{code & compliance}

FOSDEM EDITION

EV-CRA Charge with Compliance

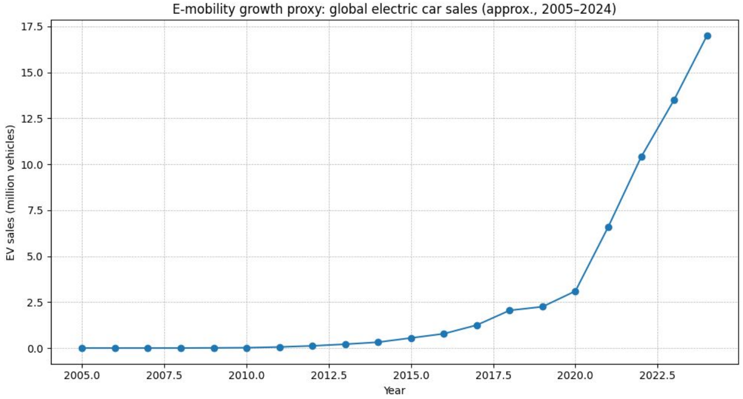
Achim Friedland // GraphDefined GmbH

29. January 2026

EV-CRA Charge with Compliance

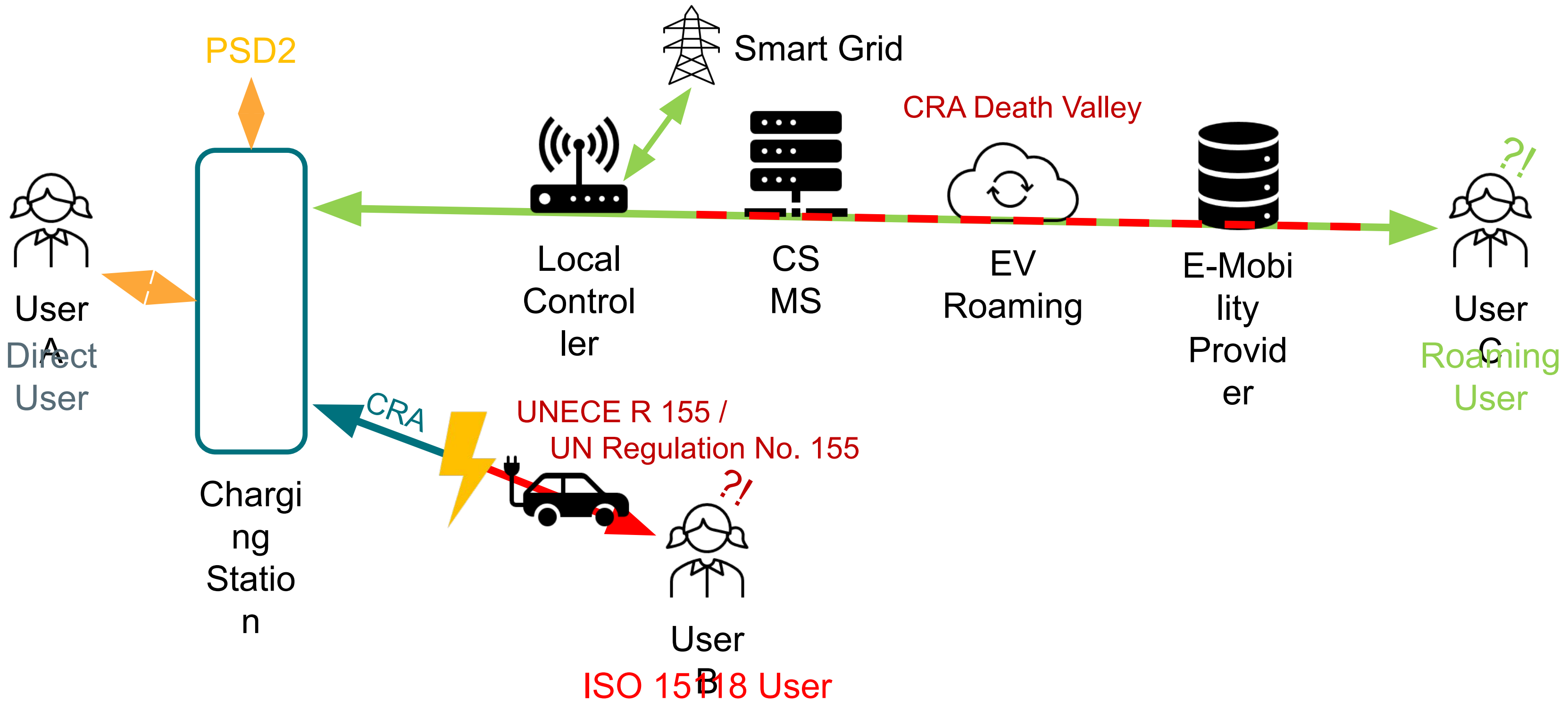
- EV Charging is no longer a niche **Internet-of-*broken*-Things** topic
- EV Charging is now **critical digital infrastructure**
- This talk is about **architecture**, not legal interpretation
- CRA and NIS2 are treated as **design constraints**, not paperwork

