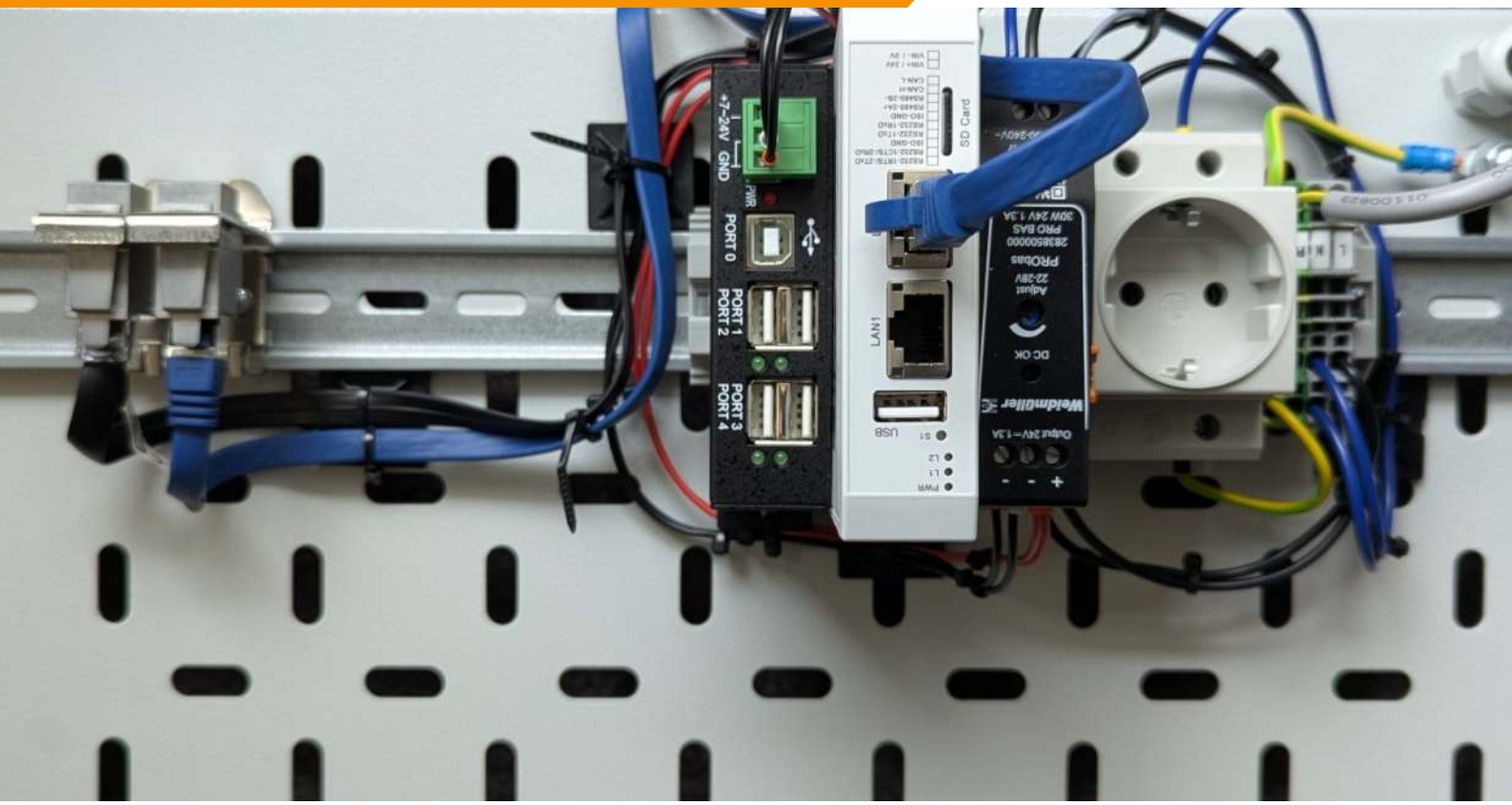

Security Maintenance and Regression Test Services

Complex embedded systems are now the norm. Kernels, drivers, libraries, system services, and applications must work together on real hardware. The Cyber Resilience Act (CRA) demands manufacturers manage vulnerabilities throughout the entire product lifecycle and continuously assess security risks. A Software Bill of Materials (SBOM) helps to identify Common Vulnerabilities and Exposures (CVEs), but identification alone is not sufficient. CVEs must be assessed to determine whether they affect a system and, if so, must be patched. However, CVE fixes can impact performance, stability, and system behavior, and may introduce regressions if not properly validated. Testing, performance benchmarking, and early detection of negative trends caused by security updates or configuration changes on the patched system are important to ensure smooth system operation.

CVEs and Testing

The number of reported CVEs has increased steadily and at an increasing rate over the period from 2016 to 2025 and is expected to grow further.

