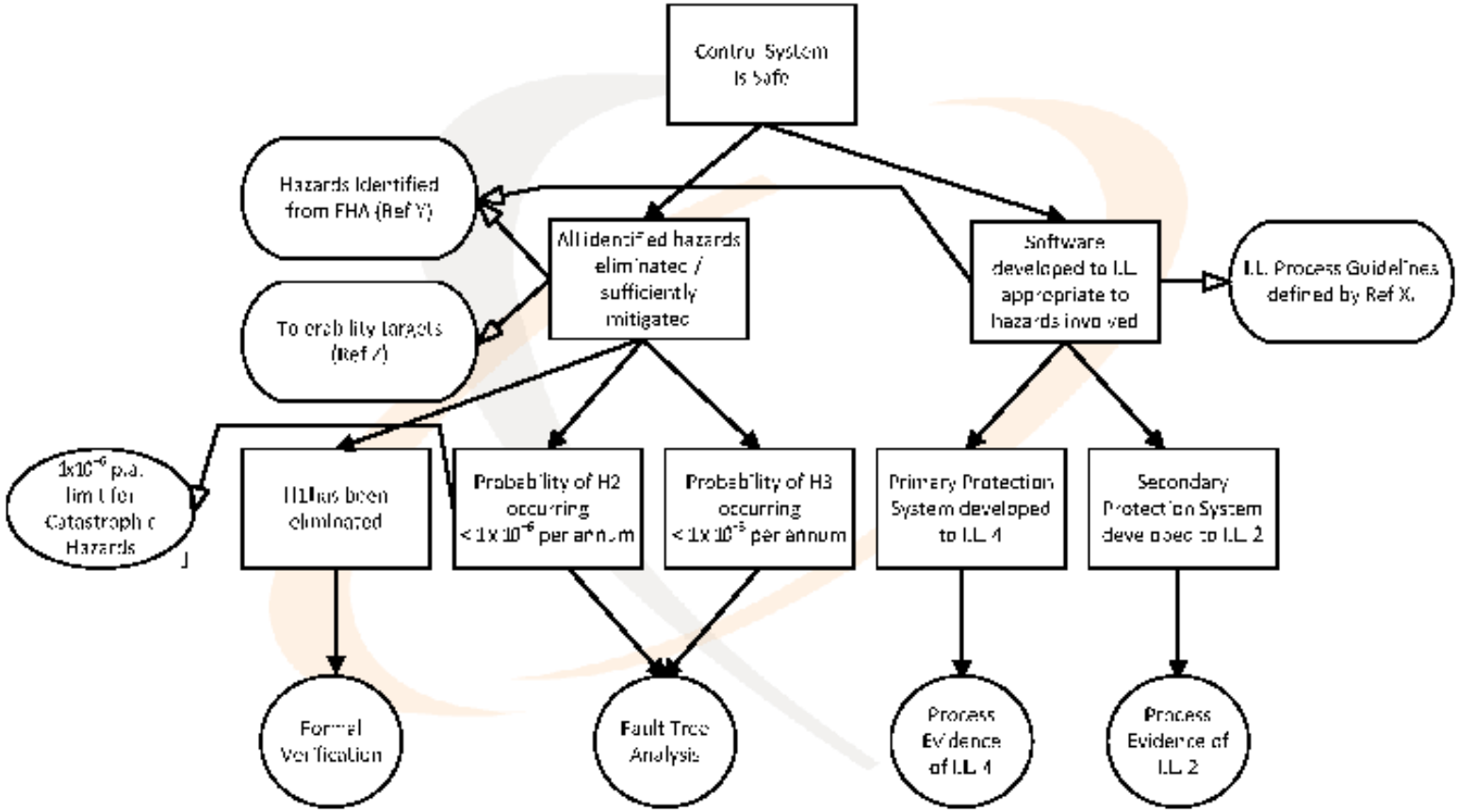
SACM

- Structured Assurance Case Metamodel
  - Software Assurance Evidence Metamodel
  - Argumentation Metamodel

- Claims-Evidence-Arguments

- SACM Open Source Implementation (Eclipse)
  - http://nasa.github.com/CertWare/

A Simple Goal Structure



OSD SwA Working Groups 2003

- What if ……. ?
  - Automobile vulnerabilities (e.g. OnStar), SCADA vulnerabilities, etc.
  - Wireless devices, Engine Controls, ABS….
- OnStar – GM Commercial: Car Chase, disable EEC.
- Researchers from the University of Washington and the University of California, San Diego, who were able to take control of cars via their OnStar network and force them to stop, turn off their engines, disable their brakes, or—most troubling—discharge window washing fluid with wanton abandon.
  - *Pick your news source of preference*

