

August 11, 2017

1

UL 2900-2-3

Outline of Investigation for Software Cybersecurity for Network-Connectable Products, Part 2-3: Particular Requirements for Security and Life Safety Signaling Systems

Issue Number: 1

August 11, 2017

Summary of Topics

With the increasing threat of cyber-attacks affecting security and life-safety-critical products and service infrastructure, the proposed UL 2900 series of Outline of Investigations aim to provide a foundational set of requirements that manufacturers of network connectable products used in security and life safety signaling systems can pursue to establish a baseline of protection against known vulnerabilities and a foundational set of cyber security risk controls to consider relative to their existing overall product risk assessments. The objective is to provide a Outline of Investigation for testing products that implements established security design principles into the testing regimen.

The proposed first edition of the Outline of Investigation for Software Cybersecurity for Network-Connectable Products, Part 2-3: Particular Requirements for Security and Life Safety Signaling Systems, UL 2900-2-3, describes requirements regarding the vendor's risk management process for products used in security and life safety signaling systems ; methods by which a product's software shall be evaluated and tested for the presence of vulnerabilities, software weaknesses malware; and requirements regarding the establishment and testing of security risk controls in the architecture and design of a product. The requirements leverage the requirements of the Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements, UL 2900-1, with additional requirements that take into consideration security and life safety signaling systems context, environment, reliability, and safety concerns.

UL's Outlines of Investigation are copyrighted by UL LLC. Neither a printed nor electronic copy of an Outline of Investigation should be altered in any way. All of UL's Outlines of Investigation and all copyrights, ownerships, and rights regarding those Outlines of Investigation shall remain the sole and exclusive property of UL LLC.

UL COPYRIGHTED MATERIAL –
COPYRIGHT © 2017 UL LLC
NOT AUTHORIZED FOR FURTHER REPRODUCTION OR
DISTRIBUTION WITHOUT PERMISSION FROM UL



Documents

Document Sharing Hub

No Text on This Page

**UL COPYRIGHTED MATERIAL –
NOT AUTHORIZED FOR FURTHER REPRODUCTION OR
DISTRIBUTION WITHOUT PERMISSION FROM UL**



Documents

Document Sharing Hub

CONTENTS

INTRODUCTION

1 Scope	5
2 Normative References	6
3 Glossary	6
4 General	6

DOCUMENTATION OF PRODUCT, PRODUCT DESIGN AND PRODUCT USE

5 Product Documentation	7
6 Product Design Documentation	7
7 Documentation for Product Use	7

RISK CONTROLS

8 General	8
9 Access Control, User Authentication and User Authorization	9
10 Remote Communication	10
11 Sensitive Data	10
12 Product Management	10

RISK MANAGEMENT

13 Vendor Product Risk Management Process	11
---	----

VULNERABILITIES AND EXPLOITS

14 Known Vulnerability Testing	12
15 Malware Testing	12
16 Malformed Input Protocol Testing (also reference Appendix D)	12
17 Structured Penetration Testing	13

SOFTWARE WEAKNESS ANALYSIS

18 Software Weakness Analysis	14
19 Static Code Analysis	14
20 Static Binary and Bytecode Analysis	14
21 Organizational Assessment	15

APPENDIX A

A1 Sources for Software Weaknesses	A1
--	----

APPENDIX B

B1 Requirements for Secure Mechanisms for Storing Sensitive Data and Personally Identifiable Information	B1
--	----

APPENDIX C

C1 Requirements for Security Functions	C1
--	----

APPENDIX D

D1 Level 1 Malformed Input Protocol List	D1
--	----

**UL COPYRIGHTED MATERIAL –
NOT AUTHORIZED FOR FURTHER REPRODUCTION OR
DISTRIBUTION WITHOUT PERMISSION FROM UL**

**Documents**

Document Sharing Hub

INTRODUCTION

Note: This Outline of Investigation for Software Cybersecurity for Network-Connectable Products, Part 2-3: Particular Requirements for Security and Life Safety Signaling Systems refers to the Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements, UL 2900-1.

1 Scope

1.1 This security evaluation Outline of Investigation applies to the evaluation of security and life safety signaling system components. It applies to, but is not limited to, the following products:

- a) Alarm Control Units
- b) Intrusion Detection Equipment
- c) General Purpose Signaling Units
- d) Digital Video Equipment and Systems
- e) Mass Notification and Emergency Communication / Evacuation Equipment and Systems
- f) Control servers;
- g) Alarm Automation System Software
- h) Alarm Receiving Equipment
- i) Anti- theft Equipment
- j) Automated Teller Machines
- k) Fire Alarm Control Systems
- l) Network Connected Locking Devices
- m) PSIM Systems
- n) Smoke Control Systems
- o) Smoke / Gas / CO Detection Devices
- p) Audible and Visual Signaling Devices (fire and general signaling)
- q) Access Control Equipment and Systems

1.2 This Outline of Investigation does not contain general requirements that are intended to address functional testing of the product unless expressly specified.

UL COPYRIGHTED MATERIAL –
NOT AUTHORIZED FOR FURTHER REPRODUCTION OR
DISTRIBUTION WITHOUT PERMISSION FROM UL



Documents
Document Sharing Hub

1.3 This Outline of Investigation also describes requirements for the product risk management process carried out by the vendor of the product, including a list of security controls that the product (or the vendor, as applicable) shall comply with unless a risk assessment done by the vendor shows that the risk of not implementing one of these security controls is acceptable.

