LINUX FOUNDATION
COLLABORATIVE PROJECTS

CIVIL INFRASTRUCTURE PLATFORM

CIP Security towards achieving Industrial grade security

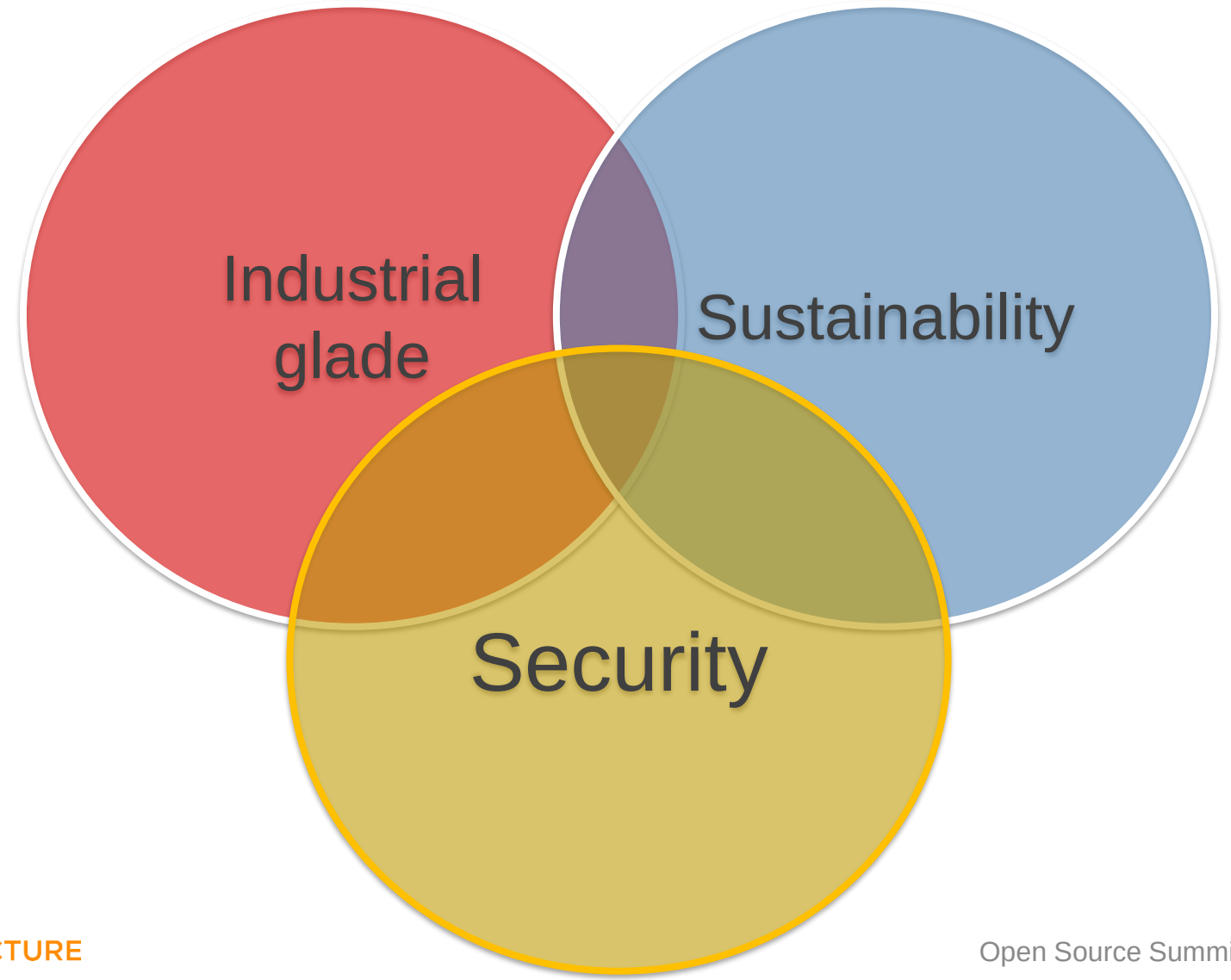
Kento Yoshida, Renesas Electronics Corporation &

Dinesh Kumar, Toshiba Software India

Agenda

- First session
  - The structure of the security working group
  - CIP-IEC-62443-4-x assessment progress
  - The report of the investigation for IEC 62443-4-2
- Second session
  - CIP approach to meet IEC-62443-4-1 requirements
  - IEC-62443-4-1 key practices
  - IEC-62443-4-1 key requirements and challenges to meet
  - Advantage CIP Vs non-CIP OSS distributions

