

# COTS and Safety Are They Mutually Exclusive?

BAE SYSTEMS



*Note: Large portions of this paper were derived from the work of the RTCA SC-190 to which both authors are members. This paper is designed as more of an infomercial than a replacement for the CNS/ATM Guidelines for Software Assurance which should be published late this calendar year and certainly contains substantive information not provided in this paper. It is highly recommended that all readers of this paper purchase the Guidelines when they become available.*

By: Ronald Stroup  
FAA Safety & Certification Lead

Warren Naylor  
BAE SYSTEMS System Safety Manager

# Defining COTS

BAE SYSTEMS



- COTS products encompass a wide variety of general-purpose off-the-shelf products, Non Developmental Items (NDI) and Previously Developed Software (PDS).

*Note: Some of these products are designed to be user selectable/modifiable (e.g., a compiler). Vendor supplied modifications or selectables are still considered COTS. However, it must be understood that once a program modifies or enhances COTS software to meet their respective system requirements, than the modified COTS must then be considered application code, subject to all certification requirements, without exception.*

# COTS Issues and Concerns

BAE SYSTEMS



- Obsolescence
- Version Control
- Vendor support
- Testing Issues (regression testing)
- Robustness of Vendor's testing is Unknown
- Inability to perform adequate structural coverage
- Maintenance
- Training
- Product Maturity
- Undisclosed Problems
- Absence of COTS Data (e.g., source code, test, validation, etc.)
- Vendor's Development Process is Unknown
- Lack of knowledge in determining the best COTS product for your needs
- Security



# Security Issues With COTS

BAE SYSTEMS



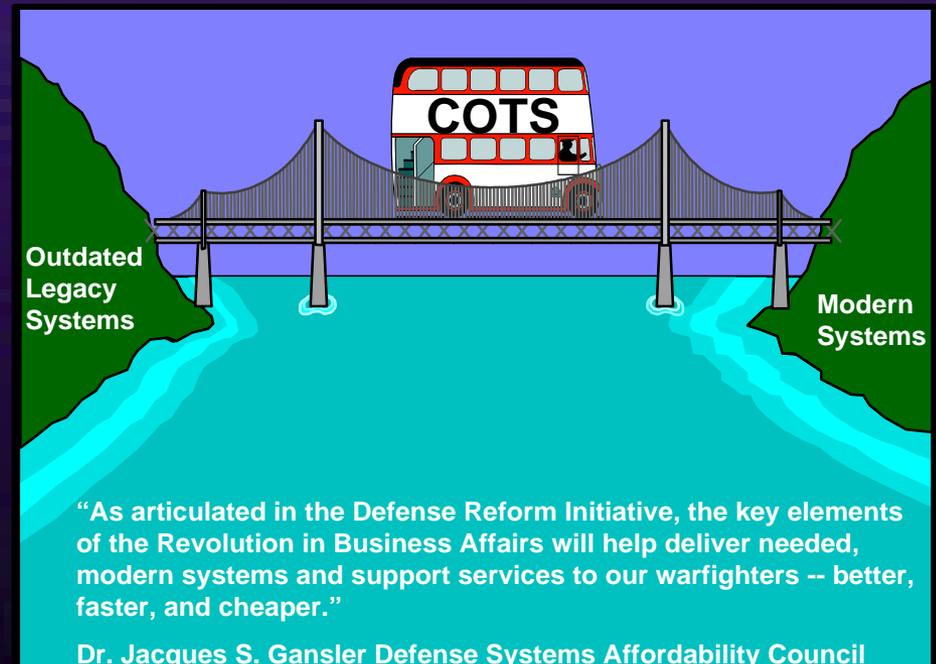
1. COTS products are inherently susceptible to intrusion
2. COTS developers are:
  - Outside the control of the developing and contracting organizations!
  - COTS development personnel in all likelihood, do not possess a security clearance!
  - Many COTS products are developed in designated countries which may be sympathetic and possibly even supportive of terrorist organizations!
  - Outside organizations know more about your vulnerabilities than you do and can take advantage of them!
  - Time bombs can be placed within code that is virtually impossible to detect without the source code, etc. !

# How Did We Get Here?

BAE SYSTEMS



Economic pressures and the much larger market place drive COTS products. The Government is no longer the leader or even a trendsetter in the market place. The Government has taken the position of Better, Faster, Cheaper and has identified COTS as the vehicle towards that end.



# Why COTS?

BAE SYSTEMS



- Primary drivers
  - Cost
  - Schedule
  - Timely replacement of legacy systems
  - Keeping pace with emerging technologies
  - Lack of viable alternatives

# Safety's Role

BAE SYSTEMS



**It is the safety community's responsibility to take a proactive leadership role in mitigating the risk of COTS.**



See,



Hear, &



Speak,

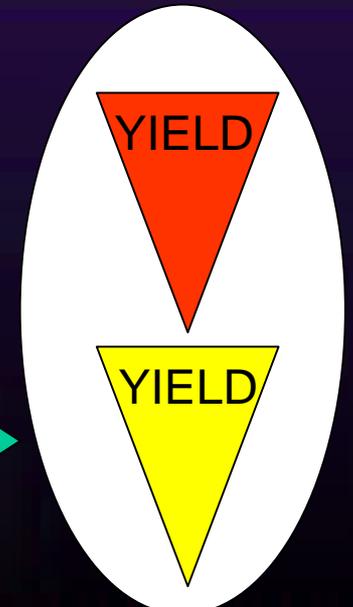
**No Evil**

# Safety Role (cont'd)

BAE SYSTEMS



- Safety cannot be perceived as a stop sign as program's will quickly learn to bypass safety to meet their objectives.
- We cannot, as a community, only present concerns and objections; we must also suggest solutions and alternatives.



