stonetusker

Stonetusker Insights · Five-minute checklist

Hardware-Bound and Safety-Critical: 5-Minute Delivery Risk Checklist and Dates to Watch

Eight yes or no questions for teams that ship firmware and connected devices. Each one links to the page that explains it, and the dates below show which gaps carry a deadline.

For: Leaders of teams that ship firmware or connected devices in embedded, defence, automotive, energy or telecommunications products.

Skip if: Your company ships only cloud software with no device or firmware component.

By Subeesh Sivanandan, Founder, Stonetusker Systems · Updated 29 October 2026 · About 3 minutes to read · PDF version

Technical and engineering guidance. Please confirm legal obligations with your own counsel.

The short version

- Eight yes or no questions about delivery risk for hardware-bound and safety-critical products.
- Ask your team to answer them in five minutes, from what they know today, with no checks run first.

- A "no" marks a gap worth a closer look. The dates below show which gaps carry a deadline.

Eight questions for your team

1. Could someone list every component in the firmware you shipped last quarter from stored records, without a rebuild? Why it matters
2. Do you know which Yocto Project release each shipping product is built on, and does that release still receive security fixes from the project? Why it matters
3. Is one named person responsible for sending an early warning when a vulnerability in your product is actively exploited, with access to the European Union reporting platform already in place? Why it matters
4. Can the team say, from a measured release, how long a fixed build takes to reach devices in the field? Why it matters
5. Does the component record of each release include a hash and a licence for most components, and a signature? Why it matters
6. For each product version you will sell in the European Union after 8 December 2026, can you show which security updates it received and when? Why it matters
7. Has the team stated a support period for each product you will sell after December 2027, and how updates will reach devices for that period? Why it matters
8. Can a certificate pinned in a device or built into a firmware image be replaced without a new product release? Why it matters

Reading your answers

- **7 or 8 yes:** in good shape. Ask the questions again each quarter.
- **4 to 6 yes:** pick the first "no" that has a date attached, and give it an owner.
- **3 or fewer yes:** start with the dated items below, in date order.

Dates for your team

Date	What changes	Details
April 2026 (passed)	Yocto Project 4.0 Kirkstone is out of support. Scarthgap is supported until April 2028 and Wrynose until April 2030.[1]	Radar: Yocto Kirkstone
In force since 11 September 2026	Cyber Resilience Act reporting: actively exploited vulnerabilities and severe incidents go through the Single Reporting Platform, with an early warning within 24 hours and a notification within 72 hours.[2]	Reporting and Yocto Kirkstone
After 8 December 2026	Product Liability Directive: Directive (EU) 2024/2853 applies to products placed on the market or put into service after 8 December 2026, and Member States must transpose it by 9 December 2026. Software counts as a product.[3,4]	Radar: Product Liability Directive
11 December 2027	The Cyber Resilience Act applies in full, including a support period of at least five years (unless expected use is shorter) and security updates kept available for at least 10 years.[5,6]	Radar: Cyber Resilience Act in full

A note to forward to your team

Hardware delivery risk checklist

Please answer the eight yes or no questions in this note from what you know today. It takes about five minutes.

Reply by [date] with:
1. The number of "yes" answers (out of 8)
2. The numbers of the questions answered "no"

Owner: [name]
Note: https://stonetusker.com/insights/checklist-hardware-safety-critical.html

Want a second opinion?

Answer the eight questions with your team first. If you would like a second opinion, reply with two things only: the number of "yes" answers and the numbers of the questions answered "no". Nothing else is needed. Within five working days you receive a short written note on what to do first. It is free and confidential, and a call is optional.

Ask for a second opinion

The button opens an email to subeesh@stonetusker.com with the subject and the numbers to fill in. You can also use the contact page, or reply to the email or LinkedIn message that brought you here.

Next page for your situation

- Cyber Resilience Act reporting and Yocto Kirkstone: the 30-minute check for each product line behind questions 1 to 4.
- European Union dates for device makers: the Data Act, the Machinery Regulation and the Cyber Resilience Act dates in one table.

Sources

1. Yocto Project: Releases
2. European Commission: Cyber Resilience Act reporting obligations
3. Official Journal of the European Union: Directive (EU) 2024/2853 on liability for defective products
4. Official Journal of the European Union: Corrigendum to Directive (EU) 2024/2853 (7 May 2026)
5. European Commission: Cyber Resilience Act
6. Cyber Resilience Act, Article 13 (support period)

About the author

Subeesh Sivanandan is the Founder and CEO of Stonetusker Systems. He has worked for more than 27 years in release engineering, DevOps, platform engineering & embedded Linux. His career includes serving as the Principal Engineer & Manager of Release Engineering at Stryker, alongside earlier roles at Nokia, VeriSign, and IP Infusion. LinkedIn profile.

Revision history (recent 3 updates)

Version 1.0, 29 October 2026. Every fact on this page is checked against a minimum of two sources each month.

Version	Date	Change
1.0	29 October 2026	First edition