- "Cars hacked through wireless tire sensors"
  - Engine Control Units affected
  - http://www.technologyreview.com/communications/25962/ (MIT)
- Toyoto Untended Accel. - http://www.nhtsa.gov/UA

THE Open GROUP

Home | Login | Sitemap Search Blog

Subject Areas | Get Involved | Standards | Certifications | Events | Consortia Services | Software | Publications | About Us

Subject Areas

- Security
  - Trusted Technology
    - The Open Group Trusted Technology Forum
  - Cybersecurity
  - Events
  - Identity Management
  - Jericho Forum

Trusted Technology

Developing open standards for a more trusted global supply chain

The Open Group provides a collaborative, open environment for technology companies, customers, government and supplier organizations to create and promote guidelines for manufacturing, sourcing, and integrating trusted, secure technologies. Our objective is to shape global procurement strategies and best practices to help reduce threats and vulnerabilities in the global supply chain.

Governments and enterprises that use global standards in their technology strategy and purchasing decisions can rely on a more comprehensive approach to risk management and product assurance when selecting commercial off-the-shelf technology products. Vendors and suppliers that adhere to these practices will be able to better protect the integrity of their products and services as they move through the global supply chain.

Leveraging its more than 20 years of experience in creating industry best practices, standards, certification and accreditation programs for global organizations in all verticals, The Open Group provides guidance and a vendor-neutral collaborative environment for The Open Group Trusted Technology Forum (OTTF) members to identify industry best practices and define a globally recognized program for providers who implement the best practices.

Chair, Andras Szakal, IBM

OMG OBJECT MANAGEMENT GROUP

Interchangeability and “My Baby”

Term Discussion

- Interoperability – *(Generally connections between components)*
  - Brake lines are connections between Master Cylinder and wheel calipers. Braking Fluid is “the message”.
  - Gigabit, Ethernet, ATM, Firewire, 1553, Fibrechannel, etc.
  - Protocols: TCP/IP, UDP/IP, etc.
  - CORBA, DDS, Web Services

- Interchangeability / Portability – *The ability to isolate change due to DMS within the architecture!*
  - Car Parts: Bendix, TRW, Holley, Edelbrock, Aftermarket vs. OEM, etc.
  - 6U Form Factor, etc.
  - Embedded Avionics Systems:
    - CORBA, DDS
    - Operating Systems: POSIX, UNIX Single Specification, LINUX
    - Hardware: X86 processors (AMD, INTEL, etc), PowerPC (IBM, Motorola, etc.)

- Conformance vs. Compliance (Open Group, POSIX, UNIX)
  - Compatible (a MITRE standards term)

*COTS Middleware (CORBA, DDS, etc.) are examples of both Interoperability and Interchangeability attributes.

OSA Modular Avionics Objectives

Processing Architecture Objectives

1) Layered Commercial Open System Standards
Enables SW/HW Ease-Of-Change

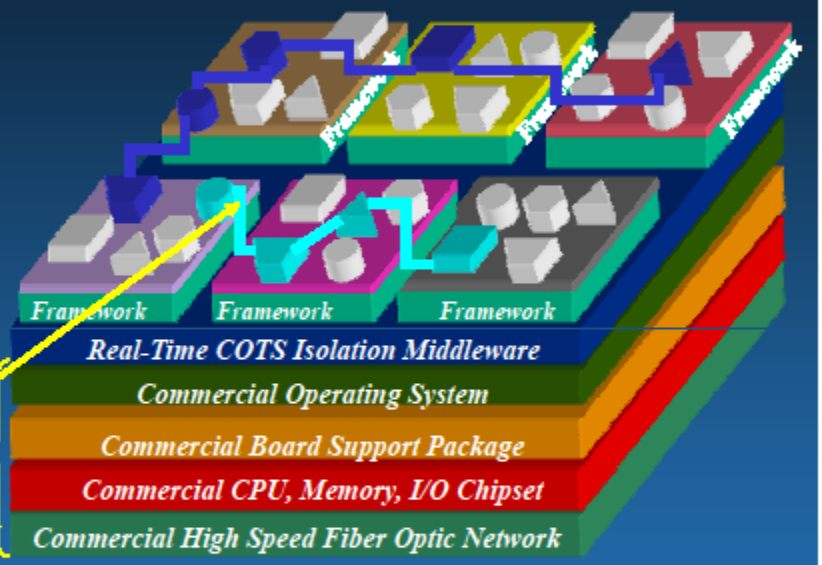
2) Hardware / Software Change Isolation
Enables Proactive Technology Refresh