E-Mobility in a nutshell

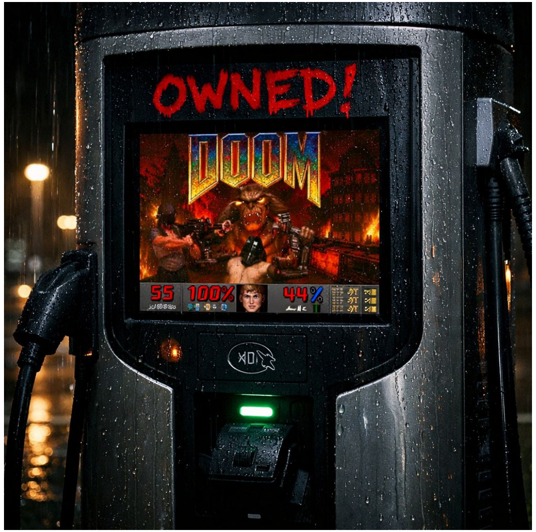


- Fast deployment, weak foundations, *“ship-and-forget”* mentality.
- Security, resilience, updateability, lifecycle and auditability are all vendor-specific secondary concerns.
- This created *long-term technical debt.*

EV Operational Environments



When specs fail to produce trust



- RFID/AutoCharge

  ~Secure technology, insecure context/environment

- German Calibration Law (Eichrecht)

  Formal compliance, no driver benefits

- ISO 15118

  Cryptography on the charging cable… only

- EU Radio Equipment Directive (EU RED)

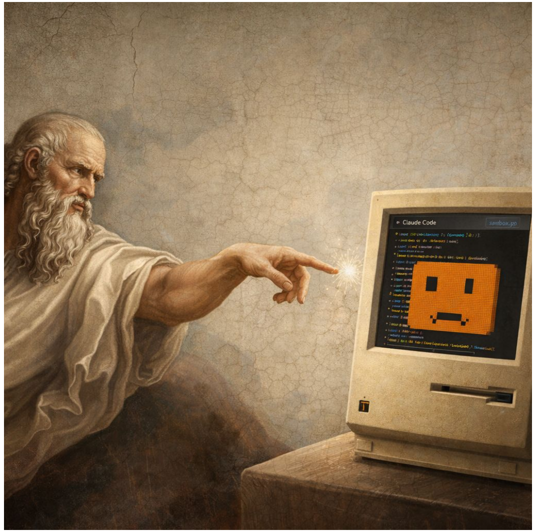
  Manufacturers prefer to disable features, instead of securing them!

