

10. March 2026

Leveraging Open Source for IEC 62443-Compliant Embedded Systems

Dr. Florian Kauer, florian.kauer@linutronix.de

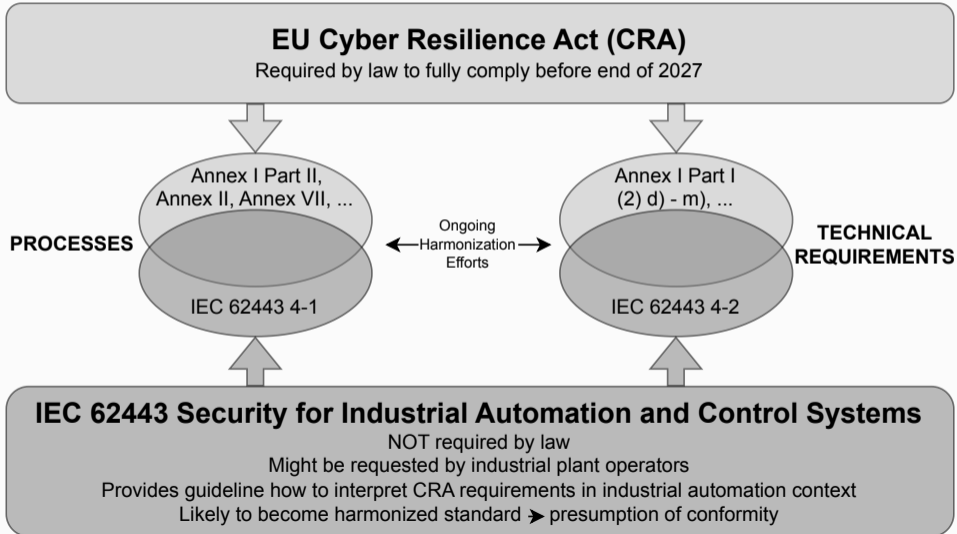
General	IEC 62443-1-1 Terminology, concepts and models	IEC 62443-1-2 Master glossary of terms and abbreviations	IEC 62443-1-3 System security conformance metrics	IEC 62443-1-4 IACS security lifecycle and use-cases
Policies & Procedures	IEC 62443-2-1 Security program requirements for IACS asset owners	IEC 62443-2-2 IACS security protection scheme	IEC 62443-2-3 Patch management in the IACS environment	IEC 62443-2-4 Security program requirements for IACS service providers
System	IEC 62443-3-1 Security technologies for industrial automation and control systems	IEC 62443-3-2 Security risk assessment for system design	IEC 62443-3-3 System security requirements and security levels	
Component	IEC 62443-4-1 Product security development life cycle requirements	IEC 62443-4-2 Technical security requirements for IACS components		

IEC 62443-4-1 - Secure product development lifecycle requirements



IEC 62443-4-2 - Technical security requirements for IACS components





Open Source in Industrial Automation

Collaborate on the Core, Compete on the Edges

Open Source in Industrial Automation

Collaborate on the Core, Compete on the Edges

But is that feasible if compliance and certification is required?

Open Source in Industrial Automation

Collaborate on the Core, Compete on the Edges

But is that feasible if compliance and certification is required?

Idea: Certify a demonstrator built from open-source components

Case Study: IEC 62443-4-2 Certification of IGLoS Secure Beacon

- ▶ Embedded device with simple application:
Remote control of blinking LED
- ▶ Locked-down and hardened Linux system
- ▶ Fulfills all 57 applicable security requirements from 4-2
- ▶ Certified by TÜV SÜD according to IEC 62443-4-2 in Q1 2025
- ▶ Serves as blueprint to implement more complex applications



How is Open Source Relevant for a Product Certification?



**Traceable
Documentation**



**Technical
Requirements**



**External
Components
Management**

How is Open Source Relevant for a Product Certification?



**Traceable
Documentation**



**Technical
Requirements**



**External
Components
Management**

Traceable Documentation is the Primary Evidence for Certification

IEC 62443-4-1 SM-1

A [...] process shall be documented and enforced [...] that include [...] b) product description and requirements definition with requirements traceability [...]

