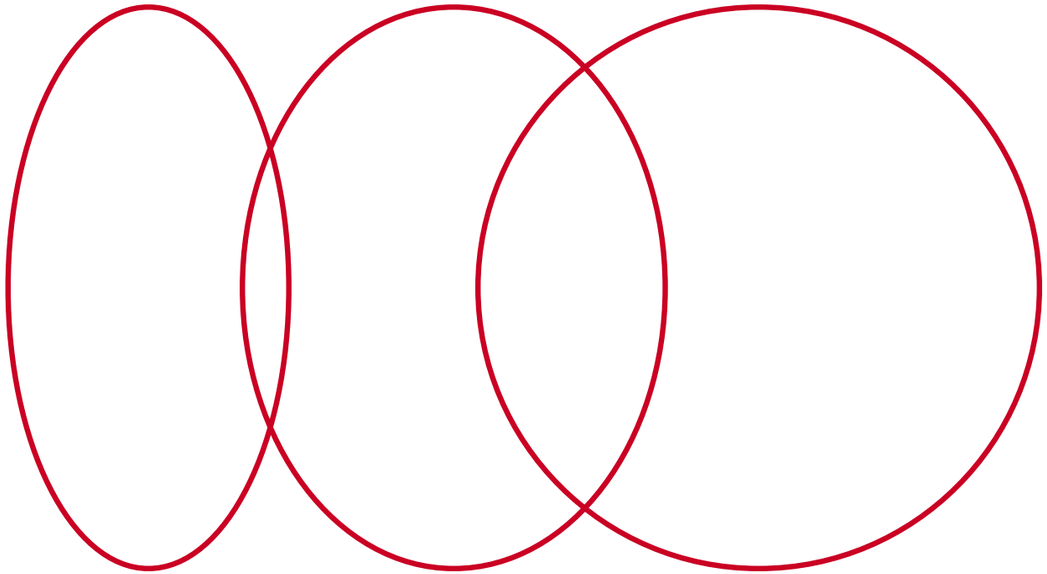
Cybersecurity of medical devices

LET’S GO

UL Solutions

Safety. Science. Transformation.™

Table of contents



Relevant standards 5

Systems engineering process 6

System requirements gathering 8

Design 8

Implementation 9

Release 9

Maintenance 10

Strategies for success 10

Benefits to different roles in your organization 11

Why UL Solutions? 12

Cybersecurity of medical devices

Why is the term “cyber secure” increasingly important, and how “secure” is “secure enough?” Learn how to plan for cybersecurity in your organization with the tools available to produce more cyber secure medical devices.

UL Solutions offers manufacturers of medical devices and health and wellness products guidance to navigate a complex regulatory environment and meet critical patient needs. This is especially important for the cybersecurity aspects of medical devices because both rapid innovation and regulatory changes are happening at the same time.

For example, the U.S. Food and Drug Administration (FDA) amended the Food, Drug and Cosmetic Act (FD&C) in 2023. Section 524B(b)(2) requires, among other things, that manufacturers of cyber devices design, develop and maintain processes and procedures to provide a reasonable assurance that the device and related systems are cyber secure.

So, not only does the growing complexity of medical devices require more advanced testing and certification to evaluate cybersecurity, but the documented processes of manufacturers are being scrutinized. By collaborating with a trusted third party to develop a comprehensive testing strategy, manufacturers of medical devices and laboratory equipment can streamline testing and certification, save time and simplify compliance.

Relevant standards

To help manufacturers understand what is expected, the FDA has highlighted two standards that are particularly useful:

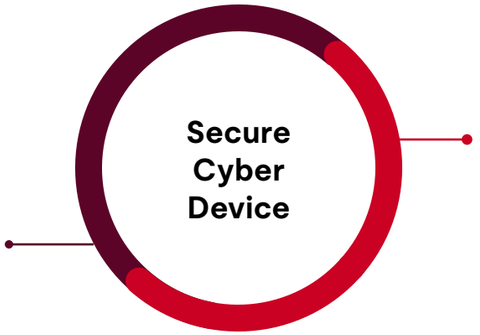
- UL 2900-2-1, the standard for Software Cybersecurity for Network-Connectable Products of Healthcare and Wellness Systems
- IEC 81001-5-1, Health software and health IT systems safety, effectiveness and security activities in the product life cycle

The UL 2900 Standard was written with FDA pre- and post-market cybersecurity and American National Standards Institute (ANSI) Technical Panels guidelines in mind. The standard also supports regulatory submission processes found in FDA guidance. These two standards work together to cover both the product and the processes followed to create it.

