AUTONOMYLOCK™

Rapidly Deploy Secure Autonomy

Deploy Advanced Autonomy Rapidly and Securely with AutonomyLock from Secmation

MEETING THE CHALLENGES

and demands of a swiftly evolving and growing market for autonomous systems requires tools which allow rapid development and deployment of secure autonomous systems. Secmation's AutonomyLock provides an intuitive engineering development tool for UxS designers and integrators to reduce the cost of development and deployment of autonomous systems by providing an automated framework for the application of security controls and the generation of security compliance documentation. AutonomyLock automatically identifies and applies security controls consistent with certification standards such as DIU's BlueUAS, AUVSI's GreenUAS, and AUVSI's Trusted Cyber Framework, allowing the UxS developer to focus on control system design instead of implementing security controls.

AUTONOMYLOCK™ speeds the deployment of autonomous capabilities by allowing direct incorporation of control systems designed in MATLAB, Simulink, and ROS (Robot Operating System). This allows an autonomous systems developer to design a system in a known tool, import to AutonomyLock to secure the system, and use AutonomyLock to rapidly deploy the system to secure hardware. AutonomyLock also provides a direct interface to simulation toolsets, such as Gazebo, which allows the developer to test a secure control system in a simulation environment prior to deployment, decreasing the cycle time for iterative development of control systems.

KEY FEATURES

- Intuitive drag-and-drop interface reduces learning curve
- User-selectable security policy automatically applies security controls, saving time and money
- Automatic generation of security compliance documentation significantly reduces cost associated with obtaining security certifications
- Direct import from MATLAB/Simulink leverages existing industry knowledge to reduce development time
- Direct output to Gazebo simulation allows real-time analysis of control laws, reducing test cycle time
- Execution environment secured using industry best practices, providing confidence that a deployed system is secure
- Existing repository of hardware and software components to be re-used to reduce development time

SECMATION 15200 Weston Parkway, Suite 103, Cary, NC 27513 • sales@secmation.com • (919) 887-2560 • www.secmation.com

AutonomyLock Integrated Development Environment and Secure Hardware

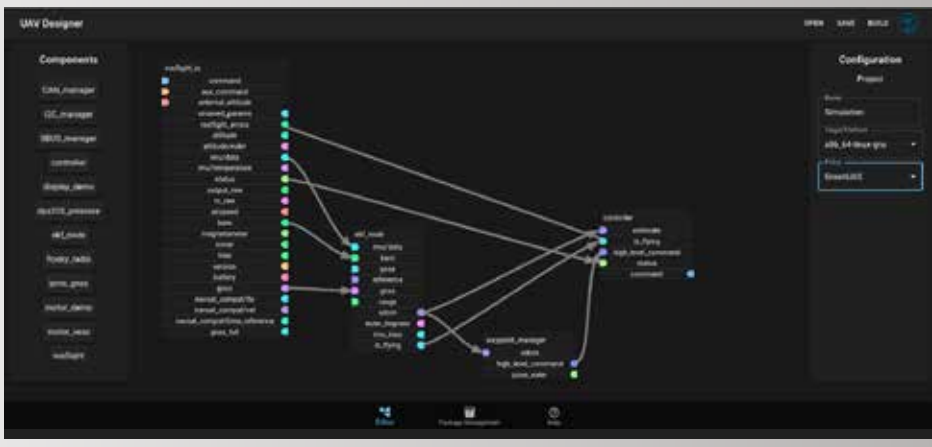
THE AUTONOMYLOCK Integrated Development Environment (IDE) provides the control system developer an intuitive drag and drop interface to connect different components of the control system. The unique value provided by AutonomyLock is that the connections created within the IDE are combined with the security policy rules for the selected regulatory standard to produce a functional autonomous system which is security-compliant out of the box. The AutonomyLock IDE automates the software build process and produces a digitally signed software package ready to execute on secure hardware or in simulation using the integrated Gazebo-based visualization.

The AutonomyLock secure hardware provides a ready-to-use secure computing environment for rapidly deploying autonomy to UxS. The secure hardware includes a secure processor integrated with a FIPS certified Hardware Security Module and security hardened Linux operating system. The secure hardware provides a powerful 1.5GHz, quad core Arm A35 based CPU for execution of autonomy software along with a user configurable set of interfaces including Dual Ethernet, CAN, RS-232, USB, I2C, UART, GPIO and PWM. The secure hardware supports the ability to network multiple units together to increase the total compute power available for a particular control system. Additionally, the secure hardware can serve as a secure bridge to special purpose processing such as AI accelerators by isolating them from external security threats.

Rapidly deploy secure autonomy to target UxS using the AUTONOMYLOCK™ Secure Hardware

Secure Hardware Specifications

Size	5” x 3.5” x 1”
Weight	6.4 oz.
Power	15W, 6-36 Vdc
Processor	Colibri iMX8X
Connectors	USB-A, RJ-45 (2), 4-pin JST (2), 6-pin JST, 40-pin JST



Rapidly design secure autonomous systems using the AutonomyLock IDE

Need help determining certification requirements?

Ask us how we can help you get security certifications for your UxS faster and cheaper!

Streamlined Security Certification:

Security certification processes are notoriously time consuming and expensive to complete. AutonomyLock provides the ability to select a pre-configured security policy aligned directly with the target certification standard like DIU’s BlueUAS or AUVSI’s GreenUAS standards and will automatically apply the necessary security controls to meet the certification standard. AutonomyLock also automatically produces security compliance documentation including a list of controls implemented for specific requirements and a full Software Bill of Material (SBOM), both of which are key enablers for security certification. AutonomyLock saves time and money by automatically applying security controls and documenting them through a repeatable process allowing certification reviewers to efficiently review new systems using familiar documentation formats.

Want to use your own hardware?

Ask us about hardware design licensing and options for integration with custom hardware!

Rapid Prototype Development

AutonomyLock allows developers to move from design concept to secure operation faster than ever before. With built-in support for ROS that includes building a custom secure wrapper for ROS code, AutonomyLock provides access to a vast library of existing automation capabilities which can be securely deployed. AutonomyLock similarly provides support for the MATLAB and Simulink products developed by MathWorks, allowing a developer to directly import control systems from these tools and automatically secure them using the AutonomyLock tools. The same security controls are also available to custom functions written by the developer, allowing the developer to focus on creating a functional control system instead of security compliance.