OMNISECURE®

SUPPLY CHAIN RISK MANAGEMENT

SOFTWARE BILL OF MATERIALS

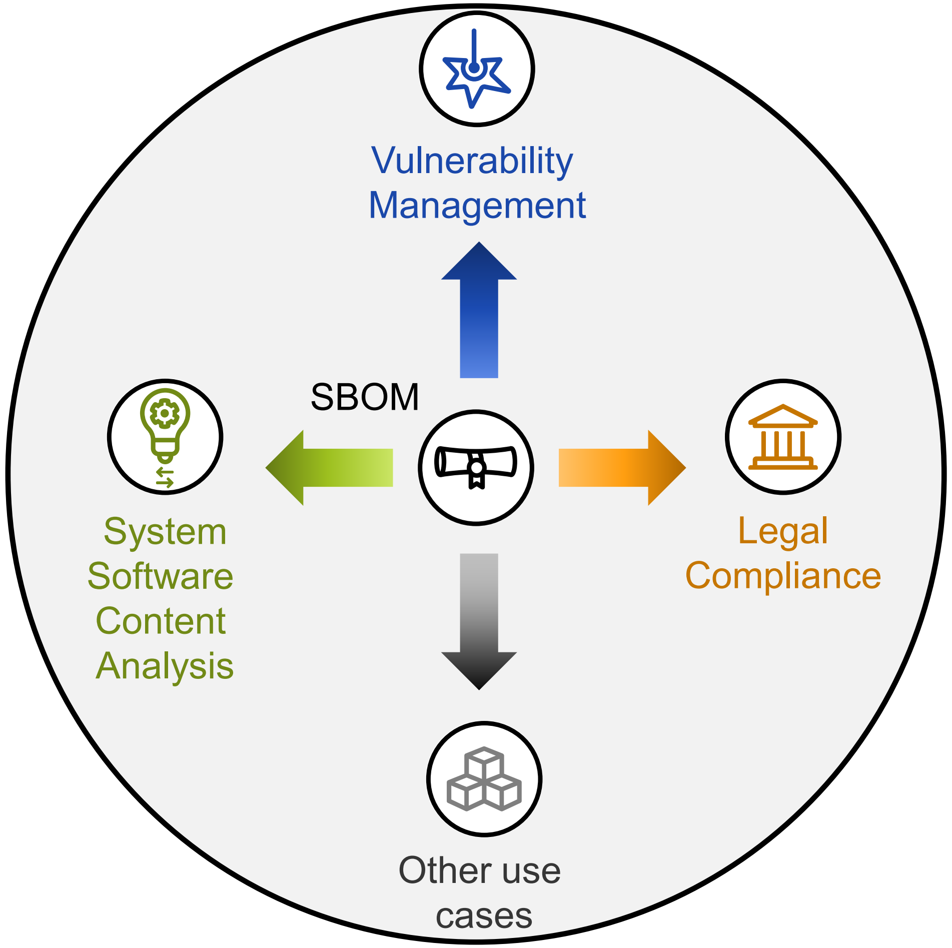
Hauke Meyn
Fellow, Head of Software Security Assessment