UL.com/Solutions

How UL 2900 and IEC 81001-5-1 interrelate

When used in tandem, these two standards can address many aspects of product security:



IEC 81001-5-1
Processes and Objectives

Provides more specificity on the **processes** that need to be addressed

UL 2900
Product Implementation and Verification

Provides more specificity on the **implementation or testing** details that need to be addressed

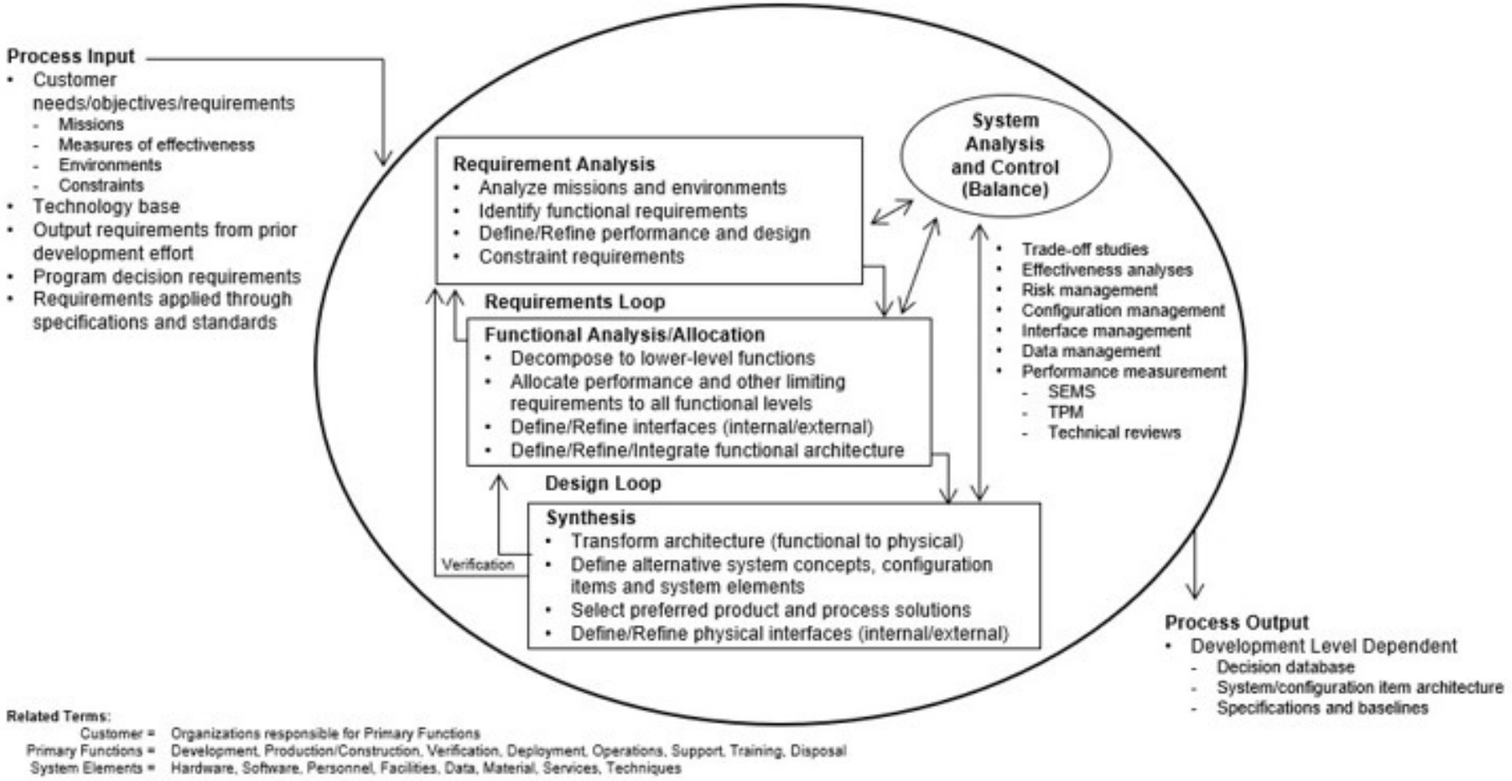
Together, these two standards help manufacturers of medical devices demonstrate they implement adequate quality management and software development life cycle processes as well as generate the proper testing and verification artifacts that can be useful when dealing with regulatory issues.

Systems engineering process

By highlighting these two standards, the FDA has made it clear that it expects manufacturers of medical devices to start systems planning early. Product security is critical, of course. That is why establishing safety and security processes — especially those that align with regulations and standards — is also critical. This is especially true when the end product is entirely an intangible product, like software. Software products are ultimately a function of the development processes designed to create them.

One way to do this is to follow the systems engineering process.