More Effective

# Alternate Methods to Gain Assurance

BAE SYSTEMS



- The use of COTS often requires the use of alternate methods to gain assurance that the systems predefined acceptable residual risk levels are met. These methods may include:
  - Product service history,
  - Prior assurance,
  - Process recognition,
  - Reverse engineering,
  - Restriction of functionality,
  - Formal methods,
  - Audits and inspections.

Data may or should also be combined from more than one method to gain assurance data or an acceptable level of confidence is met.

# Alternate Methods to Gain Assurance (cont'd)

BAE SYSTEMS



- It should be noted that alternate methods are not the prescribed solution; they are what they are called, alternate methods, only to be used when:
  - Acceptable safety/certification data is unobtainable from the COTS vendors and
  - Cannot be produced by the developer.

# Defining a COTS Process

BAE SYSTEMS



- Planning Process
  - Strategic planning for implementation via a Strategic Lifecycle Technology Refresh Plan
  - Address COTS lifecycle issues
- Assessment Process
  - Requirements Definition
  - Assessment
  - Selection
- Verification Process
  - Demonstration of compliance to existing requirements
  - Alternate methods for verifying non-compliant objectives

# COTS Planning Process

BAE SYSTEMS



- Current implementation of COTS into mission/safety critical systems appears to be an ad hoc process
- Cost, schedule and safety are the apparent victims of this ad hoc process
- The successful implementation of COTS products into safety critical systems requires a formal standard process
- The need to define a COTS Process is long overdue

# Strategic Technology Refresh Plan

BAE SYSTEMS



- Your Strategic Technology Refresh Plan should include the following considerations:
  - Product availability
  - Requirements
  - Availability of lifecycle data
  - Ease of integration and extent of additional efforts such as glue code, architecture mitigation techniques etc.
  - Product Service history
  - Supplier qualifications such as use of standards, history and length of service, technical support, etc.
  - Configuration control including visibility into COTS supplier's product version

# Strategic Technology Refresh Plan (cont'd)

BAE SYSTEMS



- Modified COTS have additional considerations of warranty, authority to modify, continued technical support, etc
- Maintenance issues such as patches, retirement, obsolescence and change impact analysis
- Relationships among COTS planning process, acquisition process, integral processes should be defined
- Relationships between COTS processes and appropriate system lifecycle processes should be defined
- Ensure the COTS transition criteria are compatible with the system transition criteria and verifiable

# COTS Assessment/Acquisition Process

BAE SYSTEMS



- An unwise purchase of a COTS product could doom your program to cost and schedule overruns and more importantly induce safety instability that in all likelihood will never be adequately mitigated

# COTS Assessment/Acquisition Process Requirements Definition Process

BAE SYSTEMS



- Identification of software requirements COTS can satisfy
- Identification of excess features
- Derived or supplier provided definition of features
  - Examples include platform dependencies, interrupt handling, resource requirements, usage constraints, error handling, partitioning
- All COTS software requirements and the resulting derived requirements should be provided to the program's system safety assessment