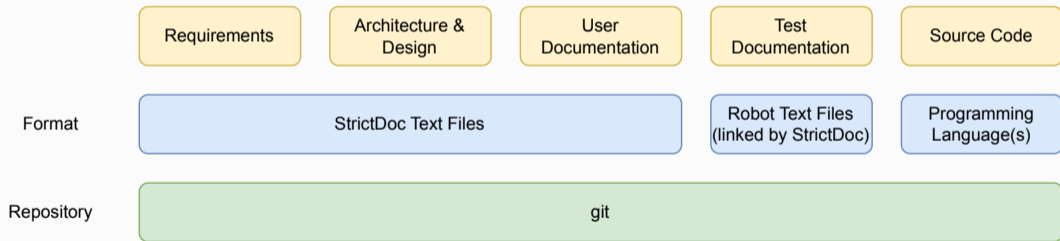
IEC 62443-4-1 SI-1

A process shall be employed [...] including [...] d) review of the implementation and its traceability to the security capabilities defined to support the security design [...]

Exemplary Toolset for Product Development Documentation

	Requirements	Architecture & Design	User Documentation	Test Documentation	Source Code
Format	IBM DOORS	Confluence Markup	Adobe FrameMaker	Xray	Programming Language(s)
Repository	DOORS Server	Confluence	Network Share	Jira	git

Product Development Documentation with StrictDoc



StrictDoc Format

[REQUIREMENT]

MID: af79e33fb4324cccbd02fb83cdb553a1

UID: REQ-SB-DEVICE-PASSWORD-INPUT-DIALOG

TITLE: Device Password Input Dialog

TYPE: Security

STATUS: Reviewed

IMPLEMENTATION: Reviewed

STATEMENT: >>>

The [LINK: REQ-SB-INITIAL-DEVICE-PASSWORD] input dialog shall mask the password during entry by displaying only asterisks.

On authentication failure, the UI shall present an error message that indicates login failure without further details.

<<<

RELATIONS:

- TYPE: Parent

VALUE: REQ-SB-COMMISSIONING-UI

- TYPE: Parent

VALUE: REQ-SB-INITIAL-DEVICE-PASSWORD

The screenshot displays the StrictDoc web interface for a requirement document. The breadcrumb path is: IGL Specification / Requirements - IGLOS Secure Beacon (Reference Implementation) / Document. The left sidebar contains a navigation menu with categories like Overview, Requirements - IGLOS (IGL Operating System), Requirements - IGLOS Secure Beacon (Reference Implementation), Design, Threat Models, Testing, Supplier Guide, User Guide, Development Infrastructure, GitLab Merge Request Reviews, Annex, and Compliance Matrix. The main content area shows a requirement titled "1.4.3.3. Device Password Input Dialog" with a yellow highlight. The requirement details include: MID: af79e33fb4324ccbd02fb83cdb553a1, UID: REQ-SB-DEVICE-PASSWORD-INPUT-DIALOG, PARENT RELATIONS: REQ-SB-COMMISSIONING-UI Commissioning User Interface, REQ-SB-INITIAL-DEVICE-PASSWORD Initial Device Password, COMP CR 1.10 IEC62443 4-2 CR 1.10 compliance, CHILD RELATIONS: DESIGN-COMMISSIONING Commissioning (Implements), FILE RELATIONS: src/systest/Tests/SystemTests/00-Commissioning.robot, lines: 19-23, function Password Field Security() (TestCase); src/systest/Tests/SystemTests/00-Commissioning.robot, lines: 33-39, function Invalid Password Error() (TestCase). The STATEMENT is: "The Initial Device Password input dialog shall mask the password during entry by displaying only asterisks." The TYPE is Security, and the STATUS is Reviewed. The IMPLEMENTATION is also Reviewed. A right-hand sidebar shows a hierarchical table of contents for the document, with "1.4.3.3 Device Password Input Dialog" highlighted in yellow. The bottom right corner of the interface indicates it is built with StrictDoc 0.9.4.