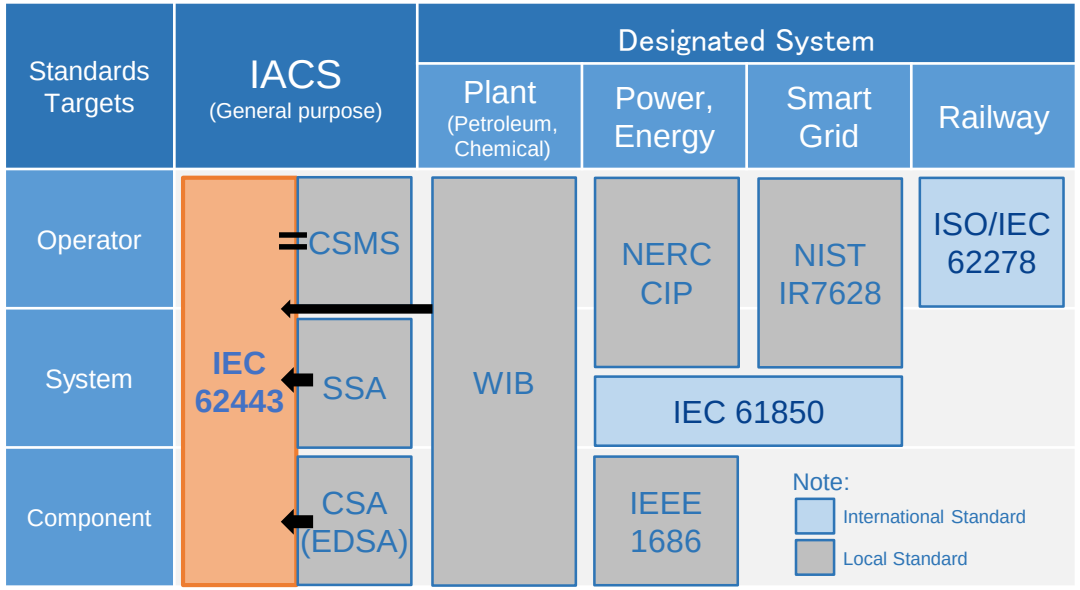
Security is one of the key challenges of the CIP project

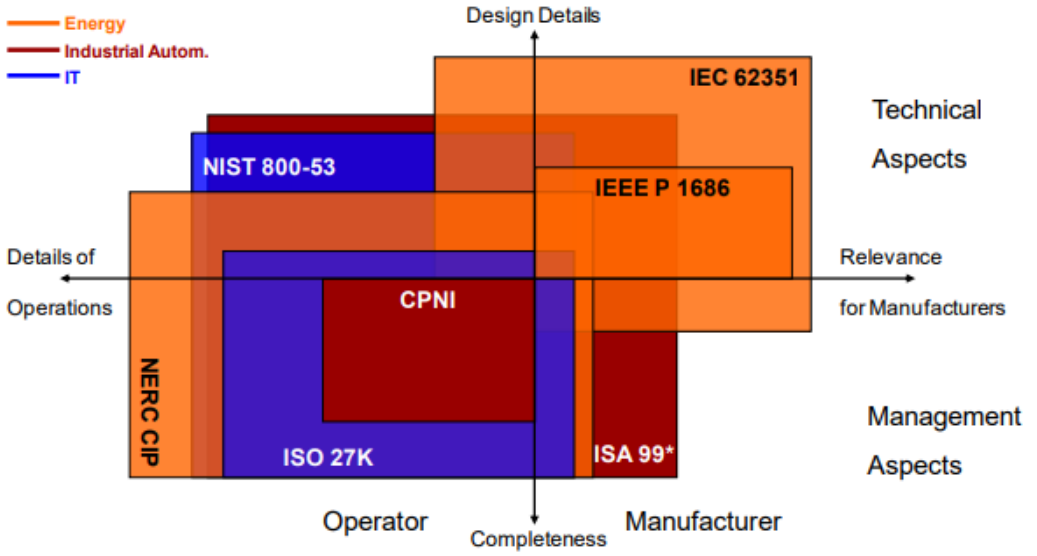


CIVIL INFRASTRUCTURE PLATFORM

Addressing integrated cyber security for the industry

- IEC 62443 is an international standard series that integrates major industrial security standards for each industry. And the series is for all players in the industrial automation and control systems, IACS.





*ISA 99 indicates IEC 62443

Mission and goal

- Security working group's mission:

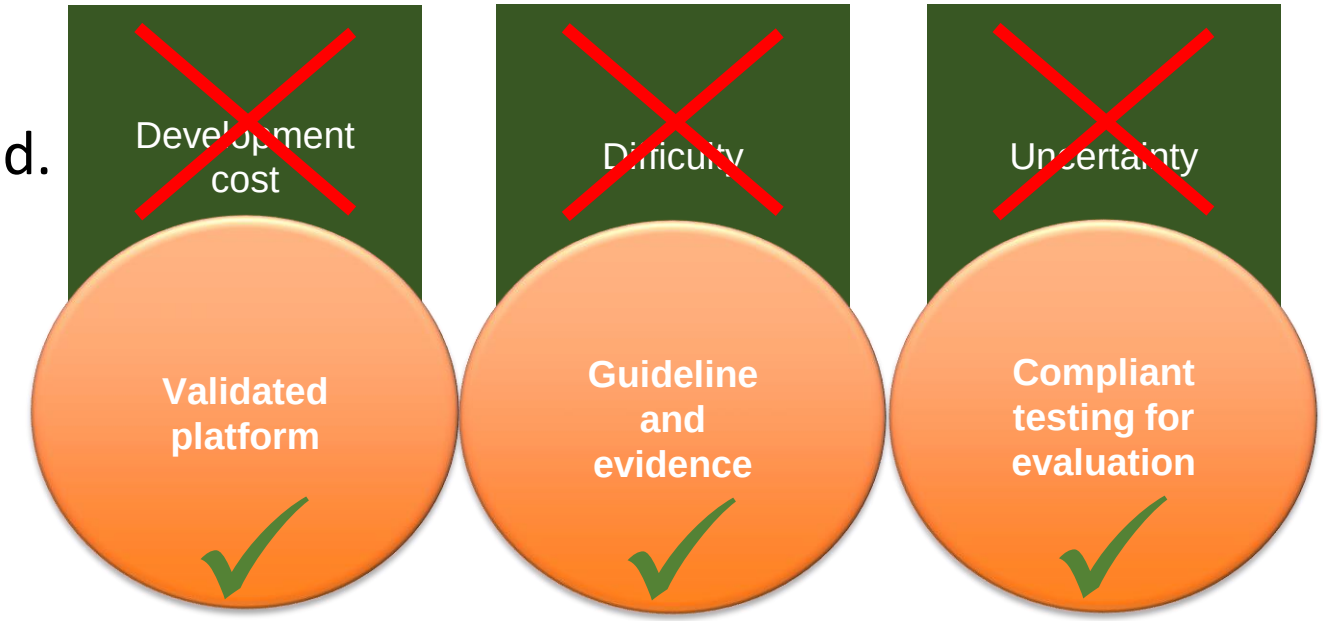
  Provide "Open source base layer - OSBL" needed for developing products compliant with IEC 62443-4-2 security requirements as well as to keep its security up to date.

- Goal:

  Get suppliers IEC 62443-4-2 certified.

  For that...

  Our solution makes IEC 62443-4-2 certification easier!



CIVIL INFRASTRUCTURE PLATFORM

The structure of this working group

- Members

  8 people from 6/8 CIP member companies

- Meetings

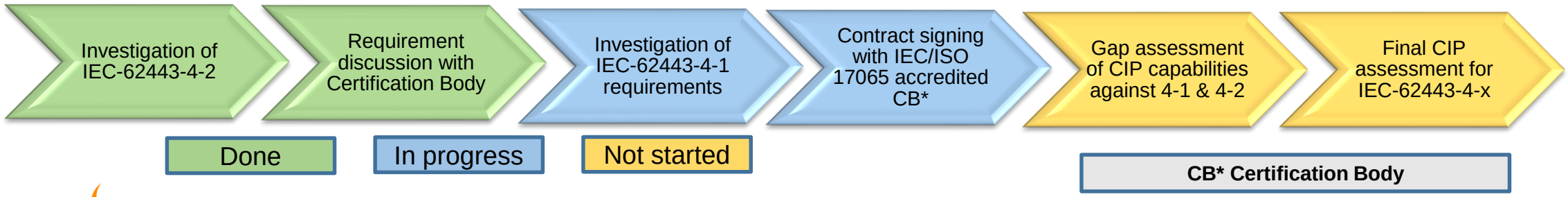
  <In private> CIP security WG meeting, every other Wednesday

  <In private> CIP security technical IRC, every Thursday

  CIP TSC meeting, CIP kernel IRC, ...

CIP-IEC-62443-4-x assessment progress

- CIP Security Work Group began investigation of IEC-62443-4-2 to understand about security requirements
- Each requirement of IEC-62443-4-2 was reviewed and investigated how it can be met by adding Debian packages
- From CIP's investigation of IEC-62443-4-2, it was evident CIP can meet SL-3, however it is yet to be confirmed with Certification Body
- We have clarified several queries with CB related to development and maintenance, but still few things would be clarified as part of Gap assessment
- Further details is available at [CIP IEC info page]
- One of the IEC/ISAO 17065 accredited Certification body has been finalized for CIP IEC-62443-4-x assessment