MAY 2023

NXP | SECURE CONNECTIONS FOR A SMARTER WORLD

PUBLIC

SOFTWARE BILL OF MATERIALS
ENABLING KEY USE CASES



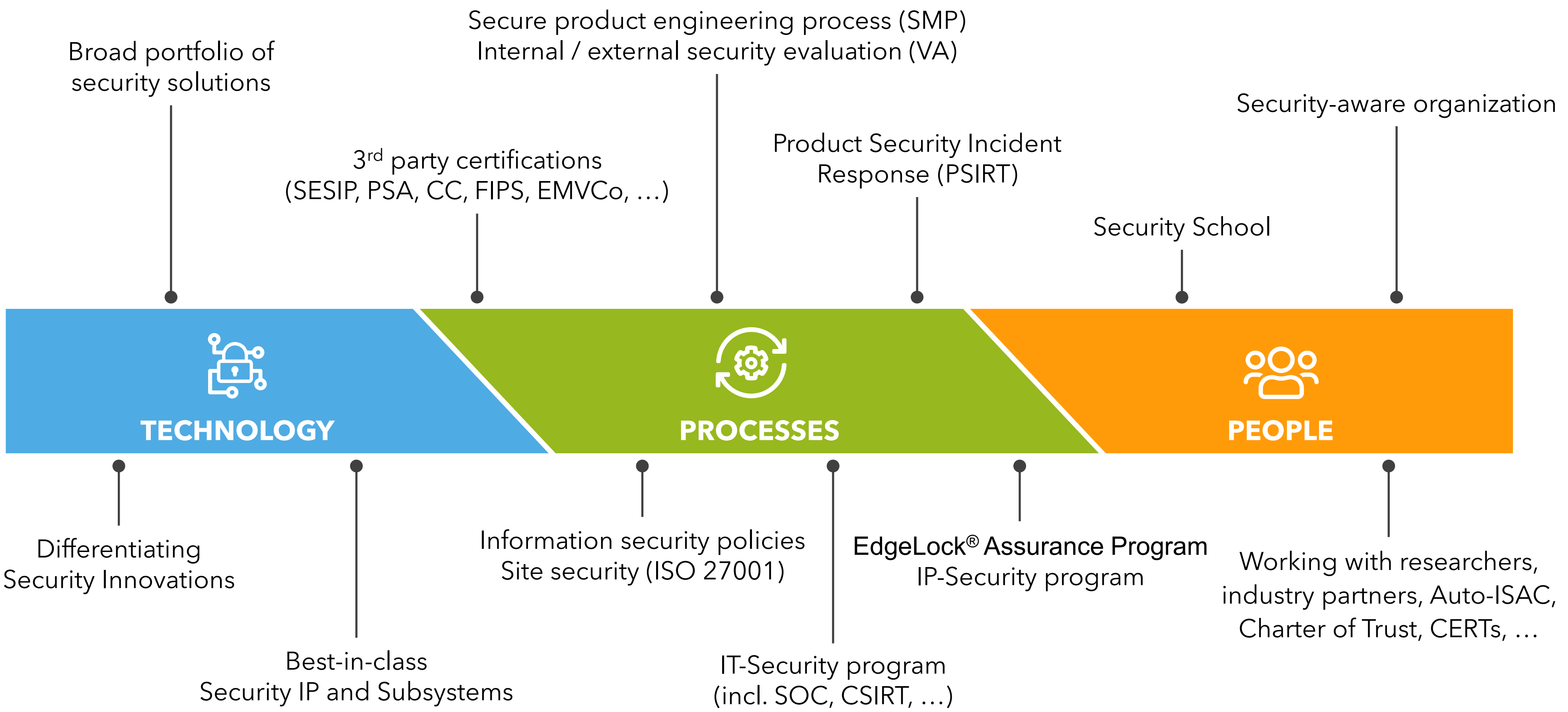
- A Secure Supply Chain requires an active risk management of several aspects; key ingredients are
  - A system level Software Content Analyses
  - Legal Compliance (per involved party)
  - Vulnerability Management (per included component)
  - An overall Software Bill of Materials (SBOMs)
- SBOMs are
  - A baseline towards additional use cases
  - A means to propagate information along the supply chain (hierarchical SBOMs)
  - Not a plain list of contained source code files
- NXP is applying those key ingredients for many years

SECURITY-BY-DESIGN AT NXP

- A holistic approach to product (cyber)security through technology, processes, and people
- Some examples thereof
  - EdgeLock® Assurance
  - Product Security Incident Response Team
  - Security Evaluations for IoT Platforms

A holistic approach to product (cyber)security – aligned with industry standards & best-practices