Simplified Example:
Software controlled ventilator



Source: http://www.dau.mil/pubs/pdf/SEFGuide%2001-01.pdf "Systems Engineering Fundamentals."] Defense Acquisition University Press, 2001

This process begins by gathering process inputs, such as customer needs and requirements; time, budget and material constraints; and goals to measure success. The next steps then loop until a satisfactory process output is achieved:

- Requirements analysis
- System analysis control
- Functional analysis and allocation
- Design synthesis
- Verification

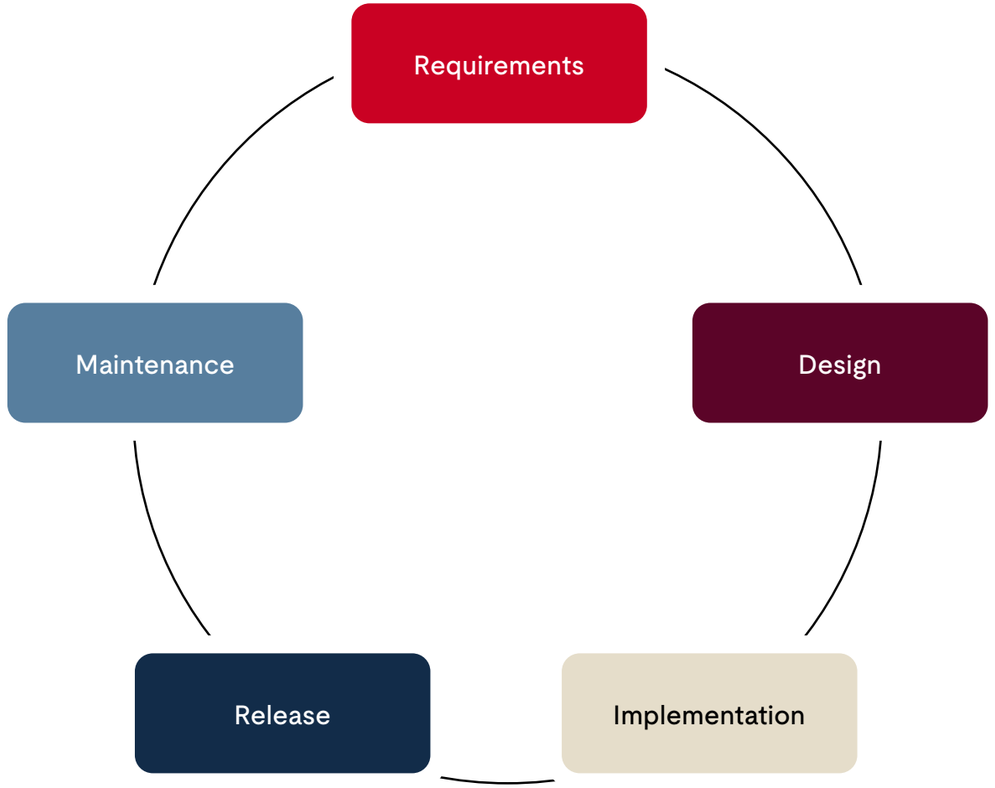
Besides the device itself, this process will help manufacturers produce artifacts that can help demonstrate that goals have been attained so that stakeholders, such as regulators and purchasers, will have necessary documented proof.

A good system engineering process will have:

- **Inputs** that are clear and well-defined
- **Processes** that move you toward your goals
- **Outputs** that demonstrate that you have attained those goals

One way to keep your process on track is to design traceability into it. Traceability requires configuration controls, such as versioning and documentation. And this traceability must be present throughout all stages of the product life cycle:

- System requirements gathering
- Design
- Implementation
- Release
- Maintenance



System requirements gathering

This first stage is important to set the goals for the project. What consumer need is being addressed? What are the intended uses? What are potential risks that need to be planned for? What technology will be used?

Example: System requirements

Inputs	Process	Outputs
• Customer needs • Intended uses • Risk Analysis (Threat model) • Technology	• Technical adaptation • Hazard Analysis (Threat model) • Hazard Mitigation • Decisions • Management Reviews	• Requirements that meet the customers needs • Requirements that address identified hazards • Specifications that are clear and useable • Sign-off

Design

These same inputs, processes and outputs remain important during the design stage. What requirements can you meet? How will you design the overarching architecture of the product? How will you design the user interfaces? How will your document data flow?

Example: Design

Inputs	Process	Outputs
• Requirements • Specifications	• High level software design • Hazards addressed • Architecture, modularization, partitioning • Interfaces defined • Design reviews	• Block diagrams, control flow and data flow • Safety / security critical software separated from non-safety / security critical software • HW/SW; SW/SW; User interfaces • Review reports

Implementation

For the implementation stage, the inputs are the designs created in the previous stage, and the processes developed include the selection of the coding language and version control tools. The outputs are the source code documentation, data models and test results.

