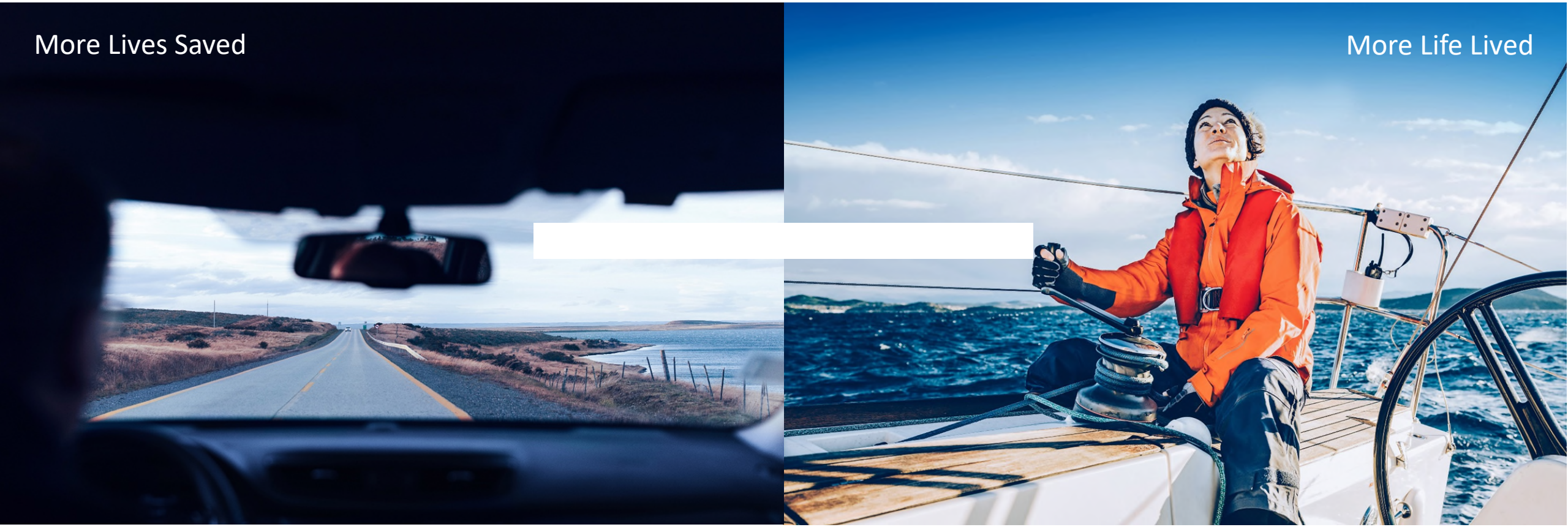

Open source i praktiken – IP-risker och strategiska överväganden för industriföretag

Linnea Harnesk

Head of IP Legal

Autoliv

IP and Open Source

Introduction – Why Open Source & IP Risk Matters Across Industry

- Open source now underpins most software-driven products: vehicles, med-tech, telecom, robotics, industrial automation, consumer electronics, AI/ML systems, and cloud services.
- Dependencies are deep, fast-moving, and often opaque.
- Regulatory frameworks (cybersecurity, product safety, export controls) increasingly intersect with open-source usage.
- Industry trend: more software, more connectivity, more updates → more exposure.

Autoliv

Licensing Landscape – Industry-Agnostic Overview

- Permissive licenses (MIT, BSD, Apache-2.0)

- Easier integration; fewer obligations.

- Popular in cloud, AI, and embedded systems.

- Weak copyleft (LGPL)

- Allows dynamic linking with conditions.

- Strong copyleft (GPLv2/v3, AGPL)

- Requires derivative works to be shared under same terms.

- AGPL extends obligations to network-based services.

- Business Impact:

- Compliance failures can lead to forced disclosure of proprietary IP or injunctions.

Autoliv

Open Source – General Definitions

Open Source: Source code is publicly accessible for inspection, modification, and redistribution under defined licenses.

Common industry interactions:

Using open-source components in products or internal tools.	Contributing to open-source projects individually or as a company. •Key tensions: •Innovation speed vs. compliance obligations. •Collaboration benefits vs. risk of disclosing proprietary know-how.

Autoliv

Industry-Wide Risk Patterns

Hidden copyleft exposure through:Statically linked GPL components inside proprietary firmware.	• Lack of clarity on what constitutes a “derivative work” across sectors. • Kernel-space vs. user-space ambiguity • Real-time systems (industrial robots, medical devices, vehicles) have tight coupling where separation boundaries are difficult to prove
SBOM quality gaps	• Incomplete or inaccurate SBOMs from suppliers remain a universal industry problem. • Over-broad claims by suppliers on what they are “allowed” to relicense.
Fragmentation of software supply chains	• Multi-tier suppliers, integrators, and global component sourcing create unclear accountability.