NXP'S PRODUCT SECURITY PROGRAM



20+ YEARS IN THE SECURITY INDUSTRY

Broad portfolio of security solutions

3rd party certifications (SESIP, PSA, CC, FIPS, EMVCo, …)

Secure product engineering process (SMP)
Internal / external security evaluation (VA)

Product Security Incident Response (PSIRT)

Security School

Security-aware organization

Differentiating Security Innovations

Best-in-class Security IP and Subsystems

Information security policies
Site security (ISO 27001)

IT-Security program (incl. SOC, CSIRT, …)

EdgeLock® Assurance Program
IP-Security program

Working with researchers, industry partners, Auto-ISAC, Charter of Trust, CERTs, …

EdgeLock® Assurance

Security is fundamental to the solutions we create. When you see EdgeLock® Assurance, you'll know it's designed to meet industry standards. Proven processes and validation assessments help ensure we deliver trusted solutions for your security challenges. Together, we can advance the world securely with confidence.

EDGELOCK® ASSURANCE by NXP

PRODUCT SECURITY INCIDENT RESPONSE TEAM (PSIRT)

Manages product security incidents

Global across products / markets / regions

Established in 2008 after the MIFARE Classic hack

Committed to coordinated / responsible disclosure

In alignment with the security community

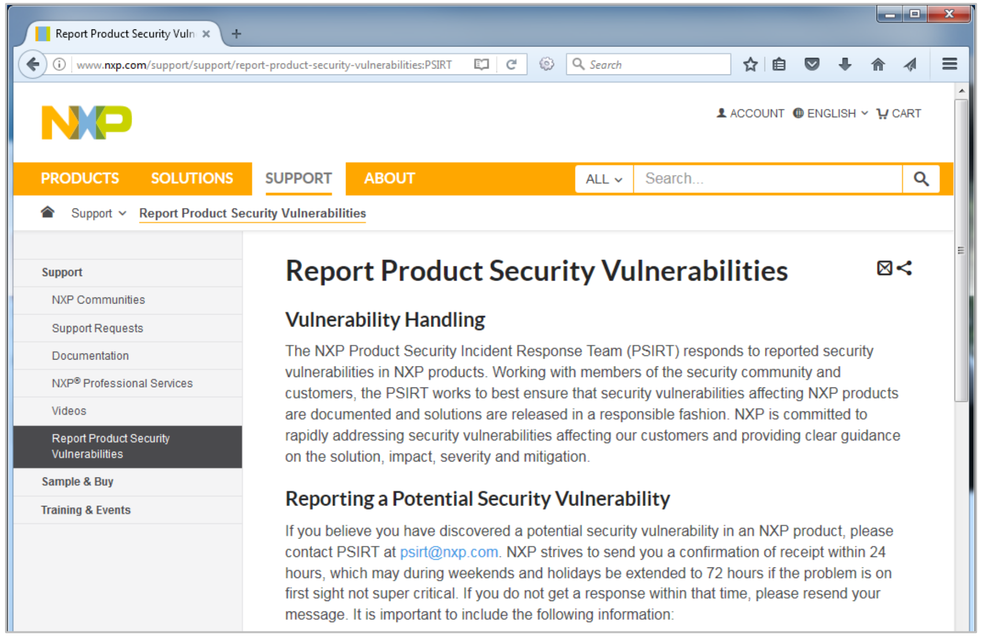
With our customers, partners, Auto-ISAC, CERTs

Key success factors

Timely sharing of ‘complete’ information, on a need-to-know basis

Preparation and exercises

Continuous improvement – e.g., evaluate and benchmark against Auto-ISAC’s best practice guide for incidence response


Report Product Security Vuln ×
www.nxp.com/support/support/report-product-security-vulnerabilities:PSIRT
Search
NXP
ACCOUNT
ENGLISH
CART
PRODUCTS
SOLUTIONS
SUPPORT
ABOUT
ALL
Search...
Support
Report Product Security Vulnerabilities
Support
NXP Communities
Support Requests
Documentation
NXP® Professional Services
Videos
Report Product Security Vulnerabilities
Sample & Buy
Training & Events