When specs fail to produce trust

- Security ≠ Deployed Security
- Compliance ≠ Trust
- Intent ≠ Evidence

Once released, specs ossify asap and lame manufacturer excuses take over.

Regulation becomes design input



- Security & Resilience are no longer *“best effort”*.
- Both must be designed in and provable.
- Regulations now constrain architecture, product lifecycle development and day-to-day operations.

Uncomfortable questions for engineers

What must be enabled/dissbled by default?
What must be observable?
What must be provable years later?

- What must be enabled/disabled by default?
- What must be observable?
- What must be provable years later?

- Ad-hoc answers don’t scale!

The uncomfortable reality for regulators

- Security & resilience are cross-manufacturer obligations, not single manufacturer concerns.
- CRA/NIS2 should be interoperable between manufacturers of the same product type, otherwise security & resilience often fails.
- Inconsistent deployments increase systemic risk under NIS2.

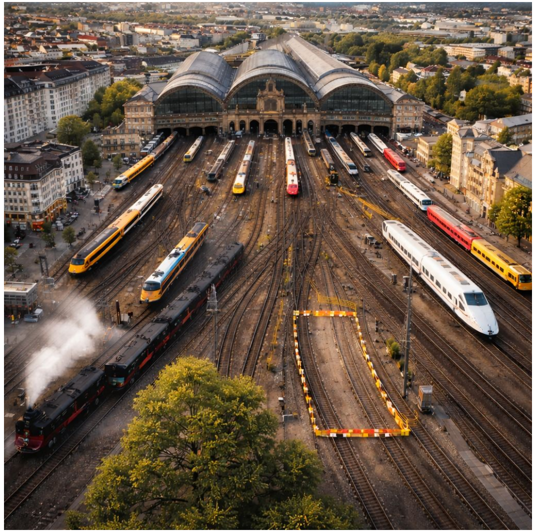
Open-Source Protocols as compliance surfaces

https://nlnet.nl/project/EVQI/

- Products & services implement some open-source management protocol, *e.g. Open Charge Point Protocol by the Open Charge Alliance (a CRA OSS Steward?)*
- Protocol encodes key assumptions, syntax, behavior, message formats, state machines, error semantics, …
- Defaults matter more than options
- Missing primitives → incompatible vendor hacks