Autoliv

Industry-Wide Risk Patterns

- Hidden copyleft exposure through:
  - Statically linked GPL components inside proprietary firmware.
  - Lack of clarity on what constitutes a ‘derivative work’ across sectors.
- Kernel-space vs. user-space ambiguity
- Real-time systems (industrial robots, medical devices, vehicles) have tight coupling where separation boundaries are difficult to prove.
- SBOM quality gaps
  - Incomplete or inaccurate SBOMs from suppliers remain a universal industry problem.
  - Over-broad claims by suppliers on what they are ‘allowed’ to relicense.
- Fragmentation of software supply chains
- Multi-tier suppliers, integrators, and global component sourcing create unclear accountability.

Autoliv

Ownership & Patent Intersections

- Employment-created software generally belongs to the employer; clarity is needed when employees contribute upstream.
- Patent clauses in some licenses (e.g., Apache-2.0 includes express patent grant).

- Patent-related risks:
- - Using OSS may limit ability to enforce certain patents.
- - OSS contributions might unintentionally disclose valuable implementations (risk to patentability).

- Need for harmonized internal rules for contributions, review, and clearance.

Autoliv

Business Risks Across Industries

- Timeline uncertainty for OSS project maintenance and bug fixes.
- Support gaps → OSS communities are not obliged to provide fixes.
- Community sustainability → industrial reliance often exceeds community capacity.

- Regulatory alignment risk:

- Cybersecurity requirements (EU CRA, US security guidelines) require traceability and patchability, which may not align with OSS roadmaps.

Autoliv

IP-Related Risks (Generalized, Industry-Wide)

- Patent infringement embedded in OSS — unknown or emergent patents.
- Leakage of internal trade secrets or patented mechanisms via contributions without proper clearance.

- Accidental ‘copylefting’ of proprietary software through:
- - Mixing source files.
- - Static linking.
- - Reusing upstream patches internally.

- Integrating OSS outputs back into proprietary development without clean boundaries.

Autoliv

Legal Risks Across Industries

- Trade secret handling risks

- Employees or consultants may mix confidential third-party information into OSS contributions.

- Contractual conflicts

- Many OEM–supplier contracts explicitly restrict OSS use or require disclosure.

- Some partnerships prohibit certain licenses (e.g., GPL in safety-critical products).

- Lack of indemnification

- OSS communities generally do not provide indemnity.

- Industrial actors must self-manage all legal exposure.

Autoliv

Organisational & Technical Precautions (Applicable to All Sectors)

- Implement a company-wide OSS policy covering:

- Allowed and prohibited licenses;

- Review gateways;

- Component analysis workflows;

- Third-party software intake procedures.

- Consider using compliance tools (Black Duck, FOSSology, WhiteSource, etc.).
- Train developers, architects, and external consultants.
- Maintain clear approvals for both consumption and contribution.

Autoliv

Decision Path & Risk-Escalation (Industry-Wide)

A practical 5-step model:

1. Identify: Is any component copyleft?

2. Locate: Is it in kernel/firmware, business-critical functions, safety-critical logic, or a separable user-space/service layer?

3. Combine: Static vs dynamic linking, API boundaries, IPC separation.

4. Distribute: Will the product be distributed, licensed as SaaS, updated OTA, or provided to customers/suppliers?

5. Mitigate: Isolation, architectural alternatives, permissive substitutes, commercial dual-licenses.

→ Escalate unclear cases to legal/IP specialists.

Autoliv

Compliance Enforcement Trends

- (Industry-wide, not automotive-specific)

- Third parties (NGOs, consumers) increasingly allowed to enforce GPL/LGPL obligations.

- Authorities and courts expect usable, reproducible source packages (incl. build + install scripts).

- Injunction risk remains real for embedded devices across Europe.

Case Study

- Context:

- Product/software module with embedded open-source component.

- Copyleft component identified in core system.

- Distribution to customers or B2B partners.

- Key Risks:

- Obligation to disclose entire source if derivative work is found.

- Exposure of proprietary logic.

- Compliance burdens on distribution chain.

- SBOM gaps from multi-tier suppliers.

- Mitigations:

- - Prefer permissive alternatives.

- - Architectural separation.

- - Commercial licensing.

- - Full compliance planning.

Autoliv

Key Take-Aways

- Understand the license — permissive vs. copyleft has massive consequence differences.
- Monitor contributions — coordination prevents unwanted disclosure.
- Implement safeguards — policy, training, tools, and contractual alignment.
- Educate stakeholders — across R&D, procurement, product, safety, and legal.
- Treat OSS as a strategic asset — not an afterthought.

Autoliv

Q&A