Report Product Security Vulnerabilities

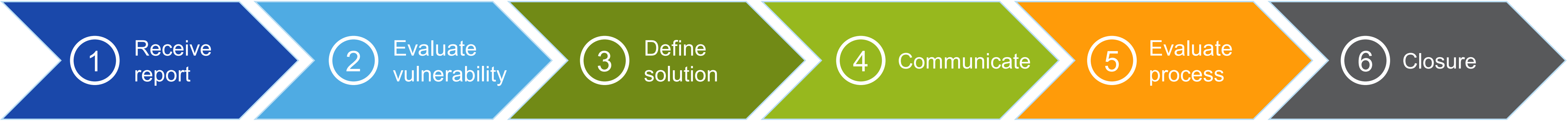
Vulnerability Handling

The NXP Product Security Incident Response Team (PSIRT) responds to reported security vulnerabilities in NXP products. Working with members of the security community and customers, the PSIRT works to best ensure that security vulnerabilities affecting NXP products are documented and solutions are released in a responsible fashion. NXP is committed to rapidly addressing security vulnerabilities affecting our customers and providing clear guidance on the solution, impact, severity and mitigation.

Reporting a Potential Security Vulnerability

If you believe you have discovered a potential security vulnerability in an NXP product, please contact PSIRT at psirt@nxp.com. NXP strives to send you a confirmation of receipt within 24 hours, which may during weekends and holidays be extended to 72 hours if the problem is on first sight not super critical. If you do not get a response within that time, please resend your message. It is important to include the following information:

Web site: www.nxp.com/psirt   Contact: psirt@nxp.com



1 Receive report

2 Evaluate vulnerability

3 Define solution

4 Communicate

5 Evaluate process

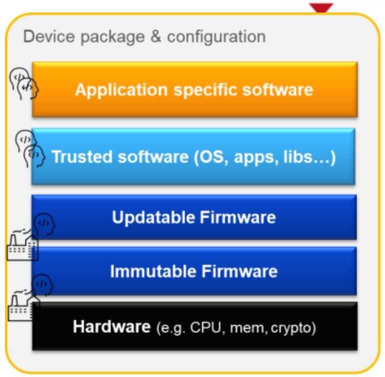
6 Closure

SECURITY EVALUATION OF SECURE IOT PLATFORMS (SESIP) – EN17927:2022

- SESIP is a security evaluation & certification framework
  - The evaluation scope and evaluation depth not pre-defined: Claims are made per product
  - Allows flexibility on security claims
  - Uses Protection Profiles as security references and baselines
- System-Level Security for IoT Applications (see Blog post)
  - Tailored to address building blocks of IoT devices up to a full platform and to evaluate their security services

  → Harmonization of functional security claims
  - Enables composition and re-use of evaluation results

cen CENELEC


Device package & configuration
Application specific software
Trusted software (OS, apps, libs…)
Updatable Firmware
Immutable Firmware
Hardware (e.g. CPU, mem, crypto)