IGL Specification / Requirements - IGLOS Secure Beacon (Reference Implementation) / Document

Overview
00_overview.sdoc

Requirements - IGLOS (IGL Operating System)
01-1_requirements_igl.sdoc

Requirements - IGLOS Secure Beacon (Reference Implementation)
01-2_requirements_refapp.sdoc

Design
03_design.sdoc

Threat Models
04_threat_models.sdoc

Testing
05_test.sdoc

Supplier Guide
11_supplier_guide.sdoc

User Guide
12_user_guide.sdoc

Development Infrastructure
21_infrastructure.sdoc

GitLab Merge Request Reviews
80_gitlab_merge_request_reviews.sdoc

Annex
90_annex.sdoc

Compliance Matrix

1.4.3.3. Device Password Input Dialog

MID: af79e33fb4324ccbd02fb83cdb553a1
UID: REQ-SB-DEVICE-PASSWORD-INPUT-DIALOG
PARENT RELATIONS: -- REQ-SB-COMMISSIONING-UI Commissioning User Interface
-- REQ-SB-INITIAL-DEVICE-PASSWORD Initial Device Password
-- COMP CR 1.10 IEC62443 4-2 CR 1.10 compliance
CHILD RELATIONS: -- DESIGN-COMMISSIONING Commissioning (Implements)
FILE RELATIONS: </> src/systest/Tests/SystemTests/00-Commissioning.robot, lines: 19-23, function Password Field Security() (TestCase)
</> src/systest/Tests/SystemTests/00-Commissioning.robot, lines: 33-39, function Invalid Password Error() (TestCase)

STATEMENT:
The [Initial Device Password](#) input dialog shall mask the password during entry by displaying only asterisks.

On authentication failure, the UI shall present an error message that indicates login failure without further details.