# COTS Assessment/Acquisition Process

## COTS Selection Process

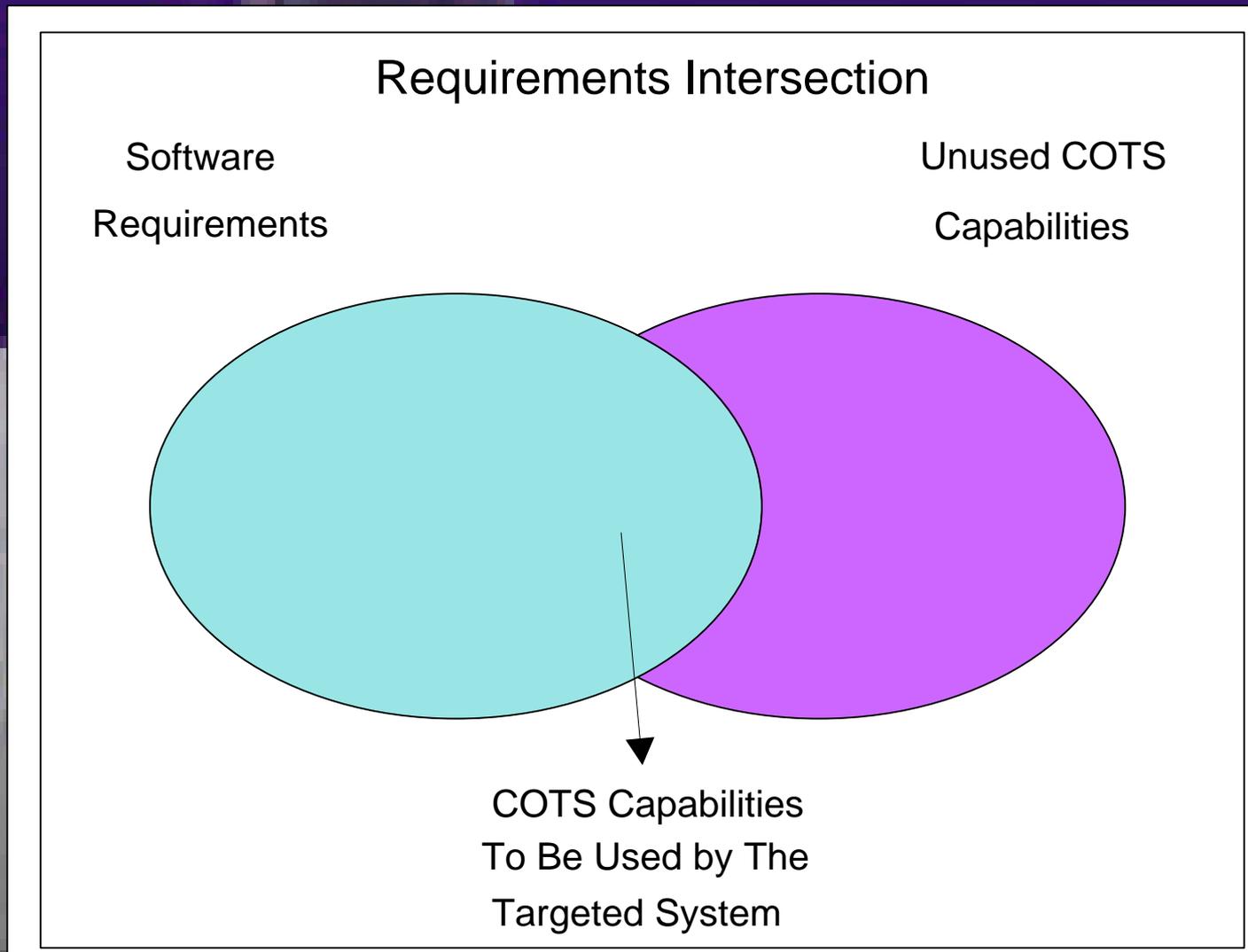


### BAE SYSTEMS

- Assessment of COTS candidates
  - Capability to implement the software requirements
  - Effect of their respective derived requirements
  - Support the assurance/severity level of the system
- Examine more than one COTS candidate at a time
  - Determine the extent of intersection of requirements with the system's software requirements
- Assess the availability and relevance of COTS life-cycle data to support the assurance level of the system
  - Comparison of COTS suppliers
    - Experience in the respective system
    - Capability to support COTS software version control and maintenance over the expected lifetime of the system
    - Commitment to keep the system design agent informed of detected errors
    - Willingness to address the issue of escrow
  - Comparison of COTS vs developing the software
- Assess impact of any unneeded features present in the COTS software

# COTS / Application Requirements Intersection

BAE SYSTEMS



# COTS Verification Process

BAE SYSTEMS



- **Common misconception:**
  - The inclusion of COTS would reduce the level of testing. The theory is that the vendor prior to purchase has previously tested the COTS products.
- **The truth:**
  - This theory has serious flaws as the thoroughness of vendor testing cannot be verified or validated. In fact one cannot even verify whether known problems were corrected.
  - Additionally, products from one manufacturer must be integrated with products from others and incompatibilities are not uncommon
  - The inclusion of COTS products into mission critical and safety critical systems has actually increased the necessity and duration of testing.

# COTS Verification Process

## Regression Testing

BAE SYSTEMS



- When and to what extent should regression testing be performed?
  - Regression testing was performed in legacy systems whenever safety critical or mission critical requirements were modified. The robustness of the testing corresponded directly with the assumed risk of the modification. This remains true in a COTS based system
  - The inclusion of COTS has introduced additional testing requirements

# Integral Processes

BAE SYSTEMS



- Configuration Management
  - The system CM should include control of the COTS version/s
- Quality Assurance
  - Assesses the COTS processes and data outputs to ensure requirements associated with COTS are satisfied

# COTS Verification Process

## Regression Testing-Worst & Best Cases

BAE SYSTEMS



- When is a complete retest required
  - Whenever an Operating System is replaced and possibly even upgraded
  - Whenever the software of the system is not fully portable to an upgraded processor forcing a recompile
- When is regression testing minimal
  - Non-critical HW specific upgrades or replacements such as output devices for data, etc may require minimal function specific retesting
  - Non-critical SW specific upgrades or replacements such as data recording/retrieval, etc may require minimal function specific retesting

*Note: Any determination of the breadth and necessity of regression testing can only be made after a risk analysis has been performed and documented on the proposed upgrades*

# Any Questions?

BAE SYSTEMS