LABS

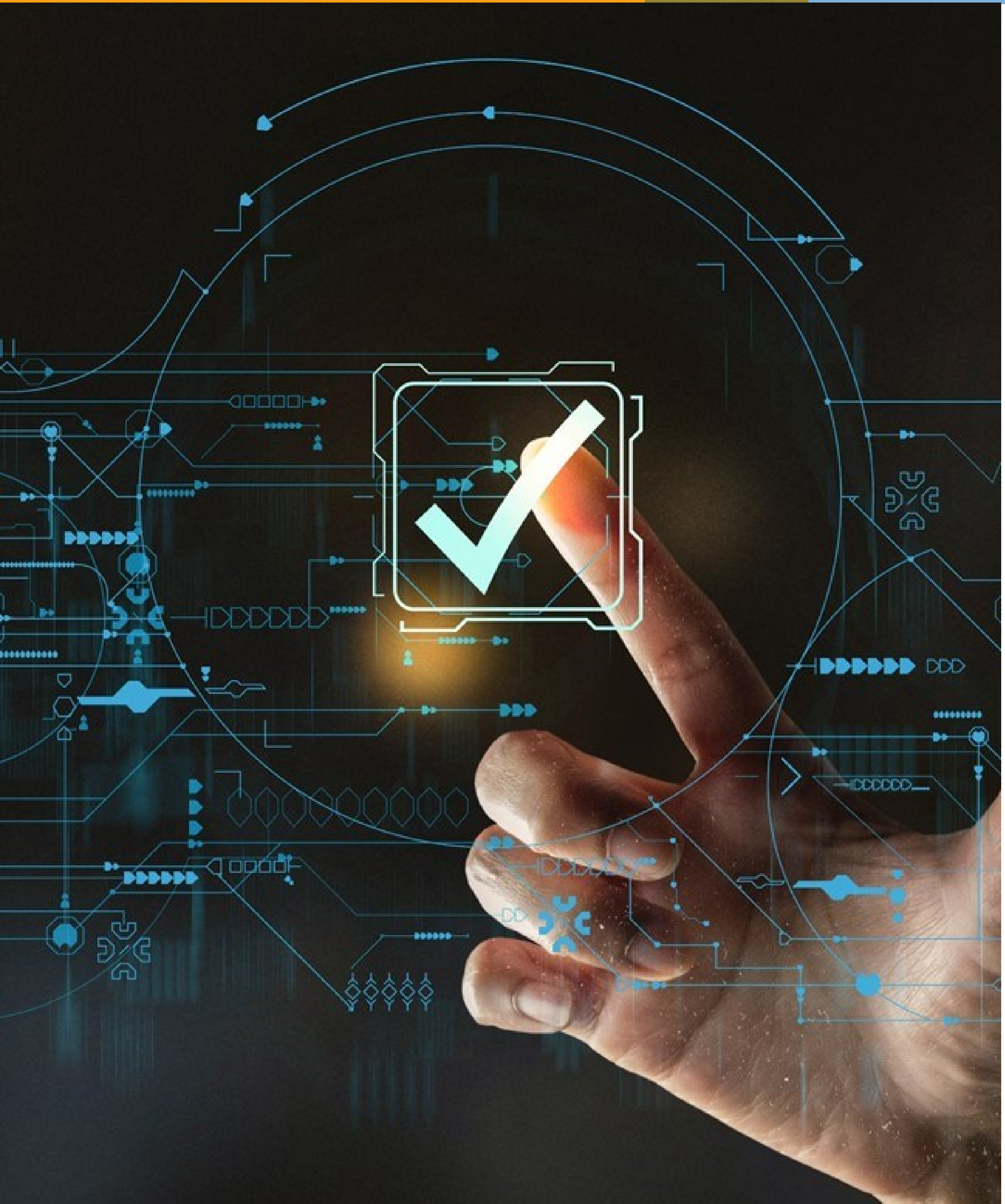
TRUSTCB Applus jtsec riscure
SGS brightsight TÜViT TÜV NORD GROUP SERMA SAFETY & SECURITY

INDUSTRY

aws freeRTOS
SECURE THINGZ TRUSTED OBJECTS
NXP SILICON LABS MICROCHIP ST life.augmented
RENESAS winbond

INDUSTRY GROUPS

psacertified™ CARCONNECTIVITY consortium®
csa connectivity standards alliance GSMA WIRELESS POWER CONSORTIUM