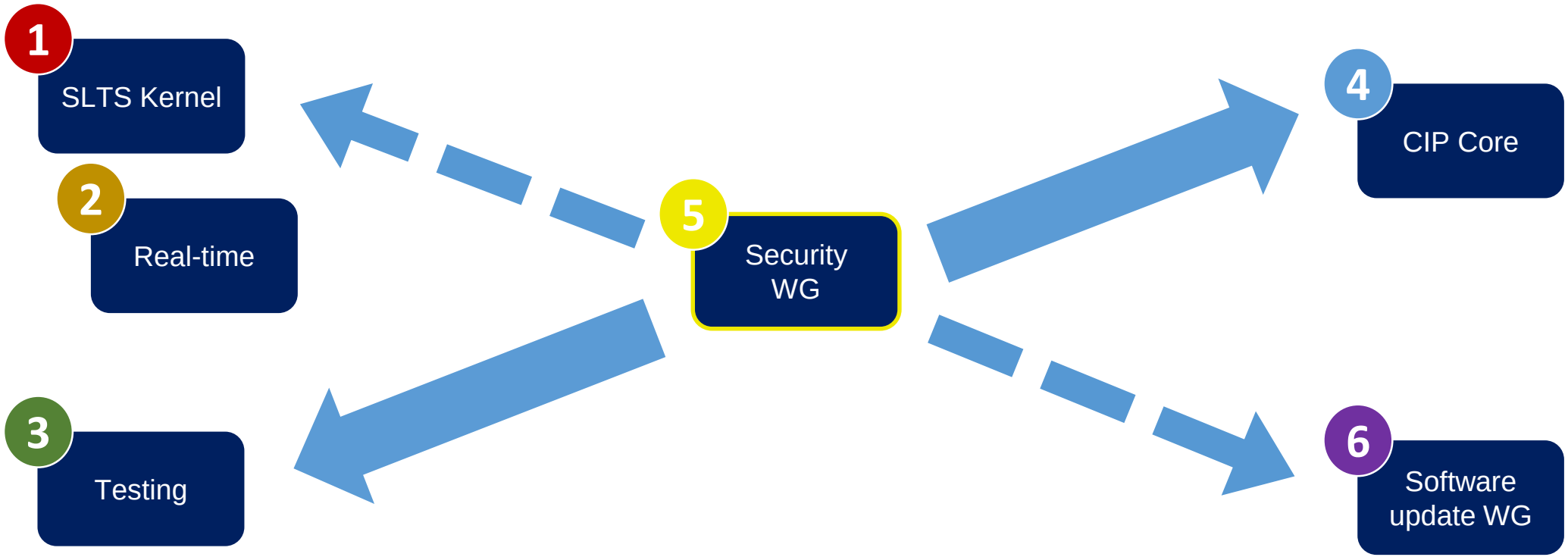


CIVIL INFRASTRUCTURE PLATFORM

Contribution to achieve industrial security

- Provide test cases / package lists / secure SW updating to meet IEC 62443-4-2 technical requirements
- Define secure process based on IEC 62443-4-1* tailored to each development life-cycle

*Required to support the secure software development processes described in IEC 62443-4-1 to get IEC 62443-4-2.



The report of the investigation for IEC 62443-4-2

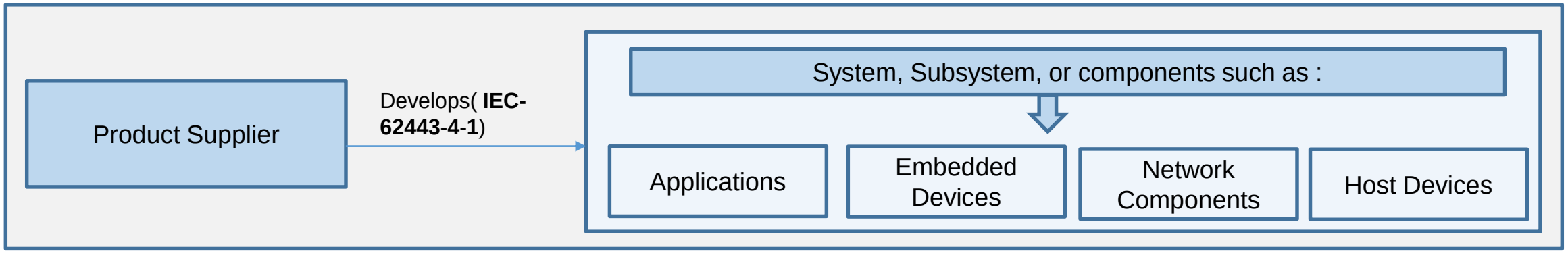
- Chose a list of about 20 valid debian packages to meet security level 3 of IEC 62443-4-2
- Provide a viable solution for 48 of all 77 requirements for embedded devices

SL-3 Requirements for embedded devices including enhancement

FR 1 – Identification and authentication control (IAC)	15 / 19 requirements, including 3 HW requirements
FR 2 – Use control (UC)	12 / 19 requirements, including 3 HW requirements
FR 3 – System integrity (SI)	11 / 20 requirements, including 6 HW requirements
FR 4 – Data confidentiality (DC)	04 / 05 requirements
FR 5 – Restricted data flow (RDF)	00 / 01 requirements
FR 6 – Timely response to events (TRE)	03 / 03 requirements
FR 7 – Resource availability (RA)	03 / 10 requirements

IEC-62443-4-1 Practices

- ✓ Security Management
- ✓ Specification of Security Requirements
- ✓ Secure by Design
- ✓ Secure Implementation
- ✓ Security verification and validation testing
- ✓ Management of security related issues
- ✓ Security update management
- ✓ Security guidelines



Source* http://my.ldrasoftware.co.uk/repository/whitepapers/Applying_IEC_62443_4_1_Technical_Overview_v2_0.pdf

IEC-62443-4-1 Key elements

- The scope of IEC 62443-4-1 is limited to the developer and maintainer of a secure product
- Encourages security concerns to be proactively addressed at an early stage in the product lifecycle
- Encourages to do Threat analysis and risk assessment to establish trust boundaries for process, data and control flow
- A thorough Security verification and validation testing

