Cybersecurity of Ground Systems

GVSETS GROUND VEHICLE SYSTEMS ENGINEERING & TECHNOLOGY SYMPOSIUM
& ADVANCED PLANNING BRIEFING FOR INDUSTRY

NDIA Michigan

Secure Rapid Prototyping of Unmanned Systems

Hal Aldridge, Ph.D., hal.aldridge@secmation.com
Fred Livingston, Ph.D., fred.livingston@secmation.com
Secmation

4/4/2023

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

Unmanned Systems Cybersecurity – Evolving Policy

- Cybersecurity is a growing concern in Unmanned Systems
- As developmental systems/capabilities transition to operational use, many will need significant cybersecurity updates slowing deployment
- While air applications have been the most affected to date by security processes/required certifications, other domains will likely be "catching up" soon
- **How do we accelerate the design process to keep up with the rapid evolution of unmanned systems without leaving cybersecurity behind?**

National Defense Authorization Act-NDAA

FY2020 NDAA SEC. 848. PROHIBITION ON OPERATION OR PROCUREMENT OF FOREIGN-MADE UNMANNED AIRCRAFT SYSTEMS.

(a) PROHIBITION ON AGENCY OPERATION OR PROCUREMENT.— The Secretary of Defense may not operate or enter into or renew a contract for the procurement of—

(1) a covered unmanned aircraft system that—

- (A) is manufactured in a covered foreign country or by an entity domiciled in a covered foreign country;
- (B) uses flight controllers, radios, data transmission devices, cameras, or gimbals manufactured in a covered foreign country or by an entity domiciled in a covered foreign country;
- (C) uses a ground control system or operating software developed in a covered foreign country or by an entity domiciled in a covered foreign country; or
- (D) uses network connectivity or data storage located in or administered by an entity domiciled in a covered foreign country

SecMUAS – Secure Modular Unmanned Aerial Systems

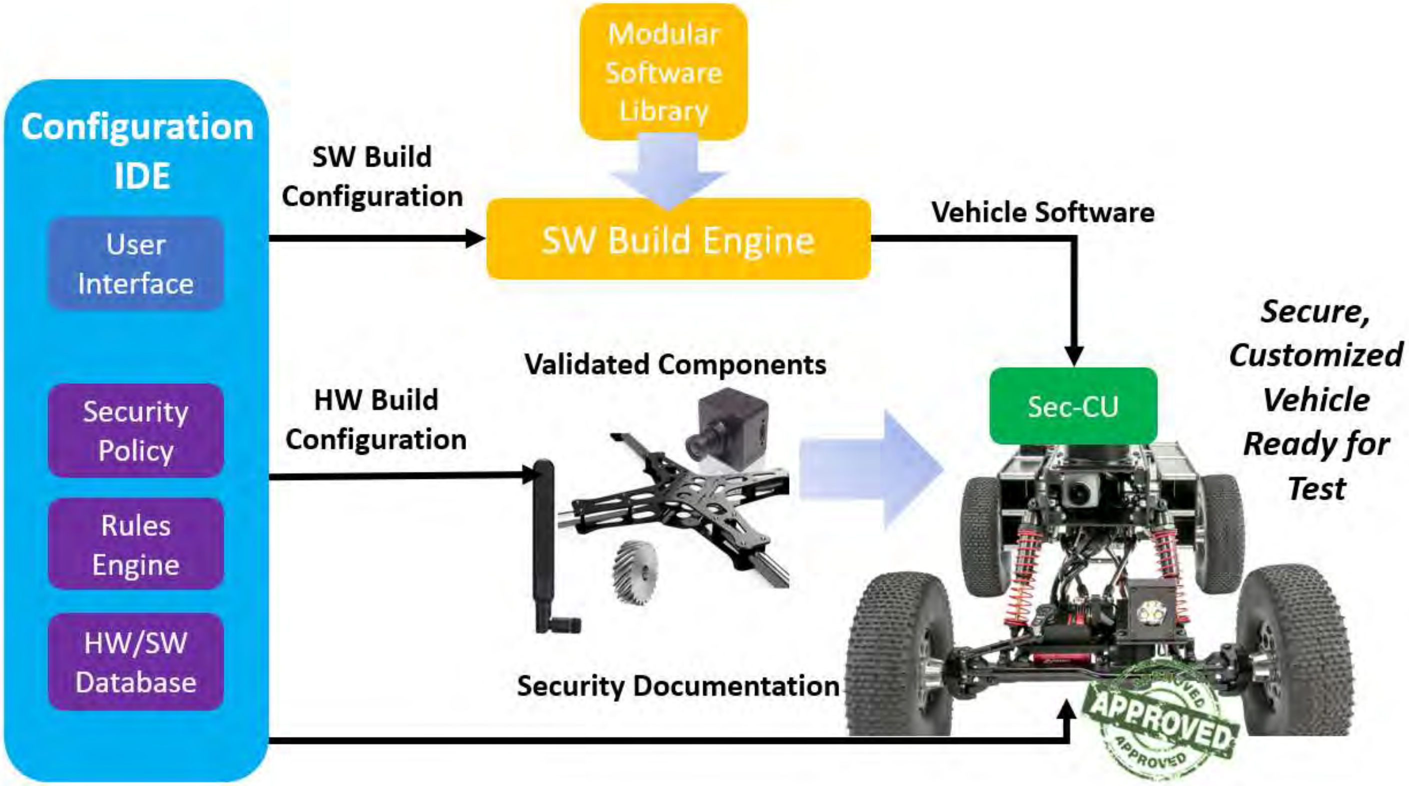
- Goal: The goal of the SecMUAS program is to enable the rapid, modular, security-enhanced unmanned systems design process
- Customer: Office of Naval Research. Code 351, Air Warfare and Weapons.
- ONR TPOC: Dr. David Gonzalez (david.r.gonzalez@navy.mil)
- Contract: Phase II SBIR