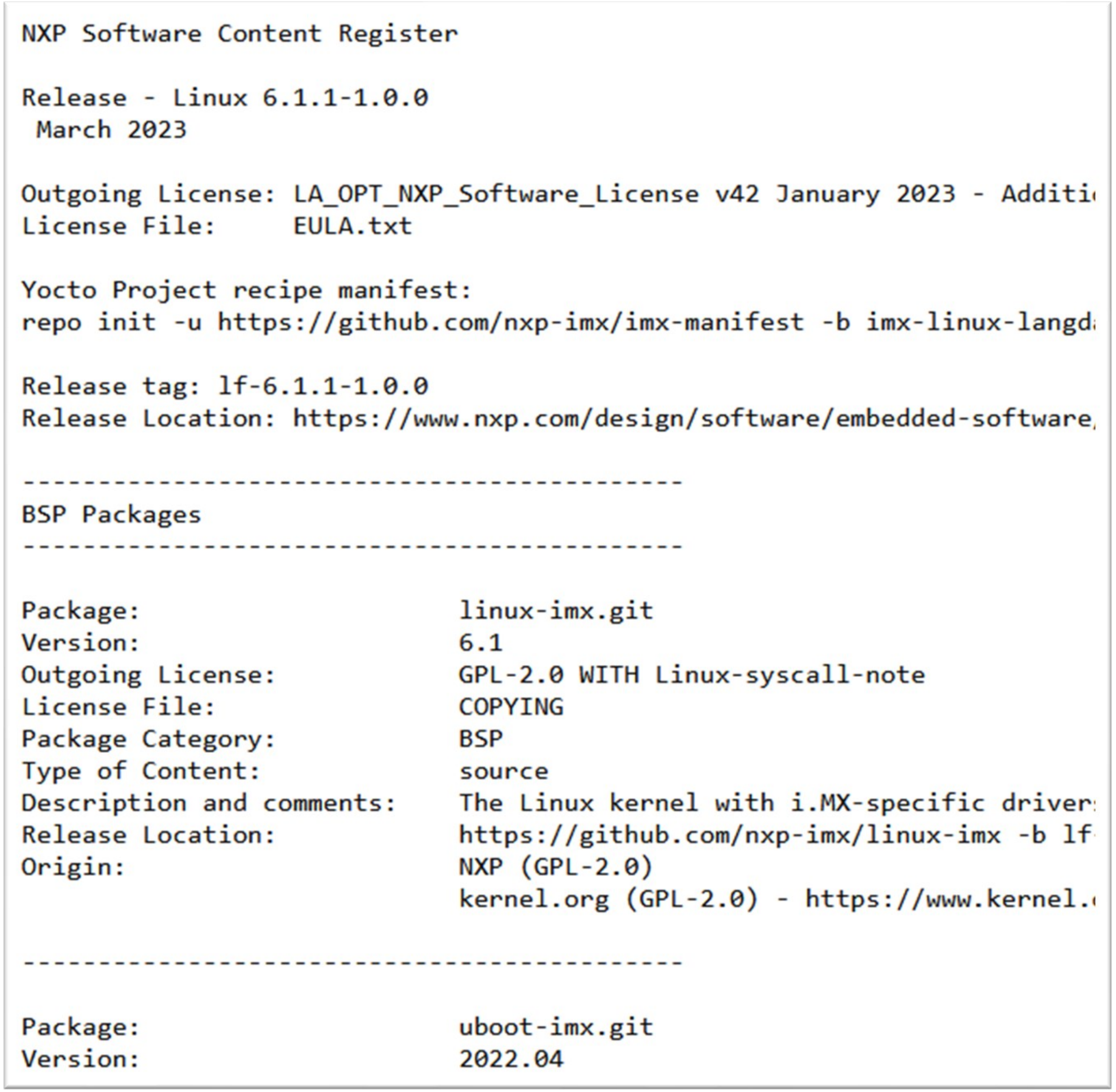
SBOMS AT NXP

- NXP delivers Software Content Registers (SCRs) for any SW release for many years already.
  - See example on next slide.
- NXP is migrating from SCRs to SBOMs in SPDX/JSON format.
  - Minimum viable and interoperable SBOM content needs global alignment.
- Vulnerability information based on CSAF/VEX and SBOMs is the next step.