Key challenges to meet 4-1 requirements in CIP

- Considering open source nature of CIP and not being end product, there are few challenges for meeting IEC-62443-4-1 requirements

Development environment security	Following secure design principles	Defence in depth measures	Security implementation review	Defining Threat Model
• In OSS development , many developers contribute, making sure all stages of development are secured is the challenge	• OSS components are designed by many people and organizations, ensuring secure design is challenging	• Ensuring defence in depth measures will be supported by environment where product is deployed is bit challenging	• Reviewing all changes or implementation to confirm security measures is challenging	• CIP being a platform poses challenge to define Threat Model since it's boundaries are not known

CIP's approach to address 4-1 key challenges

- Despite many challenges, CIP Security work group is embarking to meet these challenges and will further discuss with CB ways to overcome these challenges

Development environment security	Following secure design principles	Defence in depth measures	Security implementation review	Defining Threat Model
• Re-use existing OSS infrastructure such as combination or private and public repos • Exploit merge feature to control software modifications	• CIP plans to document how to protect open interfaces, restricted access based on roles • Few secure design principles depend upon type of product and it's use cases • Plan to discuss further with CB during Gap assessment	• The overall objective is to reduce attack surfaces • Document general measures for defence in depth • Product specific measures have to be taken by end product owners	• CIP team reviews each security fix before applying to CIP • Plans to closely track CVEs of critical issues and regularly release security fixes	• Threat model needs to be defined with respect to some product, CIP being a platform can't address all aspects of threat modelling • It is planned to define a generic threat model to meet this requirement

Maintaining IEC-62443-4-x certification for long term

Final certification for IEC-62443-4-x

CB defines change control process along with certification

Modifications after IEC-62443-4-x certification

Follow change control process and modify/update certified product

Changes are allowed as many times as required

After 3 years CB audits all the past changes

If all changes are found in accordance with change control process, certification is renewed/invalidated

CIVIL INFRASTRUCTURE PLATFORM

Creating CIP isar test image with security packages

Download isar iec security evaluation source from repository

```
$git clone https://gitlab.com/cip-project/cip-core/isar-cip-core.git
$git checkout security/iec-evaluation
```

Install kas-docker

```
$wget https://raw.githubusercontent.com/siemens/kas/master/kas-docker
$chmod a+x kas-docker
```

Build image for QEMU x86 64bit machine.

```
$ ./kas-docker --isar build --target cip-core-image-security kas.yml:board-qemu-amd64.yml
```

Run image in QEMU

```
$ ./start-qemu.sh x86
```

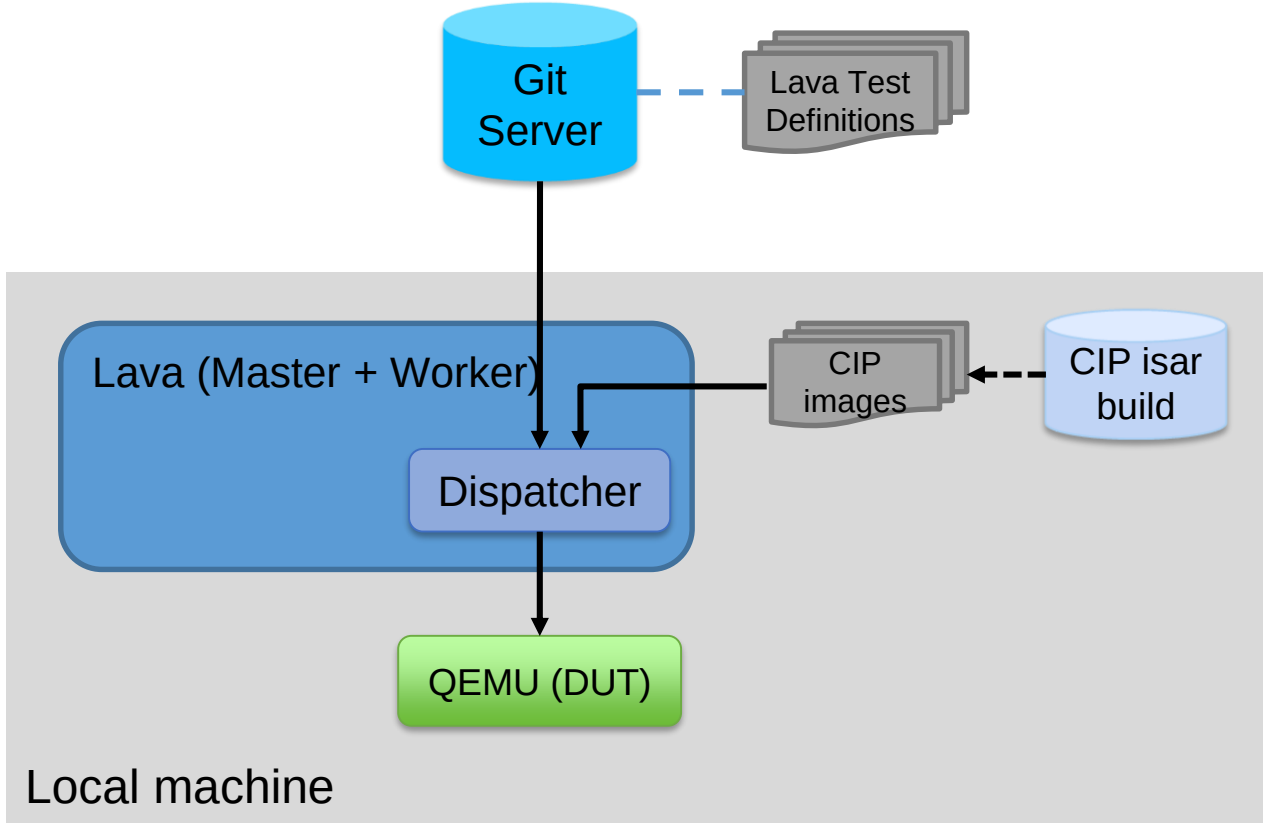
Reference https://gitlab.com/cip-project/cip-core/isar-cip-core/-/blob/security/iec-evaluation/SECURITY.md