Technical specs break under regulation

OCPP IEC 63584



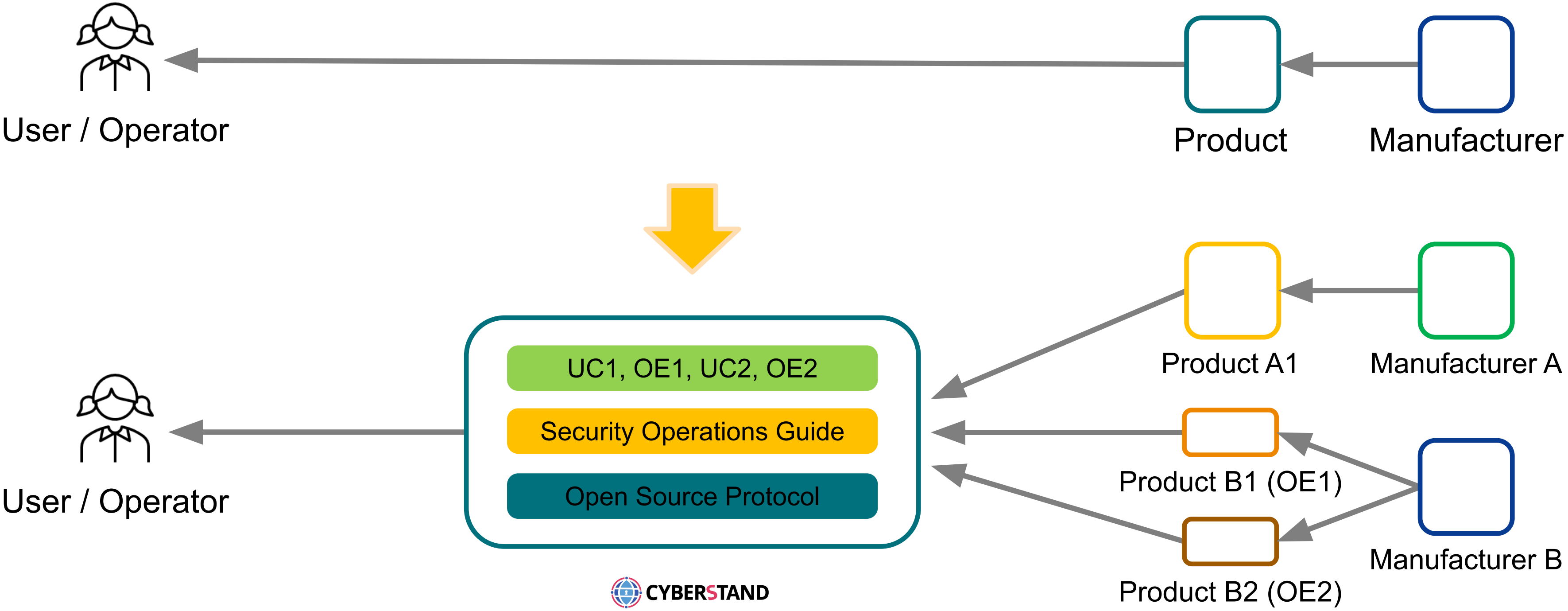
- Same protocol, too many roles.
- Same protocol, very different acceptable risks!
- Regulations care about what runs in production, not what's somehow "possible".
- Protocol ≠ deployment
- Mechanics ≠ responsibility

Security Operations Guide

https://openchargealliance.org/ocpp-info-whitepapers/security-operations-guide/