SOFTWARE CONTENT REGISTER

- Software Content Registers (SCRs) are essentially SBOMs in a plain text file

- Example taken from https://github.com/nxp-imx/meta-imx
  - File: SCR-6.1.1-1.0.0.txt



```
NXP Software Content Register

Release - Linux 6.1.1-1.0.0
 March 2023

Outgoing License: LA_OPT_NXP_Software_License v42 January 2023 - Additi
License File:     EULA.txt

Yocto Project recipe manifest:
repo init -u https://github.com/nxp-imx/imx-manifest -b imx-linux-langd

Release tag: lf-6.1.1-1.0.0
Release Location: https://www.nxp.com/design/software/embedded-software

--------------------------------------------
BSP Packages
--------------------------------------------


Package:                     linux-imx.git
Version:                     6.1
Outgoing License:            GPL-2.0 WITH Linux-syscall-note
License File:                COPYING
Package Category:            BSP
Type of Content:             source
Description and comments:    The Linux kernel with i.MX-specific driver
Release Location:            https://github.com/nxp-imx/linux-imx -b lf
Origin:                      NXP (GPL-2.0)
                             kernel.org (GPL-2.0) - https://www.kernel.


--------------------------------------------


Package:                     uboot-imx.git
Version:                     2022.04
```

CONCLUSION

- Increasing requirements for machine-readable SBOMs in the industry
  - Interchangeable SBOMs are being deployed as we speak
  - Detailed and complete Software Content Analysis required as baseline

- Exchanging vulnerability information is the next big step towards a secure supply chain

- NXP has a track record of delivering secure solutions for many years
  - Holistic approach to product (cyber)security through technology, processes, and people
  - A Software Content Register is an established part of our security culture,

  and
  - We're busy implementing and migrating towards machine-readable SBOMs

SECURE CONNECTIONS
FOR A SMARTER WORLD

TECHNOLOGY SHOWROOM

JOURNEYS BY DESIRED ENGAGEMENT

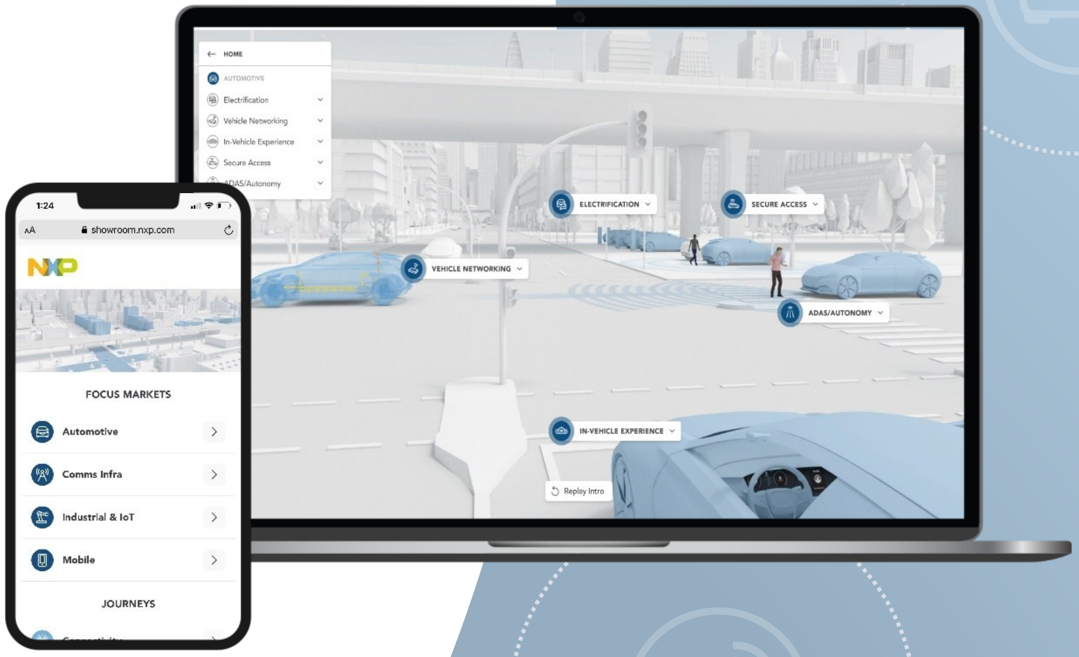
Self-guided tour
Live-streaming at set times
Guided tours