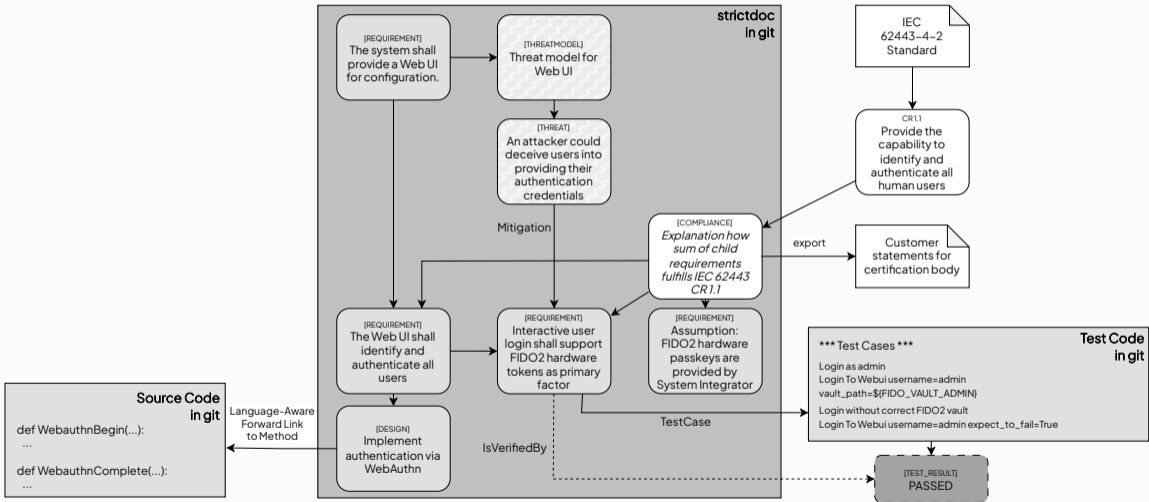
TYPE:
Security

STATUS:
Reviewed

IMPLEMENTATION:
Reviewed

1.4.2.3 Serialnumber
1.4.2.4 Initial Device Password
1.4.2.5 Initial Device Password Access Control
1.4.2.6 Transition to Commissioning
1.4.3 Commissioning
1.4.3.1 Commissioning
1.4.3.2 Commissioning User Interface
1.4.3.3 Device Password Input Dialog
1.4.3.4 Configure Host Name and FQDN
1.4.4 Operation
1.4.4.1 Operation
1.4.4.2 Provide Configuration
1.4.4.3 Configuration Hash and Change Time
1.4.4.4 Safe State
1.4.4.5 Factory Reset
1.4.4.6 User Interfaces
1.4.4.6.1 Web UI
1.4.4.6.1.1 Web UI
1.4.4.6.1.2 Show Effective System Configuration
1.4.4.6.1.3 Web UI User Authentication
1.4.4.6.1.4 Web UI Denial of Service Protection

Built with StrictDoc 0.9.4



How is Open Source Relevant for a Product Certification?



**Traceable
Documentation**



**Technical
Requirements**

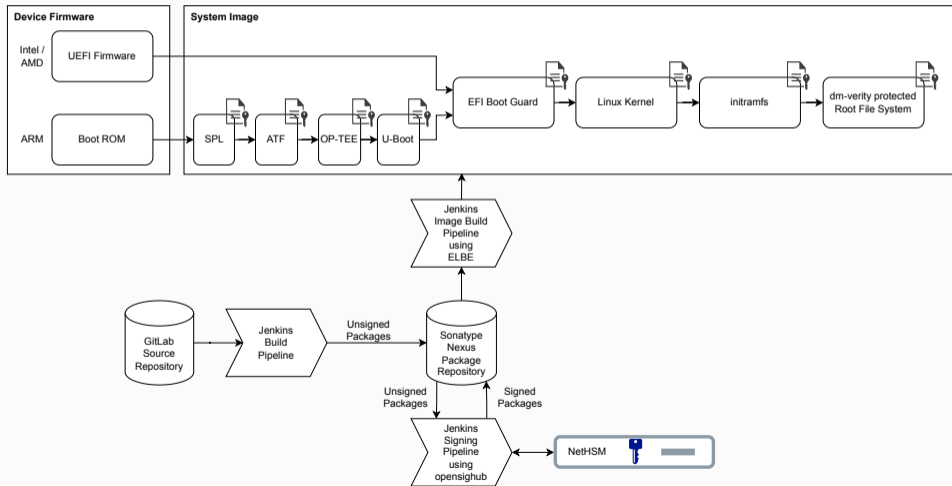


**External
Components
Management**

IEC 62443-4-2 EDR 3.14 - Integrity of the boot process

Embedded devices shall verify the integrity of the firmware, software, and configuration data needed for the component's boot and runtime processes prior to use.

IGLOS Secure Boot Chain and Signing Infrastructure



How is Open Source Relevant for a Product Certification?



**Traceable
Documentation**



**Technical
Requirements**

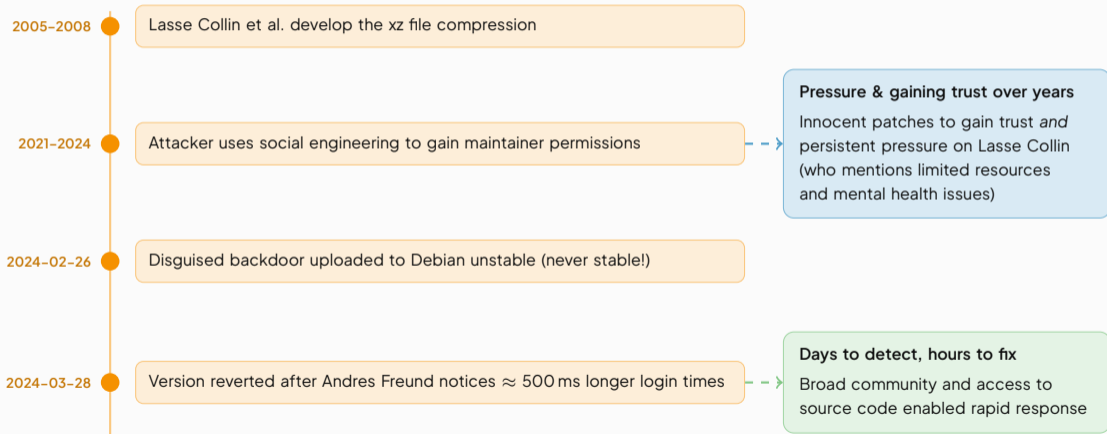


**External
Components
Management**

IEC 62443-4-1 SM-9: Security requirements for externally provided component

A process shall be employed to identify and manage the security risks of all externally provided components used within the product. [...]

