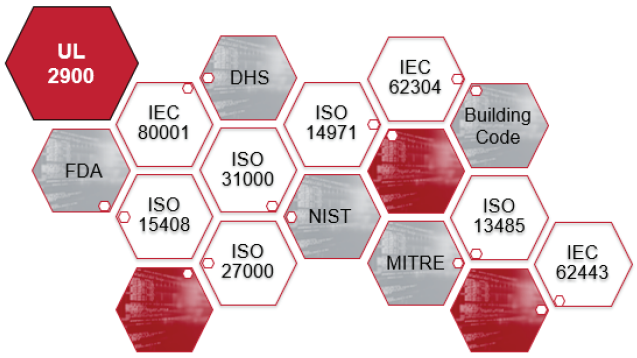
UL 2900:
A Cybersecuirty aid for industry and regulators

A baseline of cybersecurity hygiene

UL 2900 establishes that manufacturers have characterized and documented the technologies used in their products that could constitute an “attack surface”. It requires threat modeling based on intended use and relative exposure. The standard demonstrates the effective implementation of security controls protecting both sensitive data (e.g. PII, PHI) and also other assets such as command and control data. It provides objective evidence that software weaknesses, and vulnerabilities have been appropriately dispositioned and further verified via penetration testing and promotes defensive design (e.g. defense-in-depth, partitioning, etc).

UL 2900 generally helps ensure system robustness (e.g. fuzz testing / malformed input testing):

- Monitoring for security events
- Logging of security events
- Managing security logs
- Updating software to address safety, essential performance, and security issues
- Handling failures in the software update process (e.g. roll-back)
- Component purchasing controls
- Management of sensitive data
- Remote product management
- Decommissioning (e.g. purging of PII / PHI)



The relationship between UL 2900-1 and UL 2900-2-1; What is the delta?

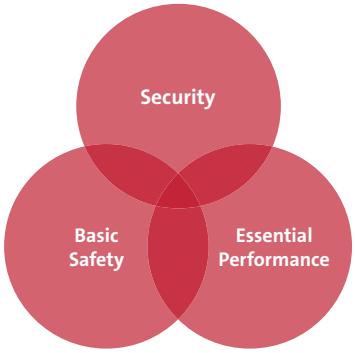
- Basic safety
- Essential performance
- Quality management system
- Software development life-cycle processes
- Risk management has a broader scope in UL 2900-2-1

Note: This includes hardware/software control structures and the impact of breach.

UL 2900 addresses software weaknesses and vulnerabilities that may impact Basic Safety, Security and Essential Performance

UL 2900-2-1 requires security controls for inputs, software execution threads and outputs of all product functions related to Basic Safety (e.g. door interlocks), Essential Performance (e.g. drug infusion), and Security (e.g. access control).

Note: This includes protection of metadata and other contextual data that couldbe an “asset” or part of an “attack vector” (e.g. exfiltration of waveform characteristics)



NIST CSF	UL 2900
Identify	Cybersecurity is required to be a core aspect of the organization’s Quality Management System.
Protect	A threat model is required, and relevant security controls are derived and tested for effectiveness.
Detect	Security-related events are to be logged and the logs are to be securely managed.
Respond	A “risks addressed” state transition is required in the event that security controls are compromised.
Recover	Products are required to be designed to be patchable, and a variety of update controls are required.

Email: Medical.Inquiry@ul.com | Website: UL.com/Healthcare

Empowering Trust™