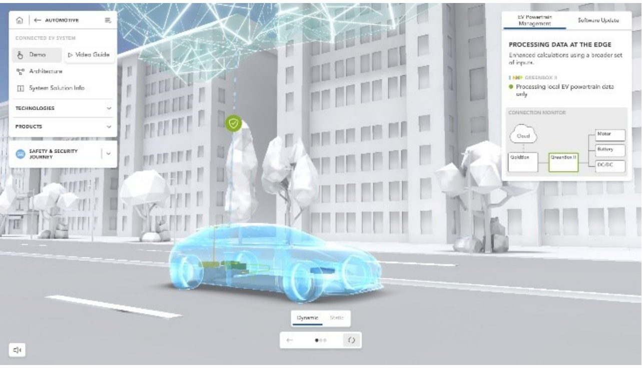
40+ VIRTUAL DEMOS

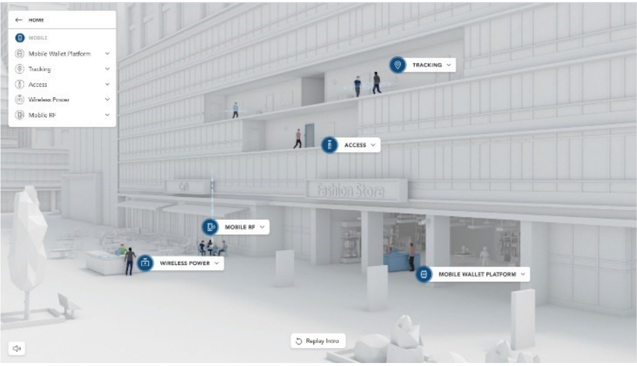
Focus on system solutions
Set up along NXP verticals

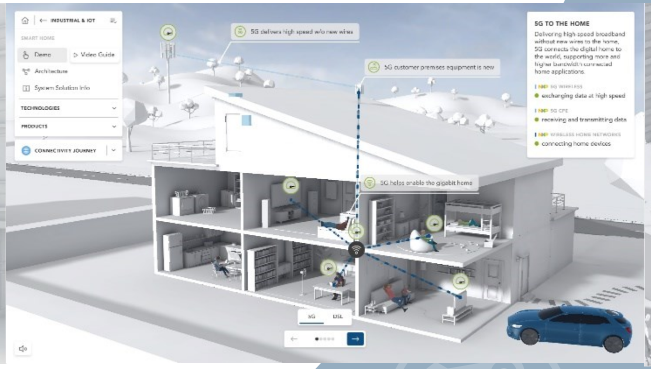
JOURNEYS BY DESIRED FOCUS

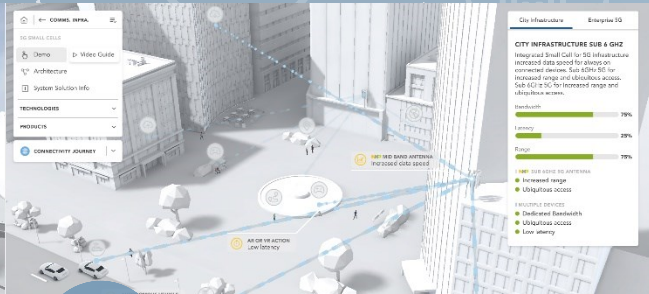
Edge & AI/ML
Safety & Security
Connectivity
Analog











SHOWROOM.NXP.COM

SECURE CONNECTIONS
FOR A SMARTER WORLD

SHOWROOM.NXP.COM