The international effort to establish OSBL of cyber security for IACS

Kento Yoshida, Renesas Electronics Corporation, Security working group chair of the CIP project @OSS/ELC EU, Oct. 28, 2020
The CIP project and security working group
What is the “CIP” project

To establish a “base layer” of industrial-grade tooling using the Linux kernel and other open source projects
The key challenges

- Apply IoT concepts to industrial systems.
- Ensure quality and longevity of products.
- Keep millions of connected systems secure.

Industrial grade
- Reliability
- Functional Safety
- Real-time capabilities

Sustainability
- Product life-cycles of decades
- Backwards compatibility
- Standards

Security
- Security & vulnerability management
- Firmware updates
- Minimize risk of regressions
What is “OSBL”

- Industrial grade
- Sustainability
- Security

CIVIL INFRASTRUCTURE PLATFORM

open source base layer (OSBL)

company-specific middleware and applications

- additional packages (hundreds)

  - CIP Core packages (tens)

  - CIP kernel
    - (10+ years maintenance, based on LTS kernels)
Collaborative development with other OSS projects

Contribute, Collaborate and use by CIP

Upstream Projects
- Mainline
- LTS
- Debian
- LAVA
- Reproducible Builds
- Yocto
- Real-Time Linux
- KernelCI
- EDGE Foundry

Contribution by CIP members as future candidates
- Jailhouse
- Fuego
- HawkBit
- 360

1. Upstream first
2. Use the upstream code
3. Integrate

CIP Open Source Base Layer (OSBL)
Scope of activities
IEC 62443 certification
Growing threats of cyber-attacks

Targets have been changed to control systems
New shape of industry

Be standard, be open for cyber security in industry 4.0

Features:
- **Evolving continuously** without perfection
- Realize **new functions** by connecting
- Geographically **distributed**
The EU Cybersecurity Act was published on June 7, 2019. A new Era dawns on ENISA.

Framework for Improving Critical Infrastructure Cybersecurity version 1.1, issued April 16, 2018

Baseline for Classified Protection of Cybersecurity, GB/T 22239-2019, effective on December 1, 2019

IoT Security Guideline, issued July 2016
Why IEC 62443

IEC 62443 series are integrated cyber security standards
Linux is acting on many components for IACS

IEC 62443 Part 4

IEC 62443-4-1: secure product development lifecycle requirements

IEC 62443-4-2: technical security requirements for IACS components

Target devices, level: Embedded and network device, level-3
Structure for IEC 62443 certification

IEC 62443 certification program

- IEC
  - IECEE
    - Scheme owner
    - Member Bodies (MB)
      - Represents, only one MB per country
    - National Certification Bodies (NCB)
    - CB Testing Laboratories (CBTL)

ISASecure certification program

- ISA
- ISCI
  - Scheme owner
  - Accreditation bodies:
    - US
    - EU
    - APAC
      - ANAB
      - DAkkS
      - JAB
        - Exida
        - TÜV Rheinland
        - CSSC

Different for each certification program
Activity updates
Security working group’s mission and goal

Provide OSBL compliant with IEC 62443 certification

- Validated platform
- Guideline and evidence
- Compliant testing for evaluation

Development cost
Difficulty
Uncertainty
Completed the gap assessment for IEC 62443-4-1, and started the gap assessment for IEC 62443-4-2.
# Key challenges to meet IEC 62443-4-1 requirements

Needed special consideration caused not being a product

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

To achieve as much support as possible as a platform

<table>
<thead>
<tr>
<th>Development environment security</th>
<th>Following secure design principles</th>
<th>Defence in depth measures</th>
<th>Security implementation review</th>
<th>Defining Threat Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Re-use existing OSS infrastructure such as combination or private and public repos</td>
<td>• CIP plans to document how to protect open interfaces, restricted access based on roles</td>
<td>• The overall objective is to reduce attack surfaces</td>
<td>• CIP team reviews each security fix before applying to CIP</td>
<td>• It is planned to define a generic threat model to meet this requirement</td>
</tr>
<tr>
<td></td>
<td>• Exploit merge feature to control software modifications</td>
<td>• Few secure design principles depend upon type of product and it’s use cases</td>
<td>• Document general measures for defence in depth</td>
<td>• Plans to closely track CVEs of critical issues and regularly release security fixes</td>
</tr>
</tbody>
</table>
Preparing user friendly documents now

Documents compliant with IEC 62443-4-1

User Manual
- How to build CIP kernel and core packages
- Configuration

Security Capabilities
- List of all security packages to meet IEC 62443-4-2 security features requirements
- Details of security features which are supported by security packages

development process documents
- Version controlling
- Review policy/cycle
- Records

Can be reused by user certification
## Essential packages to meet IEC 62443-4-2

### Started the gap assessment of security packages

<table>
<thead>
<tr>
<th>FR</th>
<th>Description</th>
<th>Selected package examples:</th>
</tr>
</thead>
<tbody>
<tr>
<td>FR 1</td>
<td>Identification and authentication control (IAC)</td>
<td>shadow, pam, openssl, openssh, fail2ban</td>
</tr>
<tr>
<td>FR 2</td>
<td>Use control (UC)</td>
<td>acl, audit, syslog-ng, chrony</td>
</tr>
<tr>
<td>FR 3</td>
<td>System integrity (SI)</td>
<td>openssl, aide</td>
</tr>
<tr>
<td>FR 4</td>
<td>Data confidentiality (DC)</td>
<td>openssl, util-linux(ipcrm, ipcs), shred</td>
</tr>
<tr>
<td>FR 5</td>
<td>Restricted data flow (RDF)</td>
<td>-</td>
</tr>
<tr>
<td>FR 6</td>
<td>Timely response to events (TRE)</td>
<td>acl, audit, syslog-ng, bro</td>
</tr>
<tr>
<td>FR 7</td>
<td>Resource availability (RA)</td>
<td>nftables</td>
</tr>
</tbody>
</table>
Considering > Packaging > Testing

- CIP members
  - Discussion & Decide
  - Request Packages & Configurations

- CIP Core Packages
  - Build & Integrate

- Testing (CI)
  - Deploy
  - SLTS kernel
  - Real-Time

- CIP Reference Hardware
  - Tested on targets

- Security WG
  - Open Source Summit / Embedded Linux Conference Europe 2020
To close
The backbone of CIP are the member companies
Join us

CIP for sustainable Smart Cities with Open Source Software
Contact information and Resources

• To get latest information:
  • Contact to our mailing list: cip-dev@lists.cip-project.org

• Other resources:
  • Twitter: @cip_project
  • CIP Web Site: https://www.cip-project.org
  • CIP wiki: https://wiki.linuxfoundation.org/civilinfrastructureplatform/

• Upcoming session
  • CIP mini-summit, Friday, Oct. 30, 11:00 GMT: https://sched.co/eDiQ
Thanks you!