While SecMUAS initial demonstration target is air systems, the system is being designed to handle ground, surface, underwater, and space applications

What makes SecMUAS Unique?

- Assist unmanned system designers to build in cybersecurity early in the design process
- How?
  - Automate security policy enforcement. Designer does not need to be a cybersecurity expert to develop a system than meets security policy requirements.
  - Provides a selection of hardware and software components with known pedigrees that can be re-used
  - Security architecture enforcing strong isolation, multiple radio/crypto options, and other cybersecurity functionality supporting cybersecurity in contested environments
- Automated document generation on cybersecurity controls implemented to enforce security policy assisting in approval process.

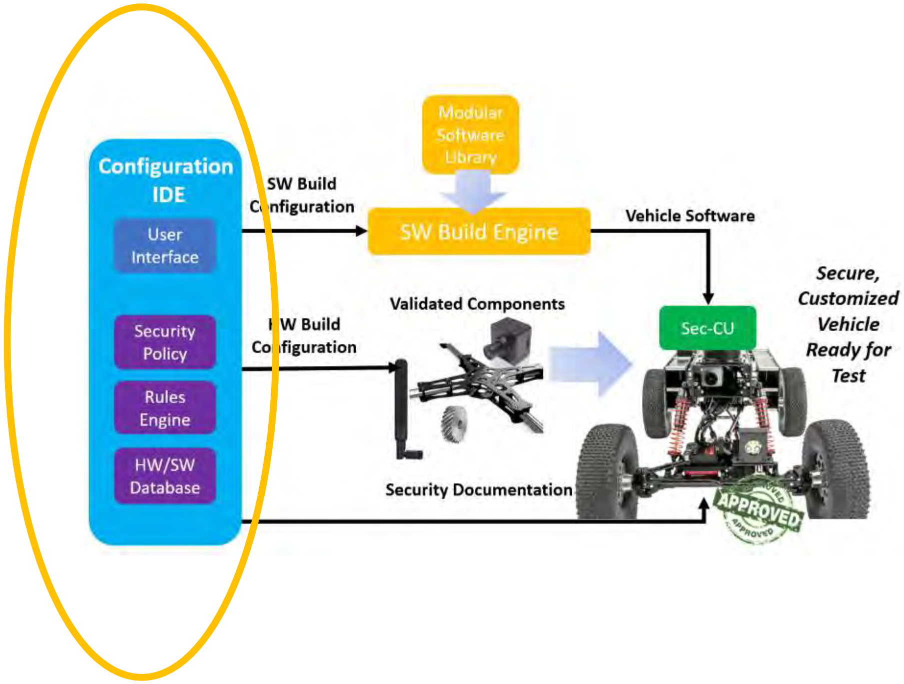
SecMUAS Overview



SecMUAS "bakes-in" security to modular unmanned systems enabling rapid transition to the warfighter

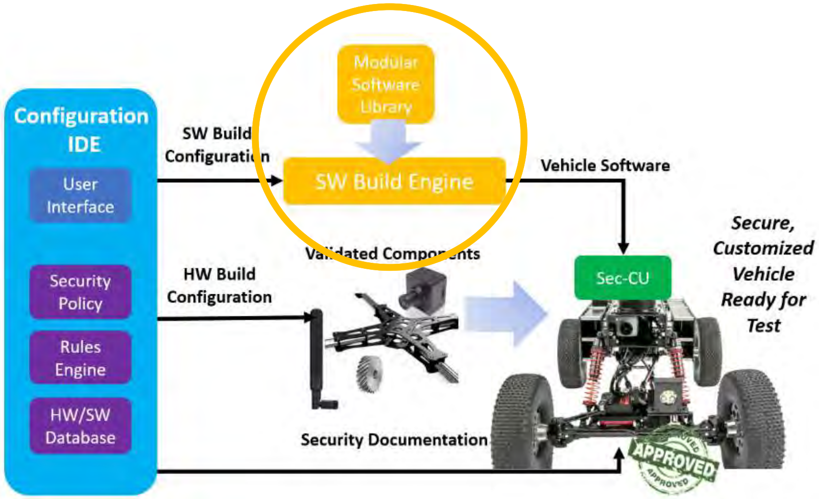
Configuration IDE

- Primary interface to designer
- Enables selection, connection, and configuration of components
- Enforces security policy in design
- NOT an engineering design tool (e.g. MATLAB/Simulink)