Example: Implementation

Inputs	Process	Outputs
• Design • Architecture	• Defined implementation practices • Writing code coding metrics • Coding language, version control including tools • Testing for hazardous states, security, performance, and functionality	• Source code documentation • Data models, libraries, etc. • Test results

Release

The inputs of the release stage include the implemented code. The processes are the version control, testing and validation steps taken. And the output is, naturally, the completed product and the acceptance thereof by management and customers.

Example: Release

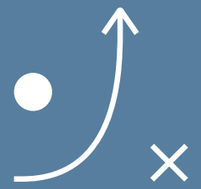
Inputs	Process	Outputs
• Implemented code	• Version control • SW/HW integration • Testing for hazardous states, security, performance and functionality • Validate to requirements, customer needs and intended uses	• Complete product • Test result • Management and customer acceptance

Maintenance

The inputs for the maintenance stage include the complete product being monitored for needed changes that might be raised by routine maintenance, complaint handling and regression testing. The outputs are a reengineered product, maintenance and security event logs, and test reports.

Example: Maintenance

Inputs	Process	Outputs
• Complete product	• User training routine maintenance complaint handling • SW upgrades and SW “debug“ / patch • New SW version configuration management • Regression testing	• Reengineered product • Maintenance logs (including authorization) • Security event logs • Test reports



Strategies for success

Working with a trusted third party that has deep, and broad knowledge of the software engineering process is critical to success. UL Solutions has decades of experience with the standards involved in medical device development and can help you understand the requirements, for you to implement this in the processes where required. Every part of your organization can benefit from collaborative assistance at different stages of the life cycle.

Benefits to different roles in your organization

R&D

UL 2900 and IEC 81001-5-1 analysis and testing can mature the product's cybersecurity posture, even during early phases of R&D

Product management

UL 2900 and IEC 81001-5-1 can provide a standards-based checklist of issues that need to be addressed to establish an acceptable baseline of security

Regulatory affairs

UL 2900 and IEC 81001-5-1 are FDA Recognized Consensus Standards that are being used globally and can be factored into your global regulatory submissions

Quality

UL 2900 and IEC 81001-5-1 integrate security into your Quality Management System

Software development

UL 2900 and IEC 81001-5-1 when combined can provide specific security targets for addressing weaknesses and vulnerabilities

Product security

UL 2900 and IEC 81001-5-1 can help set product security expectations across the organization

Procurement

UL 2900 and IEC 81001-5-1 can help establish product attributes, security processes, and technical criteria when purchasing software components

Insurance

Certification could help reduce the expenses of product liability and cyber risk insurance, as well as supporting insurance coverage and reimbursements

Why UL Solutions?

We help you bring transparency to your product and system security, especially as it relates to medical device and network-connected device cybersecurity. With years of cybersecurity science behind us, we have the expertise to confirm compliance with industry regulations, standards and best practices.

Our experience has enabled us to bring these components together to create one reliable testing and certification program. Our services can help you harden device security to thwart unauthorized attempts to change functionality, access data or gain entry through external and internal connections or communication channels within a system / device and communicate your dedication to security to the marketplace. All these things can help increase the end user's confidence in your products and your system security.

UL.com/Solutions

Advisory services

- General advisory services
- Knowledge contracts
- Regulatory research
- Cybersecurity strategy planning
- Threat modeling support
- Knowledge support for addressing security through QMS, RM & SDLC processes
- Guidance on standards, framework, and requirements
- Tailored advisory engagements for Custom Cybersecurity Training
- Medical Device - Interoperability

Trainings

- Medical device security
- UL 2900
- AAMI TIR 57
- IEC 81001-5-1
- Securing Software as a Medical Device (SaMD)
- Securing Software in a Medical Device (SiMD)
- Overview of global cybersecurity regulatory approaches
- Custom Cybersecurity Training
- UL 2800 standard training

Certification

- UL 2900-1 and UL 2900-2-1
- IEC 81001-5-1 (coming soon)
- Data Acceptance Test Lab (DATL)
- Firm Registration (Organizational Process Certifications to ISO 13485, ISO 14971, and IEC 62304)

Security testing

- Known malware testing
- Malformed input testing
- Penetration testing
- Custom testing
- Vulnerability scanning (including Software Bill of Materials (SBOM) generation) static source code analysis and security control verification

Compliance and surveillance

- Vulnerability management support
- Security capability maturity assessment and continuous improvement planning

Gap analysis and evaluations

- UL 2900-1
- UL 2900-2-1
- IEC 81001-5-1
- Manufacturer Disclosure Statement for Medical Device Security (MDS2)
- Supply chain performance management

UL Solutions has the cybersecurity expertise and capabilities to help medical device manufacturers to gain a better understanding which helps to mitigate the risk that software weaknesses and vulnerabilities pose to their systems and devices. To learn more about how we can help you develop cyber secure medical devices, visit **www.UL.com/healthcare-cybersecurity.**

UL Solutions

UL.com/Solutions