XZ Utils Backdoor



Source: <https://research.swtch.com/xz-timeline>

Better Use Proprietary Software?

SolarWinds Orion
Proprietary software for IT performance monitoring
Around February 2020: Attackers inject backdoor in official builds
Many large and governmental organizations highly vulnerable
About 10 months to find & publicly disclose

Realtek Jungle SDK
SDK for building network devices
CVE-2021-35392 - CVE-2021-35395, including remote code execution
Millions of attacks by botnets
Still many vulnerable devices expected today

Better Develop Everything Yourself?



WhatsApp

Remote code execution via custom MP4 parsing
CVE-2019-11931



DVD Content Scramble System

Custom algorithm and implementation → hacked



PlayStation 3





Custom ECDSA implementation → hacked



Keyless Car Entry

Multiple cases of weak custom crypto

How to Select Software Components?

	Security vulnerabilities	Independently auditable & patchable	Supplier can be held liable
Proprietary Software		✗	✓
Own Implementation		✓	✗
Unsupported Open Source		✓	✗
Open Source + Support		✓	✓

OpenSSF Concise Guide for Evaluating Open Source Software



Source: <https://best.openssf.org/Concise-Guide-for-Evaluating-Open-Source-Software>

Even a small systems can contain hundreds of open-source components...



Even a small systems can contain hundreds of open-source components...

We need communities and tools!



Security Metrics

OpenSSF Best Practices Badge

systemd

Projects that follow the best practices below can voluntarily self-certify and show that they've achieved an Open Source Security Foundation (OpenSSF) best practices badge. [View details](#)

If this is your project, please show your badge status on your project page! The badge status looks like this: . [Click to learn how to embed it.](#) [View details](#)

These are the best criteria. You can also view the or best criteria.

Baseline badges: [Baseline Level 1](#) [Baseline Level 2](#) [Baseline Level 3](#)

[View project](#) [View all details](#) [View all vulnerable issues](#)

Basics 2/3/20

General

What is the human-readable name of the project? [View details](#)

What is a brief description of the project?
systemd System and Service Manager

What is the URL for the project (ie a website)?
<https://www.freedesktop.org/software/systemd/>

What is the URL for the version control repository (it may be the same as the project URL)?
<https://github.com/systemd/systemd>

What license(s) is the project released under? [View details](#)

What programming language(s) are used to implement the project? [View details](#)

What is the [Common Platform Enumeration \(CPE\)](#) name for the project if it has one? [View details](#)

Other general comments about the project:

Basic project website content

MIT **Shared** [View details](#)

The project website MUST accurately describe what the software does (what problem does it solve?) [View details](#)

Debian Security Tracker

Vulnerable source packages in the stable suite

high medium low unimportant not yet assigned end-of-life hide remote scripts hide local scripts hide unstable scripts include issues to be checked (shown in purple) include issues logged into this include issues logged -upstreams include issues logged -upstreamers

