Activities of Super Long Term Support Kernel Workgroup in Civil Infrastructure Platform Project

Pavel Machek
CIP Kernel Maintainer, Denx

SZ Lin (林上智)
CIP Kernel Working Group Chairperson and TSC Representative, Moxa Inc.

ELCE 2019, France, 29th Oct.
About Us

• Pavel Machek <pavel@denx.de>
  • Cooperating with Denx
  • Kernel hacker
  • 4096R/92DFCE96
    • 4FA7 9EEF FCD4 C44F C585 B8C7 C060 2241 92DF CE96

• SZ Lin (林上智) <sz.lin@moxa.com>
  • Working for Moxa Inc.
  • Debian developer
  • Contribute to Linux and other OSS projects
  • 4096R/9561F3F9
    • 178F 8338 B314 01E3 04FC 44BA A959 B38A 9561 F3F9
Civil Infrastructure

https://www.airpano.com/360Degree-VirtualTour.php?3D=San-Francisco-USA
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
CIP is the Solution

- 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
CIP is the Solution

Establishes an “Open Source Base Layer (OSBL)”

CIP Core packages (tens)

CIP kernel (10+ years maintenance, based on LTS kernels)

additional packages (hundreds)

company-specific middleware and applications
The Scope of CIP

User space

Kernel space

On-device software stack

Product development and maintenance

Linux Kernel

1. Super Long Term Supported Kernel (STLS)

Middleware/Libraries

- Domain Specific communication (e.g. OPC UA)
- Safe & Secure Update
- Real-time support
- Monitoring

App container infrastructure (mid-term)

- Shared config.
- & logging

App Framework (optionally, mid-term)

- Multimedia

Tools

- Build environment (e.g. bitbake, dpkg)
- Test automation
- Tracing & reporting tools
- Configuration management
- Device management (update, download)
- Application life-cycle management

Concepts

- Functional safety architecture/strategy, including compliance w/ standards (e.g., NERC CIP, IEC61508)
- Long-term support
- Strategy: security patch management
- Standardization collaborative effort with others
- License clearing
- Export Control Classification

On-device software stack

Functional safety architecture/strategy, including compliance w/ standards (e.g., NERC CIP, IEC61508)

Long-term support

Strategy: security patch management

Standardization collaborative effort with others

License clearing

Export Control Classification

Build environment (e.g. bitbake, dpkg)

Test automation

Tracing & reporting tools

Configuration management

Device management (update, download)

Application life-cycle management

On-device software stack

Product development and maintenance

The Scope of CIP

Embedded Linux Conference Europe 2019
Super Long Term Support Kernel Workgroup

- The first action taken by the CIP project is to select and maintain Linux kernels for very long time (10+ years).
- Applying the PREEMPT_RT patch to CIP Kernel, then maintaining as CIP-RT.

<table>
<thead>
<tr>
<th></th>
<th>SLTS kernel</th>
<th>Real-time</th>
<th>Testing</th>
<th>CIP Core</th>
<th>Security WG(*)</th>
<th>Software update WG</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>2</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>3</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>4</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>5</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>6</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
</tbody>
</table>

(*): Workgroup

- Industrial grade ✔ ✔ ✔ ✔ ✔ ✔
- Sustainability ✔ ✔ ✔ ✔ ✔ ✔
- Security ✔ ✔ ✔ ✔ ✔ ✔

CIP Projects and its scopes
Policy and Progress
## Current LTS Versions (Retrieved 22\textsuperscript{nd}, Oct 2019)

<table>
<thead>
<tr>
<th>Version</th>
<th>Maintainer</th>
<th>Released</th>
<th>Projected EOL</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.4</td>
<td>Greg Kroah-Hartman &amp; Sasha Levin</td>
<td>2019-XX-XX</td>
<td>Dec, 2021</td>
</tr>
<tr>
<td>4.14</td>
<td>Greg Kroah-Hartman &amp; Sasha Levin</td>
<td>2017-11-12</td>
<td>Jan, 2024</td>
</tr>
<tr>
<td>4.9</td>
<td>Greg Kroah-Hartman &amp; Sasha Levin</td>
<td>2016-12-11</td>
<td>Jan, 2023</td>
</tr>
<tr>
<td>4.4</td>
<td>Greg Kroah-Hartman &amp; Sasha Levin</td>
<td>2016-01-10</td>
<td>Feb, 2022</td>
</tr>
<tr>
<td>3.16</td>
<td>Ben Hutchings</td>
<td>2014-08-03</td>
<td>Apr, 2020</td>
</tr>
</tbody>
</table>
CIP SLTS Kernel Development (Upstream First Development)

- **Goal**
  - Providing CIP kernels with more than 10 years maintenance period
    - **Super Long Time Stable kernel**

- **Status**
  - LTS review process participation
  - CIP SLTS kernels release
    - 4.4.196-cip38
    - 4.19.78-cip12
  - CIP kernel CVE tracker
  - CIP kernel failed patches tracker
Introduction to CIP Kernel Team Member

• **Chairperson**
  • SZ Lin (林上智)

• **Maintainer**
  • Nobuhiro Iwamatsu
  • Pavel Machek

• **Mentor**
  • Ben Hutchings
# Current SLTS Versions (Retrieved 22\textsuperscript{nd}, Oct 2019)