3) Modular, Portable Application Software
Domain Engineering & Object Oriented Design to Enable Software Reuse

4) Common Processing Hardware Modules
Shared Cost … Economies of Scale

5) High-Speed Network
Enables Distributed Processing

6) Task Scheduling
"Hard Real-Time" Processing Constraints Met Across Distributed Processors



7) Data Security
Ability to Segregate Processing at Multiple Levels of Classification or Safety Criticality

8) Programmable Communications

- Rapid Insertion of the Latest Commercial Technology … Continuous Modernization
- Makes DMS Transparent to Customer

How to work with COTS

- The correct way for DoD-DIB's to use commercial technologies is to fund partner vendors to achieve capabilities that
  - *Make long term business sense*
  - *Are commercially sustainable*
  - *Meet specific needs of more than one program*
    - AND
  - *DoD ASSUMES NO OWNERSHIP!!!! Proprietary rights are retained by the vendor.*

Why COTS: An RTOS / RT-CORBA Example

- COTS Financial example : annual
  - *Assume 80 people at $120,000 per year (average)*
  - *Factor 3.5 X of avg. salary for overhead.*
  - *Add 30% profit margin*
  - *$43,680,000*
  - *@ $15,000 per copy (lower in bundles)*
  - *Sell 2,912 licenses to be viable*

Amortization is the Key

- A DoD Program purchases 40 licenses for a cost of $375,000
  - *out of $43 Million: Product Touch Labor : $10,000,000*
  - *∴ An equivalent in-house S/W product cost is ~$10 Million!*
  - *COTS Annual maintenance: $100,000.*
  - *In-house proprietary maintenance: ????*

Standards and the Defense Industrial Base[1]

- Adherence to Standards are <u>necessary</u> when:
  - Interoperability or Interchangeability are a key attribute of the component or lifecycle maintenance
    - Products with multiple suppliers which must work interactively (RT-CORBA, DDS, TCP/IP, Ethernet, …)
    - Products with multiple suppliers must provide interchangeability (POSIX, UNIX)
    - Products <u>*do not rely*</u> on <u>key patents or intellectual property</u> to function
  - Specialized requirements (safety, security, etc)
    - DO-178B, FDA Medical Devices, FIPS140-2, NSA / NIAP evaluations
  - Rapid technology advancement will DMS components in short time spans
    - Conforming to standard will provide a braking action to runaway feature creep.
  - Long term reusability is desired / mandated
    - Products built to Ratified or Defacto standards tend to retain stability between product releases because standards must be revised
      - Many Windows 98 applications still run on Windows XP (Vista / 7 ?)
      - Windows / LINUX / UNIX / POSIX OS's were minimally perturbed as the X86 processor family moved from 16 to 32 to 64 BIT architectures

Standards and the Defense Industrial Base[2]