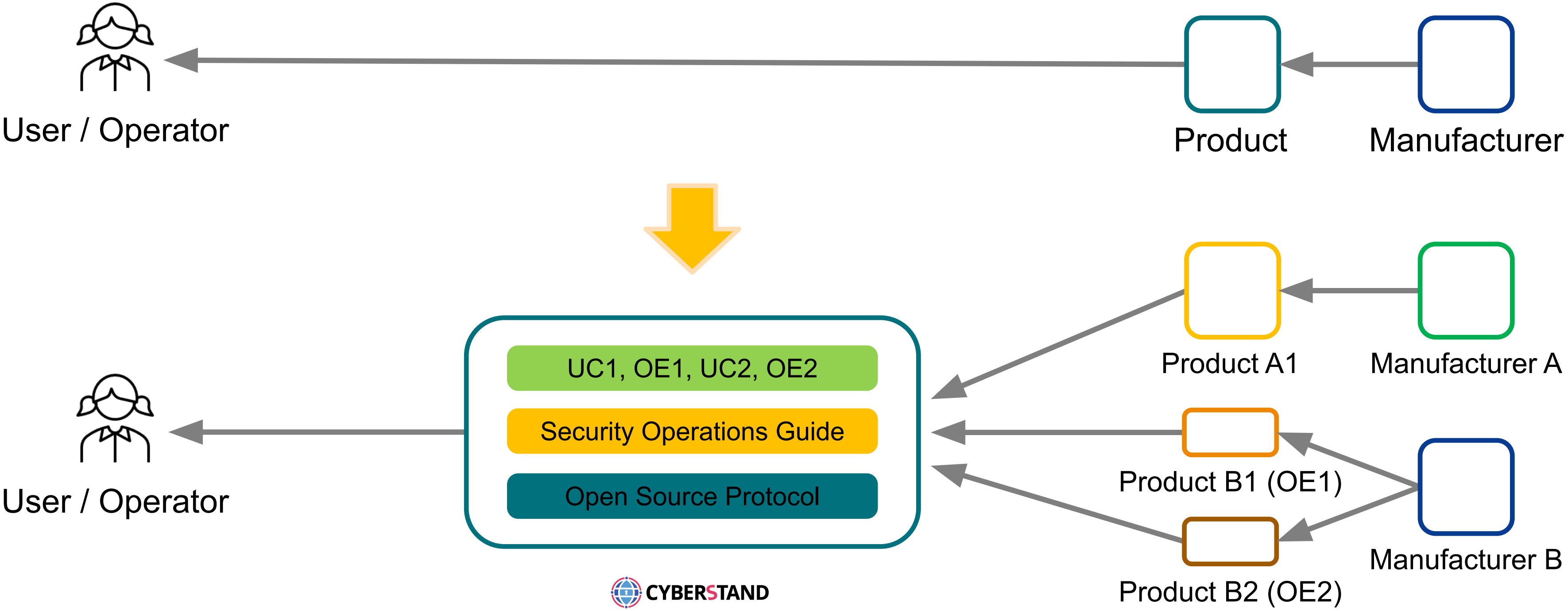
- Narrows down the protocol specification for the given use case in the given operational environment.
- Anchors operational duties.
- Describes risks, mitigations, defaults, observable controls, evidence expectations (~90% of obligations).
- Keeps interoperability stable, while allowing security and resilience to evolve.