Package	Bug	Urgency	Remote
adwintch	CVE-2026-2653	not yet assigned	no
amd64-microcode (non-free-firmware)	CVE-2024-36350	not yet assigned	no
	CVE-2024-36357	not yet assigned	no
	CVE-2025-9039	not yet assigned	no
	CVE-2025-29934	not yet assigned	no
	CVE-2025-29943	not yet assigned	no
	CVE-2025-48514	not yet assigned	no
	CVE-2025-48517	not yet assigned	no
	CVE-2025-52534	not yet assigned	no
	CVE-2025-52536	not yet assigned	no
	CVE-2025-54514	not yet assigned	no
calibre	CVE-2026-26064	not yet assigned	no
	CVE-2026-26065	not yet assigned	no
ceph	CVE-2024-31884	not yet assigned	?
	CVE-2024-47866	not yet assigned	no
chromium	CVE-2026-26448	not yet assigned	no
	CVE-2026-26449	not yet assigned	no
	CVE-2026-30550	not yet assigned	no
cpp-httplib	CVE-2025-46758	not yet assigned	no
	CVE-2025-53628	not yet assigned	no
	CVE-2025-53629	not yet assigned	no
	CVE-2025-66576	not yet assigned	no
	CVE-2025-66577	not yet assigned	no
	CVE-2026-21428	not yet assigned	no

License Compliance



Linux Foundation project
for license scanning & compliance



OSADL project for curated
license compliance data

Community Health

CHA OSS

Community Health Analytics in Open Source Software

Linux Foundation project for metrics, models & software

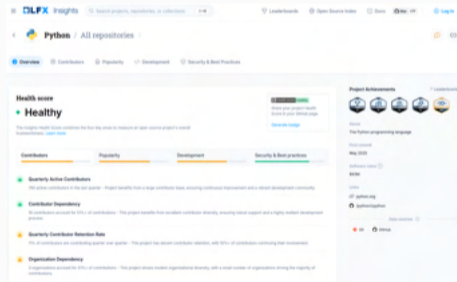
GrimoireLab



Augur



OLFX | Insights



ACTIVITY

VERSIONS **CURRENT** **3.8.9-3-amd64** from 2025-07-25 **Track** **x-Current** **Track** **security** **3.8.9-3-amd64**

UPSTREAM <https://gitlab.com/gnutls/gnutls>

DEBIAN <https://wiki.debian.org/gnutls-team/gnutls>

COMMIT LAST YEAR **272**

CONTRIBUTORS LAST YEAR **28**

POSITION IN ECOSYSTEM

SMALL CONTRIBUTORS LAST 12 MONTHS

REFUTATIONS LAST 12 MONTHS

KNOWN CVEs

MEDIUM **CVE-2025-14833** **0** **gnutls: GnuTLS Denial of Service via excessive resource consumption during certificate verification** **FIXED 3.8.9-3-amd64** **PUBLISHED 2024-02-09** **UPDATED 2025-03-02**

LOW **CVE-2011-3389** **0** **HTTPS block-wise chosen-plaintext attack against SSL/TLS (BEAST)** **PUBLISHED 2011-09-04** **UPDATED 2025-04-11**

DEBIAN CHANGES

gnutls28 (3.8.9-3-amd64) trivial: upgrade/medium

- * Add patch for CVE-2025-14833 / CVE-2025-0751-0752 from 3.8.11, CVEid: #1321348
- ** Andrew Metcaler <metcaler@debian.org> Sun, 27 Nov 2025 14:13:39 +0000

gnutls28 (3.8.9-3) unstable: upgrade/medium

- * Obsolete/fix from 3.8.10 release
- * libgnutls: Fix WSL printer dereference when the Debian WSL patch is required by Stefan Rindler
- (CVE-2025-0751-0752, CVE: medium) (CVE-2025-0391)
- * libgnutls: fix heap read buffer overflow on parsing X.509 SIZEL

BINARY PACKAGES

PACKAGE	VERSION	ARCH	COMPLETE-TIME TESTS	RUN-TIME TESTS
libgnutls30t64	3.8.9-3-amd64	ALL	✓	✓
libgnutls30t64	3.8.9-3-amd64	ARM64	✓	✓
libgnutls30t64	3.8.9-3-amd64	ARMHF	✓	✓

OPENSSF BEST PRACTICES

NAME **LICENSE** **ISSUED SINCE** **PROJECT HOME PAGE** **DESCRIPTION** **score: 100%** **PASSING**

gnutls **GPL-2.0** **2017-02-24** **<https://www.gnutls.org>** **GnuTLS is a secure communications library implementing the SSL, TLS and DTLS protocols and technologies around them. It provides a simple C language APIs to access the secure communications protocols.** **[bestpractices.dev](#)**