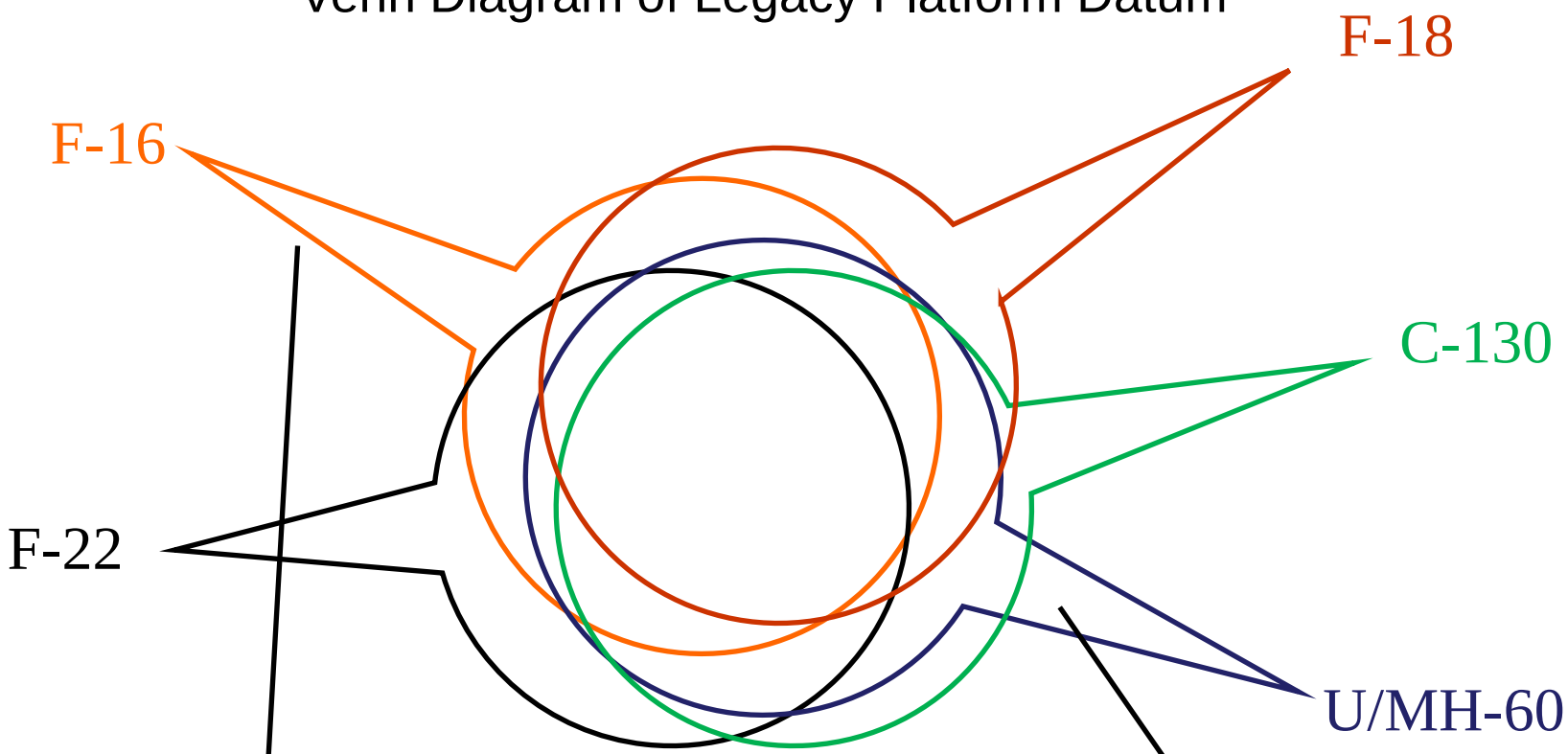
- Standards are <u>desirable</u> when:
  - Products are common, commercially available H/W or S/W computing infrastructure components
    - Widely available chip sets: CPU, DMA, I/O devices, video, etc.
    - POSIX conformant RTOS, RT-CORBA, DDS, etc.
    - …
    - <u>NOT</u> specialized EW sensor apparatus, radars, etc.
  - Products are predominately useful to the mainstream commercial market!
    - Products are equally usable in DoD and commercial systems and / or multiple DoD systems
    - Commercial viability can be (*not guaranteed to be*) problematic when product lines are too tightly constrained to specialized **<u>DoD only</u>** domains
    - Open Group Managed Consortium
      - Network Centric Operation Industry Consortium (originally TOG managed)
      - DirecNet™ - High Data Rate, Ad Hoc Communications Networks
      - Future Airborne Capabilities Environment (FACE): Business Committee WG's

FACE Conformance

- FACE standard has several layers (segments) for conformance
  - Safety, Security Technical WG's
- Key for cross platform reusability (the true capability) is the avionics data values on legacy platform.
  - A future airborne program with FACE conformant S/W and H/W infrastructure will easily support reusable FACE conformant capabilities and applications
  - Legacy platforms represent the vast majority (and potential cost benefit) of additional capability and applications
  - Legacy systems do not have uniform sensors, data values, infrastructures, etc.