A horizontal blueprint for vertical standards

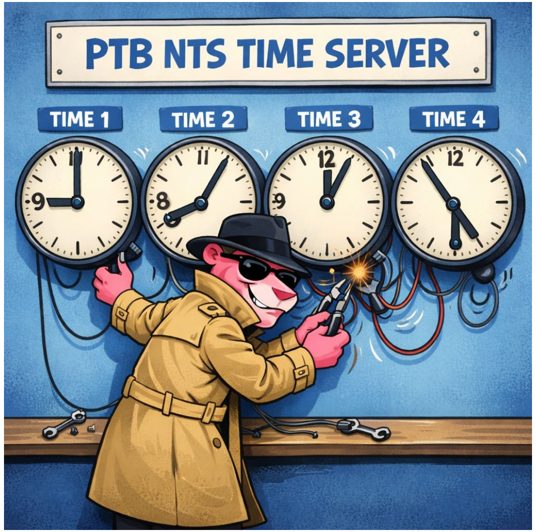


A ~~horizontal~~ blueprint for ~~vertical standards~~

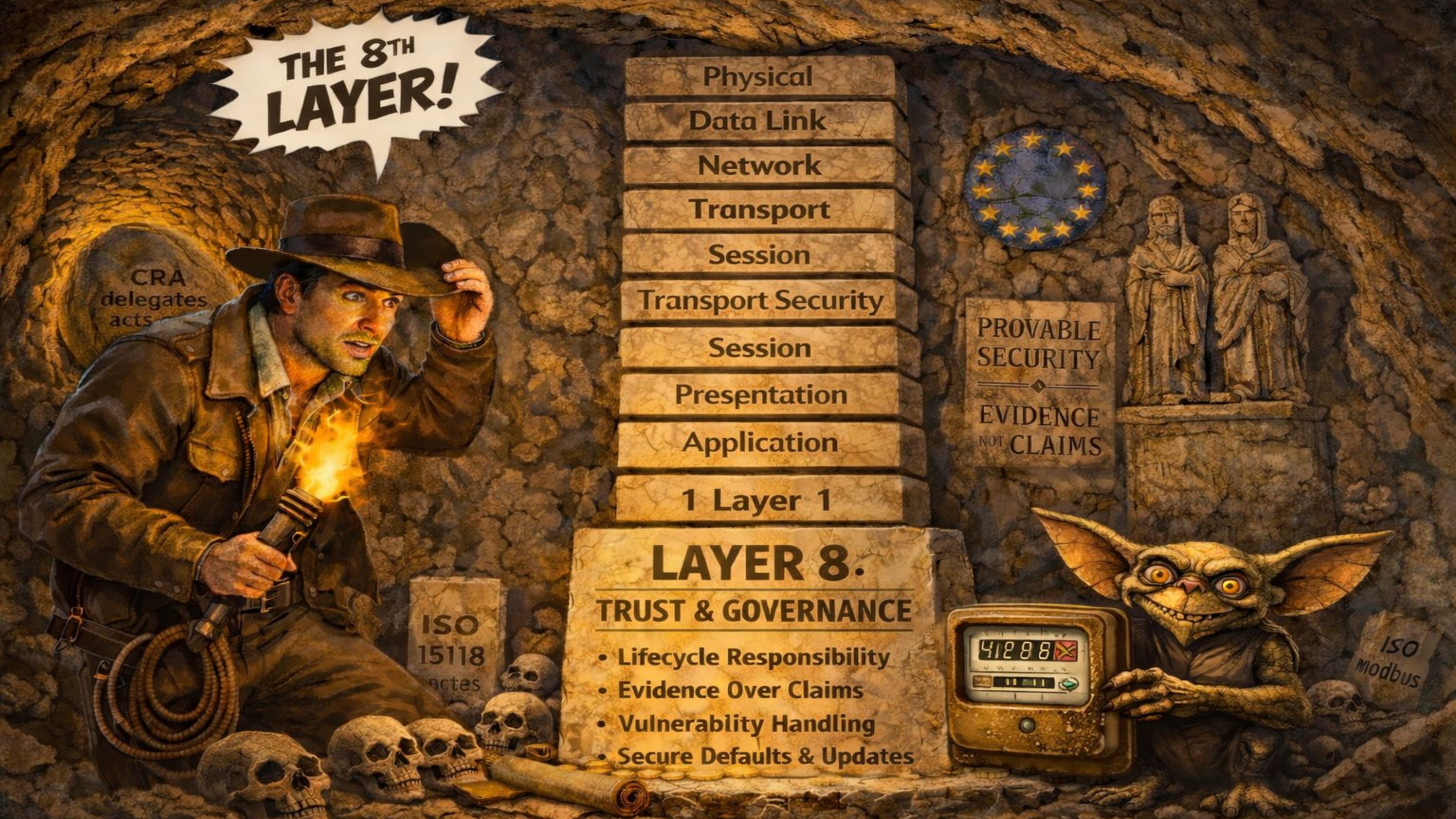
a CRA Article 25 “*Voluntary Security Attestation Framework*”?



CRA / NIS2 lives outside our protocol stacks!



- When we consume a *product* or a *service* our tooling, automation, and trust assumptions usually start on the TCP/IP networking layer: https://charging.station
- *Governance, security, resilience, vulnerabilities, …* remain *out-of-band, non-machine-readable* scattered across documentation, if mentioned at all.
- Is this still acceptable for state-of-the-art digital infrastructure?



THE 8TH LAYER!
Physical
Data Link
Network
Transport
Session
Transport Security
Session
Presentation
Application
1 Layer 1
LAYER 8.
TRUST & GOVERNANCE
• Lifecycle Responsibility
• Evidence Over Claims
• Vulnerablity Handling
• Secure Defaults & Updates
CRA delegates acts
ISO 15118 actes
PROVABLE SECURITY
EVIDENCE NOT CLAIMS
4128 8
ISO modbus

THE 8TH LAYER!
CRA delegates acts
Physical
Data Link
Netw
Trans
Sessi
Transp
PROVABLE SECURITY
EVIDENCE CLAIMS
LAYER 8.
TRUST & GOVERNANCE
• Lifecycle Responsibility
• Evidence Over Claims
• Vulnerablity Handling
• Secure Defaults & Updates
ISO 15118 actes
41288
ISO modbus

to be continued…

FOSDEM

CRA in practice Devroom

Saturday 15:30