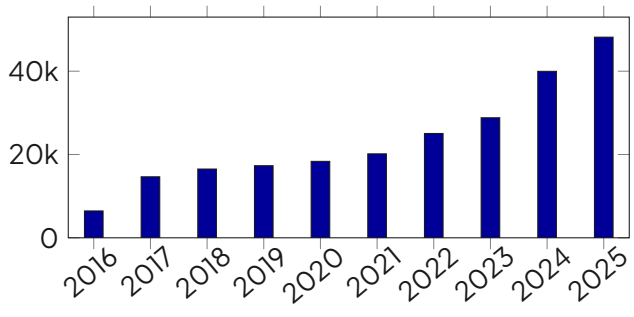

Figure 1: CVEs per Year
National Vulnerability Database (NVD)
https://nvd.nist.gov/vuln/search#/nvd/home?resultType=statistics

This high number of CVEs shows that organizations must be proactive about security. The first step is to identify the software components and compile an SBOM. Having an up-to-date SBOM provides transparency about the components used in a system, which is crucial for effective vulnerability management and essential for CRA compliance. Based on the SBOM, a CVE scan needs to be performed. These steps can often be automated, but the real work begins after the CVE scan, as CVEs need to be assessed for risk and patched if necessary. Finally, thorough testing is required to ensure that the applied patches do not cause regressions or other issues. We support you with the heavy lifting from SBOM generation to CVE scanning, to risk assessment and patching. By integrating your hardware into our test racks, we enable reproducible testing of your system with every patch.

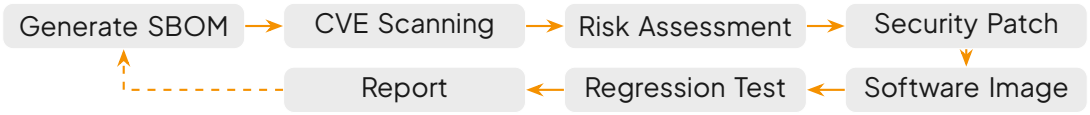

Figure 2: Linutronix Vulnerability Handling Process

Figure 2 depicts the Linutronix vulnerability handling process that is fully aligned with Annex I - Part II "Vulnerability handling requirements" of the CRA.

SBOM and CVE Scanning — Annex I Part II (1)

Linux build environments such as ELBE are able to generate an SBOM for every build. With the SBOM as input and with the help of vulnerability databases and open-source tools, we perform regular CVE scans and generate reports.

Risk Assessment & Patching — Annex I Part II (2)

When a vulnerability is first identified, it is not enough to just apply a patch immediately. A patch often needs to be developed first or, if not feasible, other mitigations need to be defined. This can only be decided based on the risk of the vulnerability for the specific system.

This requires both an elaborate threat model as well as deep technical expertise of the system and its security context. Linutronix is renowned for supporting the mitigation of software vulnerabilities, including Meltdown and Spectre in the Linux kernel.

Testing & Security Reviews — Annex I Part II (3)

After an image was generated with the necessary patches applied, it will be deployed on the target hardware for testing to ensure that applied patches do not introduce functional or non-functional issues. For this, your hardware can be seamlessly integrated into our automated test rack infrastructure, requiring no additional space or specialized skills on your side.

Whenever changes are introduced we ensure that all tests are re-executed and comprehensive, audit-ready reports are generated in StrictDoc, PDF or other required formats. To reduce the probability of vulnerabilities in the first place we also perform security reviews and for dependable tests we support you with the definition, implementation, and maintenance of tests needed for compliance, such as…

- **Regression Tests**: Detect regressions before they reach users
- **Performance Tests**: CPU, RAM, real-time latencies, network throughput, …
- **Functional Tests**: Validate core workflows and device-specific functionality
- **Application Tests**: Verify higher-level application and user-interface behavior
- **Penetration Tests**: Identify potential attack vectors before they escalate to a CVE

Communication — Annex I Part II (4) – (6)

It is crucial for your reputation and to avoid any legal consequences to communicate with your customers and authorities about vulnerabilities and mitigations in a timely and transparent manner. We provide you all the necessary information and reports to do so effectively and advise you how to handle reports of potential vulnerabilities, for example, to guide you through a coordinated vulnerability disclosure (CVD) process.

Software Updates — Annex I Part II (7) – (8)

Finally, the patched software needs to be installed on the target systems. For this, a robust software update mechanism needs to be in place from the beginning of the product lifecycle. Our IGLOS Linux distribution provides a secure and robust software update mechanism and can be adapted to various device management solutions.

Conclusion

With Linutronix you gain risk awareness, compliance, audit readiness, supply-chain security, and operational resilience. Vulnerabilities are detected early and appropriate mitigations are applied. By deploying and testing every change on your hardware, safe and stable operation is ensured. Our continuous process provides clear and defensible compliance evidence to get your security risks under control.

Linutronix GmbH
Bahnhofstraße 3 | D-88690 Uhldingen-Mühlhofen
Phone: +49 7556 25 999 0 | sales@linutronix.de
www.linutronix.de | Visit us

Are you interested?
Would you like to learn more about our products and solutions?
Simply contact us via phone or email.