FACE Data Interfaces

Venn Diagram of Legacy Platform Datum

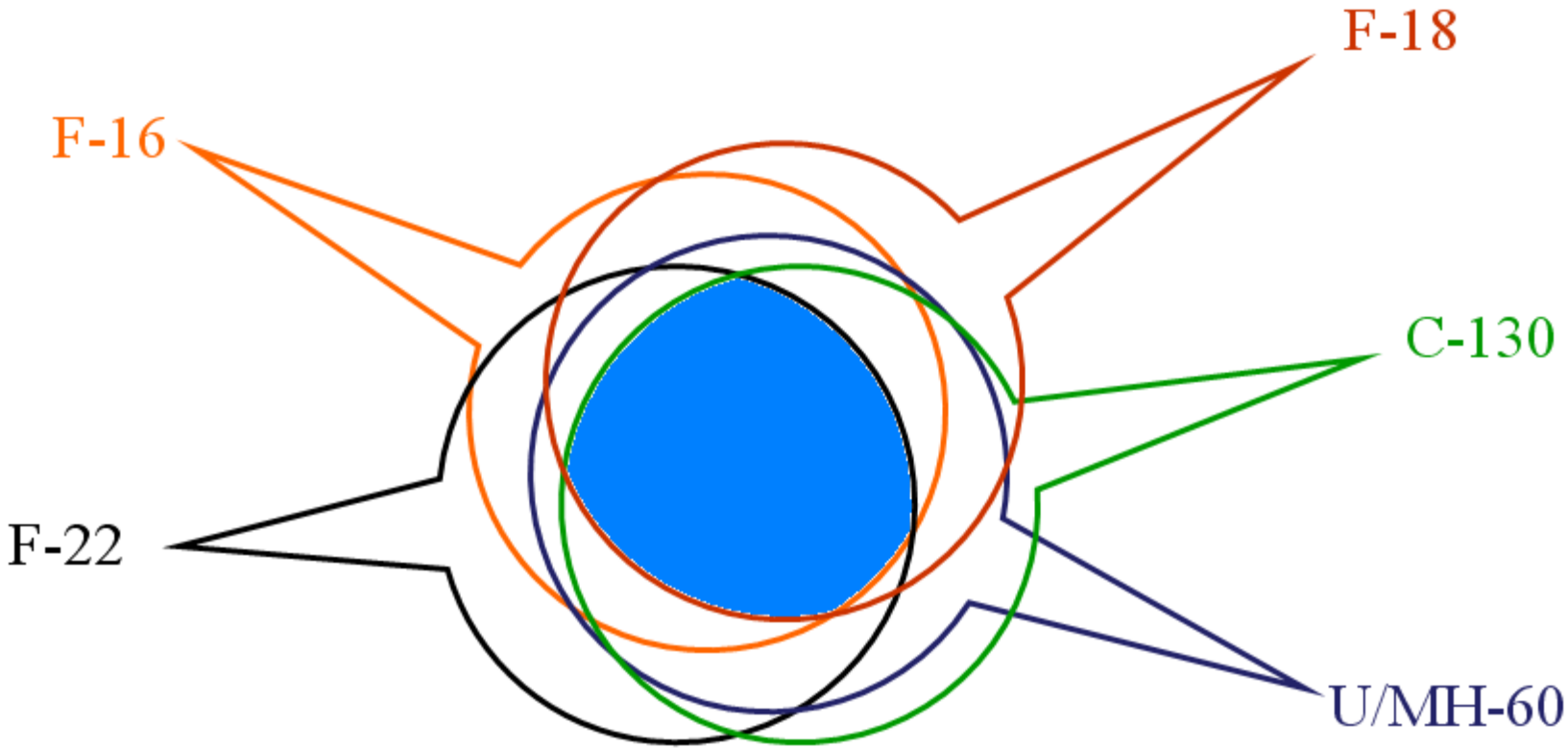


Data supported in F-16 OFP's

- Altitude
- A/S
- Position
- Heading
- ....

Data supported in Blackhawk OFP's

Intersection of all Platform Data Elements



- FACE could provide an API for the Intersection of all Platform Data points (Minima Approach: aka a **Baseline Profile** of FACE)
  - Applications written to Baseline Profile would run on ALL platforms *(Extremely Portable but may not leverage fuller capabilities of some platforms!)*

Current Acquisition Business Detractors

- COTS CORBA / DDS / RTOS Usage on a DoD Program
  - $375,000 for licenses
- Material Mgmt fee – ~6%
- CPFF – 10%(max*)
- Total Profit: $39,750

- CORBA / DDS / RTOS equivalent developed in-house
  - $10,000,000 direct labor
- CPFF – 10%
- Total Profit: $1,000,000

With a 2500% delta revenue:
Where is the financial incentive for DIB Contractors to buy COTS?
DoD needs to better incentivize ($$$) usage of standardized COTS!

*https://acc.dau.mil/CommunityBrowser.aspx?id=379516

sysa-chair@omg.org
ben.a.calloni@lmco.com