2 Normative References

2.1 All references are for the current published version of the document unless stated otherwise.

Normative References are included in Section 2 of the Standard for Cybersecurity for Network-Connectable Products, Part1: General Requirements, UL 2900-1.

3 Glossary

Glossary Terms are included in Section 3 of the Standard for Cybersecurity for Network- Connectable Products, Part1: General Requirements, UL 2900-1.

4 General

4.1 This Outline of Investigation comprises of levels of security requirements that are applicable to the product with an increasing level of security for higher levels. The levels and their description are defined in Table 4.1.

Table 4.1

Level	Description
L1	Includes foundational cybersecurity testing requirements for security risk assessment of software in products covered in this Outline of Investigation. Provides assessment of general security capabilities of a product with limited knowledge of the internal security controls of the product. L1 is recommended as a minimum level of assessment.
L2	Includes L1 assessment and testing requirements and additional supplemental requirements for security risks assessment of software in products. Provides assessment of security capabilities of a product with knowledge of internal security controls of the product.
L3	Includes L1 and L2 assessment and testing requirements and additional supplemental requirements of the vendor process and management. Provides assessment of security capabilities of a product with knowledge of internal security controls of the product and knowledge of the business practices of the vendor to support the lifecycle of the product.

4.2 The product shall comply with the clauses identified in the tables of each section of this Outline of Investigation per the Level intended. The level intended will be marked with an X per the applicable clause. Where an X is not applied, the clause is not mandatory for the Level.

DOCUMENTATION OF PRODUCT, PRODUCT DESIGN AND PRODUCT USE

5 Product Documentation

Table 5.1

	Clause	L1	L2	L3
5.1	The product shall comply with: Product Documentation, Section 4.1(e), of the Standard for Software Cybersecurity for Network-Connectable Devices, Part 1: General Requirements, UL 2900-1.	X		
5.2	The product shall comply with: Product Documentation, Section 4.1 of the Standard for Software Cybersecurity for Network-Connectable Devices, Part 1: General Requirements, UL 2900-1.		X	

6 Product Design Documentation

Table 6.1

	Clause	L1	L2	L3
6.1	The product shall comply with: Product Design Documentation, Section 5.1 of the Standard for Software Cybersecurity for Network-Connectable Devices, Part 1: General Requirements, UL 2900-1.		X	

7 Documentation for Product Use

Table 7.1

	Clause	L1	L2	L3
7.1	The product shall comply with: Documentation for Product Use, Section 6.1 of the Standard for Software Cybersecurity for Network-Connectable Devices, Part 1: General Requirements, UL 2900-1.	X		
7.2	The product shall comply with: Documentation for Product Use, Section 6.2 of the Standard for Software Cybersecurity for Network-Connectable Devices, Part 1: General Requirements, UL 2900-1.	X		
7.3	The product shall comply with: Documentation for Product Use, Section 6.3 of the Standard for Software Cybersecurity for Network-Connectable Devices, Part 1: General Requirements, UL 2900-1.	X		
7.4	The product shall comply with: Documentation for Product Use, Section 6.4 of the Standard for Software Cybersecurity for Network-Connectable Devices, Part 1: General Requirements, UL 2900-1.		X	
7.5	The product shall comply with: Documentation for Product Use, Section 6.5 of the Standard for Software Cybersecurity for Network-Connectable Devices, Part 1: General Requirements, UL 2900-1.		X	
7.6	The product shall comply with: Documentation for Product Use, Section 6.6 of the Standard for Software Cybersecurity for Network-Connectable Devices, Part 1: General Requirements, UL 2900-1.		X	

UL COPYRIGHTED MATERIAL –
NOT AUTHORIZED FOR FURTHER REPRODUCTION OR
DISTRIBUTION WITHOUT PERMISSION FROM UL

Table 7.1 Continued on Next Page



Documents
Document Sharing Hub

Table 7.1 Continued

7.7	The product shall comply with: Documentation for Product Use, Section 6.7 of the Standard for Software Cybersecurity for Network-Connectable Devices, Part 1: General Requirements, UL 2900-1.		X	
7.8	The product shall comply with: Documentation for Product Use, Section 6.8 of the Standard for Software Cybersecurity for Network-Connectable Devices, Part 1: General Requirements, UL 2900-1.		X	
7.9	The product shall comply with: Documentation for Product Use, Section 6.9 of the Standard for Software Cybersecurity for Network-Connectable Devices, Part 1: General Requirements, UL 2900-1.		X	
7.10	The product shall comply with: Documentation for Product Use, Section 6.10 of the Standard for Software Cybersecurity for Network-Connectable Devices, Part 1: General Requirements, UL 2900-1.		X	

RISK CONTROLS

8 General

Table 8.1

	Clause	L1	L2	L3
8.1	The product shall comply with: Risk Controls - General, Section 7.1.1 of the Standard for Software Cybersecurity for Network-Connectable Devices, Part 1: General Requirements, UL 2900-1.	X		
8.2	The product shall comply with: Risk Controls - General, Section 7.1.2 of the Standard for Software Cybersecurity for Network-Connectable Devices, Part 1: General Requirements, UL 2900-1.	X		
8.3	The product shall comply with: Risk Controls - General, Section 7.1.3 of the Standard for Software Cybersecurity for Network-Connectable Devices, Part 1: General Requirements, UL 2900-1.	X		

UL COPYRIGHTED MATERIAL –
NOT AUTHORIZED FOR FURTHER REPRODUCTION OR
DISTRIBUTION WITHOUT PERMISSION FROM UL



Documents
Document Sharing Hub