CIVIL INFRASTRUCTURE PLATFORM

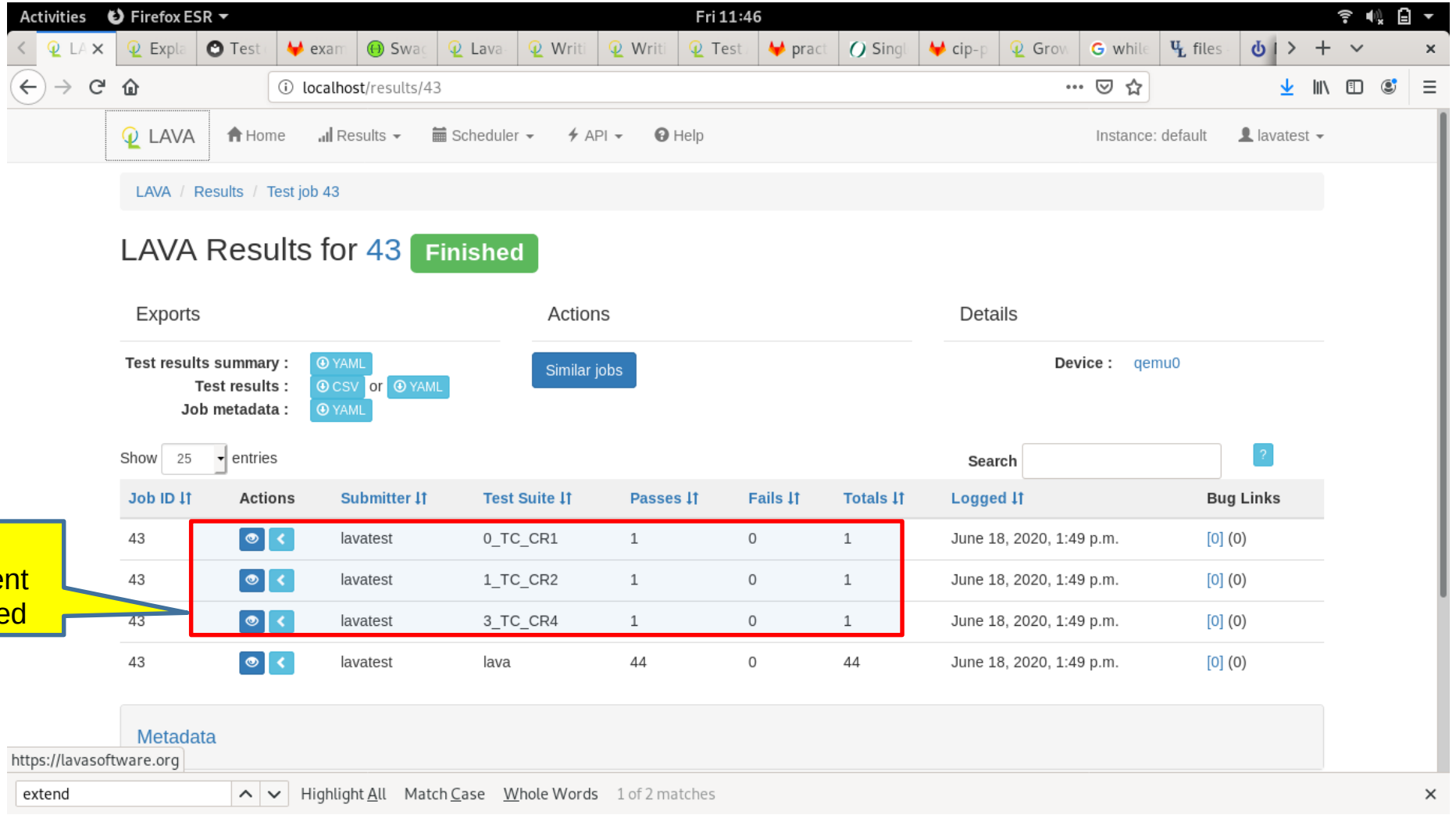
Running IEC security requirement tests in LAVA

This diagram shows current Lava setup in local machine for testing before final integrating with CIP LAVA test framework

- Lava master and worker is installed in local machine
- DUT images are build locally and accessible in local machine
- Lava test definitions are kept in gitlab server.



