Operating Room Integration and SECURITY around AV systems –

Transition to IP based AV integration comes with the question – Is it cybersecure ?

The information and guidelines provided in this document are applicable to the JAM-Labs ORION ORI Server (API) and ORION end-point devices implementing the BlueRiver solution.

As the world is becoming more connected, we are seeing an enormous number of network-connected products. However, it has been found that a significant amount of these products lacks even basic and fundamental security capabilities. For this reason, the new age of interconnected conditions requires introducing regulations to require connected products to be more secure, and accompanying standards and guidelines are being introduced by industry to help products address these new challenges.

JAM-Labs based ORION comes fully certified and ensured to support MARKET CLAIM VERIFICATION (MCV) baseline-driven security verification framework that groups sets of industry-referenced security best practices based on their necessity for implementation.

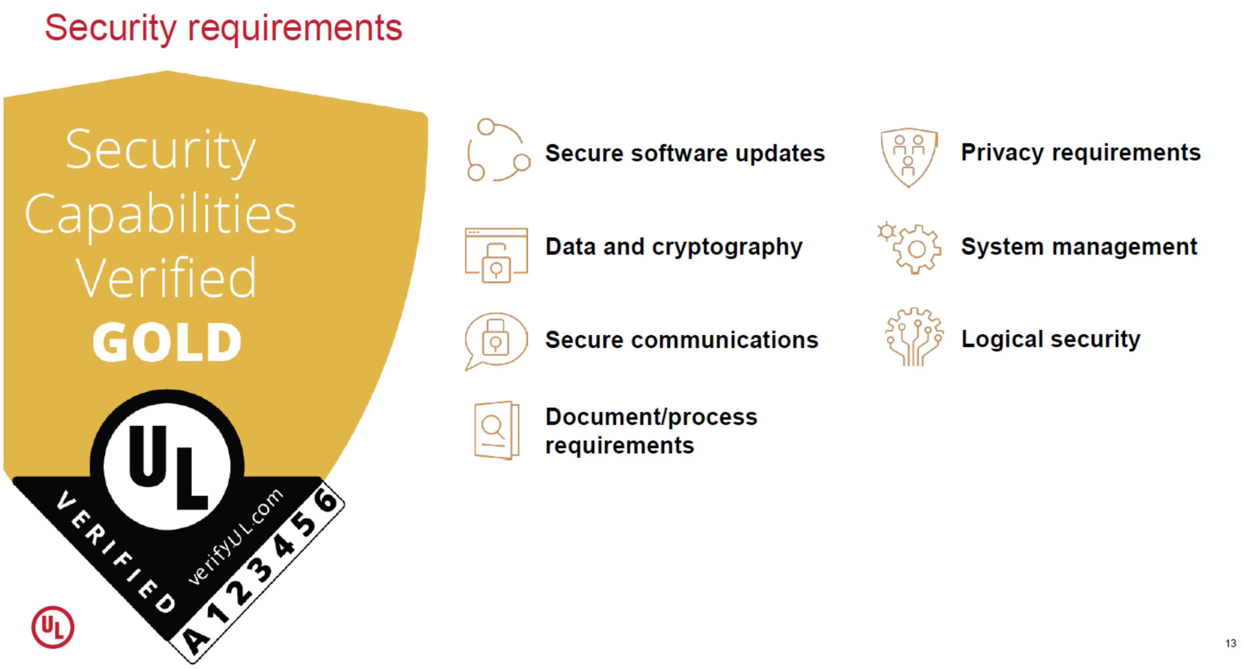
Level 1 references best practices that are considered an absolute minimum (a 'baseline') for any connected device, followed by 4 more levels of increasingly expanding sets of industry-acknowledged security capabilities that become more advanced and comprehensive in nature. References to leading security frameworks, such as EN 303 6451, NISTIR 8259A2, the CSDE C2 Consensus Report3.

JAM-Labs adheres and ensures the security maturity of ORION product, prioritize the implementation of device security capabilities, and plan for product security maturity growth. Additionally, it provides buyers/end users of our solutions the opportunity to formulate concise security requirements in line with industry best practice.
The current framework is derived from the inspiration and backbone of several industry security verification solutions, such as UL's Security Rating, retailers' connected devices security test protocols, and it is accepted by the Design Lights Consortium (DLC) as a security assessment framework for networked lighting controls.

Five-level rating

Diamond, Platinum, Gold, Silver or Bronze

Security Capabilities Verified DIAMOND
Security Capabilities Verified PLATINUM
Security Capabilities Verified GOLD
Security Capabilities Verified SILVER
Security Capabilities Verified BRONZE
UL
VERIFIED
verifyUL.com
A123456


Security
Capabilities
Verified
GOLD
UL
VERIFIED
verifyUL.com
A123456
UL

Security requirements

- Secure software updates
- Data and cryptography
- Secure communications
- Document/process requirements
- Privacy requirements
- System management
- Logical security

UL’s Security Rating aligns with

- California Bill for the Cybersecurity of Connected Devices (SB-327)
- NIST Cybersecurity Capabilities Baseline
- UK Code of Practice for Consumer Security/ ETSI TS 103 645
- EU Cybersecurity Act (ST 15786/18)
- Amazon Alexa Voice Service Security Best Practices
- ENISA Baseline Security Recommendations
- IoT Alliance of Australia IoT Security Guideline
- PCI PIN Transaction Security
- CTIA Cybersecurity Certification Program
- CTA/CSDE C2 Consensus on Device Security Baseline Capabilities
- GSMA Security Guidelines
- +many more