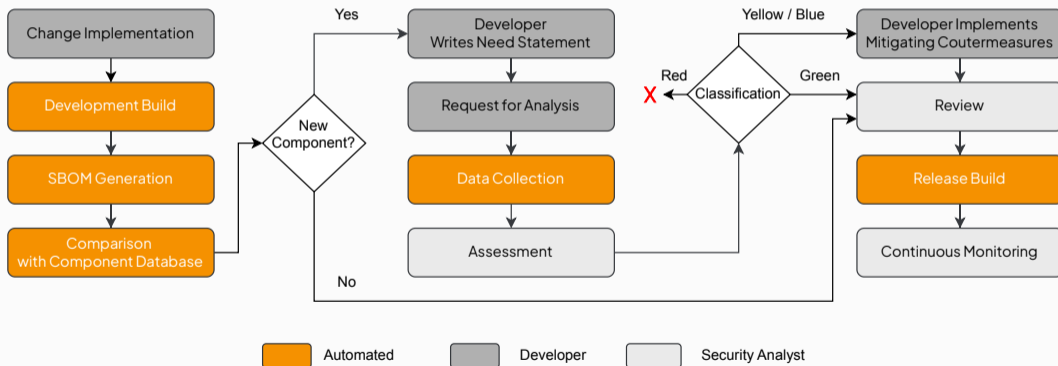
	✓ PASSING 100% 2025-07-24			✓ SILVER 100% 2025-07-24			✓ GOLD 100% 2025-07-24		
	MUST	SHOULD	SUGGESTED	MUST	SHOULD	SUGGESTED	MUST	SHOULD	SUGGESTED
Basic project website content	✓	✓	✓	✓					
FLOSS license	✓	✓	✓	✓					

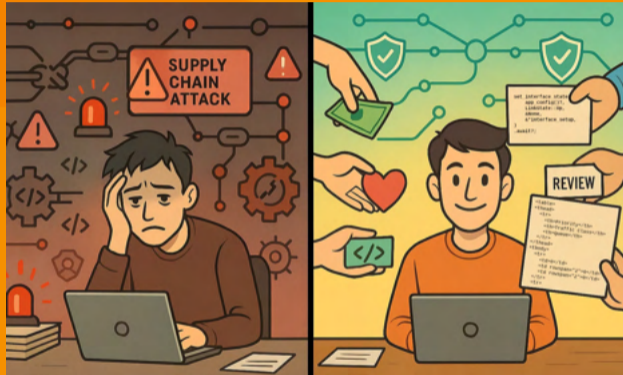
Example for an External Component Classification

Level	Category	Example in IGLOS Context
Green	Suitable for intended use*	apache2, openssl
Yellow	Suitable for use with risk-mitigating measures*	libexpat
Blue	Suitable for limited or isolated use*	python-dbus-next
Red	Not suitable for use	OpenClaw

* with continuous monitoring

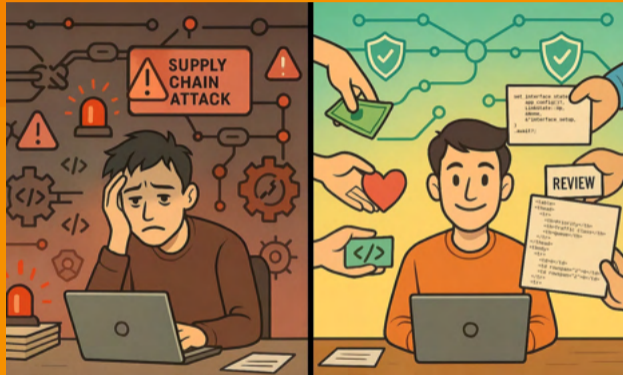
External Component Management Process





**Contributing to open source and supporting maintainers
is not only fair, but protects your supply chain!**

Visit
OSADL
Hall 4
Booth 4-168



Visit
Linutronix
Hall 4
Booth 4-250

Contributing to open source and supporting maintainers
is not only fair, but protects your supply chain!