Viewing LAVA test results



3 under development tests passed

CIVIL INFRASTRUCTURE PLATFORM

CVEs tracking plan

- In order to meet some of the IEC-62443-4-1 requirements as mentioned below, CIP plans to use existing open source tools to automate CVEs monitoring

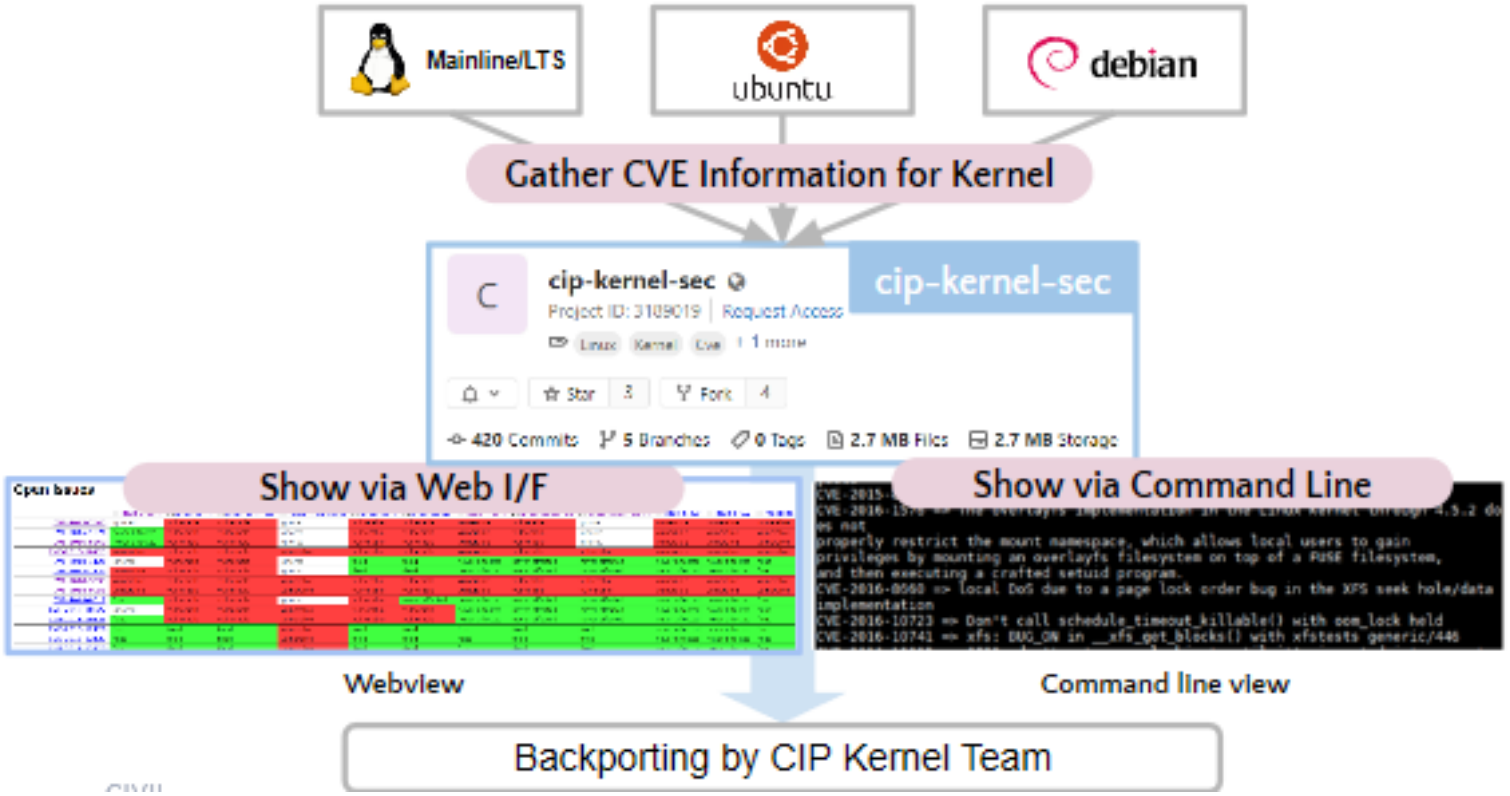
  “Before making product releases critical security fixes should be incorporated and made available to end user”

  “Receiving notifications for security related issues”

- The plan is to run vulnerability scanner such as ***cve-check-tool,*** **cvechecker, sw360 or “dependency track”** periodically on CIP packages and take appropriate actions such as applying upstream patches or backporting patches
- Investigations to finalize vulnerability scanner is in progress