Software Build System

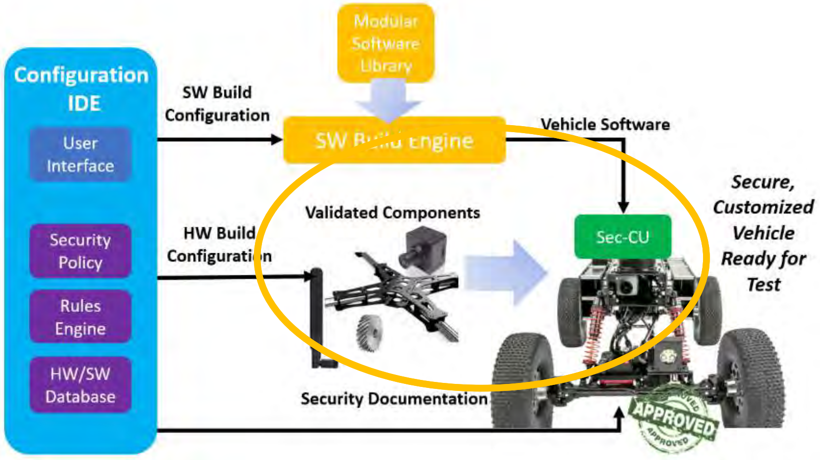
- Takes system configuration defined in Configuration IDE and automates software build
- Uses components from Modular Software Library (MSL)
- MSL can be extended through use of defined templates
- Designed to work with components from Simulink Code generation and other resources (e.g. ROS) with minimal modifications



DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

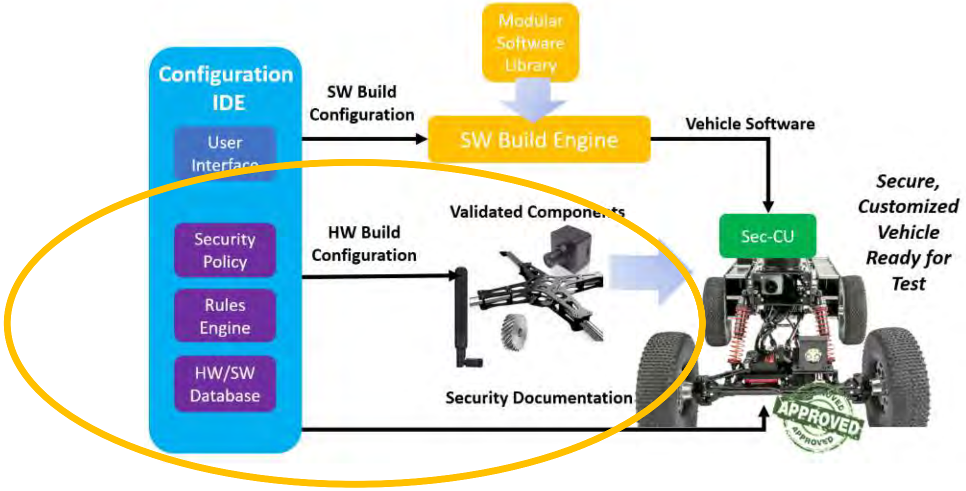
Secure Supply Chain

- Supply chain is an important cybersecurity risk for unmanned systems
- SecMUAS uses Sec-CU, a US designed controller with a secure supply chain, as a Root of Trust for SecMUAS
- Hardware component library with options from verified vendors



Document Generation/Security Approval

- Security documentation can be a “long-pole” in obtaining required certifications/approvals
- SecMUAS knows the security policy (e.g. certification requirements) and security controls selected to enforce the policy
- Security documentation is automatically generated to documents the as-built security design of the system



DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

Ground Systems Relevance

- SecMUAS adapts the modular component concepts from the ROS software framework. The vehicle control stack consists of a collection of nodes.
- Support for nodes allows researchers and developers, such as the ROS-M community, for fast integration into the SecMUAS ecosystem.
- The selection, arrangement, and interconnection of these nodes are responsible for unmanned system behavior. SecMUAS uses Data Distribution Service (DDS) as its middleware for components interactions.

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

Way Forward/Conclusion

- Development Schedule
  - Q1FY22 – Initial SecMUAS release
    - Early feedback/evaluation
    - Simulation support only
  - Q4FY22 – Second SecMUAS release
    - Initial capability to support unmanned system development
    - Demonstration quad-copter developed using SecMUAS in flight and security testing
- Looking for “early adopters” in all application domains including ground

DevSecOps for Next-Generation Unmanned Systems