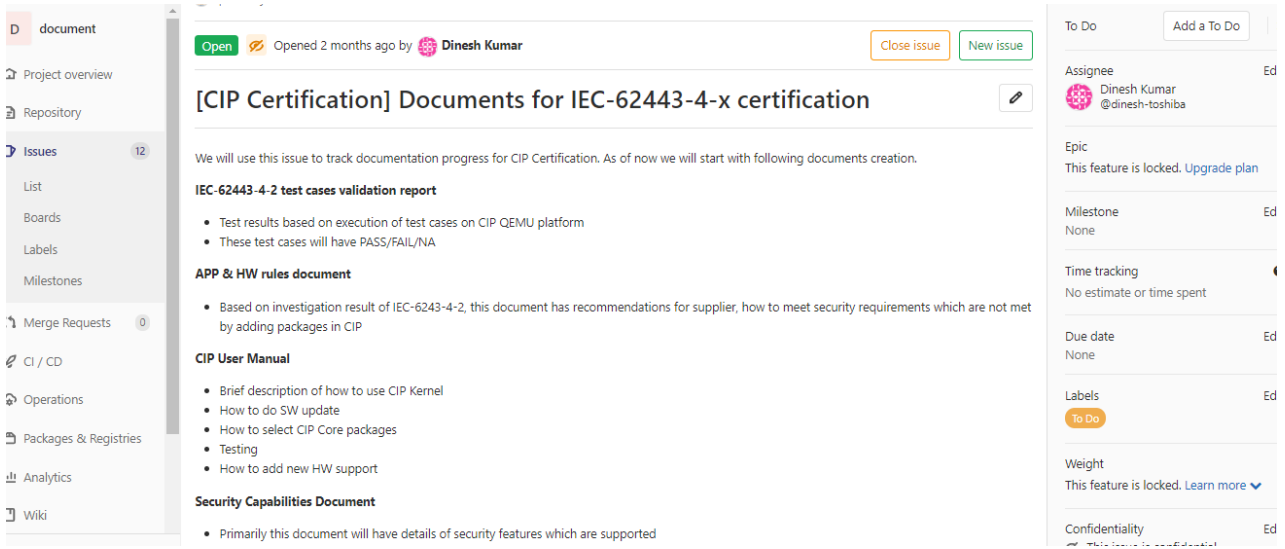
CVEs tracking in CIP kernel

- CIP Kernel team is already using **cip-kernel-sec** to track kernel CVEs



CIP IEC-62443-4-x assessment document management

- There are several requirements from CB for maintaining IEC assessment documents
  a. Maintain version of each document
  b. Restricted access of some documents such as secure design and IEC information documents
  c Versions could be compared
- Considering above points CIP has decided to maintain assessment documents
  a. Most of the documents should be created using Markdown to meet above requirements
  b. There will be two repositories, one public and another one private, private repository will have restricted access
- All documents will be maintained in CIP gitlab repositories
- Recently this document management approach has been approved by CIP TSC members



Advantages comparison CIP vs Non-CIP(OSS) distributions

Items	CIP	Non-CIP (OSS)
Dedicated kernel maintainers for SLTS up to 10 years	✓	✗
IEC-62443-4-x assessed platform	✓	✗
Close monitoring of CVEs at user and kernel level	✓	✗
Extended support from Debian ELTS for specific packages	✓	✗
Regular automated testing on multiple SOCs with published test results on KernelCI	✓	✗
Strong support from big players of embedded system industry	✓	✗

What's next from CIP security perspective

- Gap Assessment for compliance with IEC-62443-4-x
  - Finish Gap Assessment and work on gaps highlighted in assessment report
- Final CIP assessment for IEC-62443-4-1 & IEC-62443-4-2
  - Work with CB and initiate final CIP assessment for conformity with IEC-62443-4-1 & IEC-62443-4-2
- Publish Assessment reports, guidelines as well additional packages required to meet IEC-62443-4-x requirements
- Post assessment, document all the requirements of IEC-62443-4-2 which **need to be met by supplier**

References

- **To get the latest information, please contact:**
  - CIP Mailing List: cip-dev@lists.cip-project.org
- **Other resources**
  - Twitter: @cip_project
  - LinkedIn: Civil Infrastructure Platform
  - CIP Web Site: https://www.cip-project.org
  - **CIP Security**: https://wiki.linuxfoundation.org/civilinfrastructureplatform/cip-security
  - CIP News: https://www.cip-project.org/news/in-the-news
  - CIP Wiki: https://wiki.linuxfoundation.org/civilinfrastructureplatform/
  - CIP Source Code
    - CIP repositories hosted at kernel.org: https://git.kernel.org/pub/scm/linux/kernel/git/cip/
- CIP GitLab: https://gitlab.com/cip-project

CIVIL INFRASTRUCTURE PLATFORM

LINUX FOUNDATION
COLLABORATIVE PROJECTS

CIVIL
INFRASTRUCTURE
PLATFORM

Q&A section

LINUX FOUNDATION
COLLABORATIVE PROJECTS

CIVIL
INFRASTRUCTURE
PLATFORM

Thank You!

For attending CIP mini-summit OSSNA