<table>
<thead>
<tr>
<th>Version</th>
<th>Maintainer</th>
<th>First Release</th>
<th>Latest Release</th>
<th>Projected EOL</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.4</td>
<td>Nobuhiro Iwamatsu &amp; Pavel Machek</td>
<td>2017-01-17&lt;br&gt;• v4.4.42-cip1</td>
<td>2019-10-12&lt;br&gt;• v4.4.196-cip38</td>
<td>2027+</td>
</tr>
<tr>
<td>4.4-r</td>
<td>Pavel Machek</td>
<td>2017-11-16&lt;br&gt;• v4.4.75-cip6-rt1</td>
<td>2019-10-02&lt;br&gt;• v4.4.190-cip36-rt25</td>
<td>2027+</td>
</tr>
</tbody>
</table>
CIP SLTS Kernel Development

Maintenance Policy
• https://wiki.linuxfoundation.org/civilinfrastructureplatform/cipkernelmaintenance
• Follow the stable kernel development rule as the basis
• Validation will be done by CIP test infrastructure and/or members
• Feature backports from CIP members are acceptable
  • All features has to be in upstream kernel before backport to CIP kernel
  • CIP has “Upstream first” policy
• The CIP Project uses the Linux Foundation Developer Certificate of Origin (DCO)
Out-of-tree drivers

• In general, all out-of-tree drivers are unsupported by CIP

• Users can use CIP kernel with out-of-tree drivers
  • If a bug is found in such a modified kernel, users will first demonstrate that it exists in the CIP kernel source release in order for the CIP maintainers to act on it.
CIP SLTS Kernel Development

Backported patches

Mainline

4.4

4.19

Stable 4.4.y

EOL

Feature backports

Stable 4.19.y

EOL

CIP SLTS (linux-4.4.y-cip)

CIP SLTS (linux-4.19.y-cip)

Maintained by Iwamatsu and Pavel
The Sources of CIP Patches

CIP patches

- Stable patches
  - Security issue
  - Bug fixes

- Backported patches
  - Security issue
  - Bug fixes
  - Feature backports

cip-dev@lists.cip-project.org
Patches Review
Stable Patches Review Participation

Stable patches

Review Stable Patches

# Stable Kernel Patches Review Status
Please list your name and review result below the patch item

* UR: Under Review
* ACK: Acknowledge (if the patch is accepted)
* TBB: To be backported (if other patches should be also backported)
* NAK: Negative acknowledge (if the patch is rejected, please list the reason)
* IGN: Patch was not reviewed as it is out of scope for CIP project
Stable Patches Review Participation

Kernel 4.4

```
## v4.4.196
- c61ebb668f2c Linux 4.4.196

ACK: iwamatsu

- 2e486758901d NFC: fix attrs checks in netlink interface

ACK: iwamatsu

- ac375073bb39 smack: use GFP_NOFS while holding inode_smack::smk_lock
```

Kernel 4.19

```
## v4.19.77
- 6cad9d0 Linux 4.19.77
- 2c60da9 drm/amd/display: Restore backlight brightness after system resume

ACK: Pavel

- 4dbdf7 mm/compaction.c: clear total (migrate,free) scanned before scanning a new zone

ACK: Pavel

- 5bad6f6 fuse: fix deadlock with aio poll and fuse_iqueue::waitq.lock

UR: Pavel -- bad according to Eric Biggers

- bbe3e20 md/raid0: avoid RAID0 data corruption due to layout confusion.

UR: Pavel -- should this be per-array not per-module?

- 4290a9e CIFS: Fix oplock handling for SMB 2.1+ protocols

ACK: Pavel

- a3a1508 CIFS: Fix max ea value size
```
Stable Patches Review Participation

Reviewed by Pavel for 4.19-stable

```c
--- a/drivers/infiniband/core/restrack.c
+++ b/drivers/infiniband/core/restrack.c
@@ -209,7 +209,7 @@ void rdma_restrack_del(struct rdma_restr
 struct ib_device *dev;
>
> if (!res_valid)
- >     return;
+ >     goto out;
> >
> dev = res_to_dev(res);
> if (!dev)
+ #     return;
>     goto out;

This test does return, does it need to go through `goto out`, too? (I see it should not happen, but...)

```c
@@ -222,8 +222,10 @@ void rdma_restrack_del(struct rdma_restr
 down_write(&dev->res.rwsem);
 hash_del(&res->node);
 res->valid = false;
+ > > up_write(&dev->res.rwsem);
+ > +out:
+ > if (res->task)
+ >     put_task_struct(res->task);
- > - up_write(&dev->res.rwsem);
> }
```

Mainline says res->task = NULL is needed there, see fe9bc1644918a1d.

Best regards,

Pavel
Difference Between -stable Kernel Rules and Rules Imposed in Practice

a) It or an equivalent fix must already exist in Linus' tree (upstream).
Enforced. Strong preference is given to merging exactly the same patch as in upstream.

b) It must be obviously correct and tested.
Preference is given to a): buggy patch is merged, then fix is merged as followup.

c) It must fix a real bug that bothers people (not a, "This could be a problem..." type thing).
Anything that looks like a bugfix is merged, includes trivial memory leaks that leak few bytes per boot and missing of_node_put().

d) It must fix a problem that causes a build error (...), an oops, a hang, data corruption, a real security issue, or some "oh, that's not good" issue. In short, something critical.
Build-time warnings, run-time warnings, confusing printk messages and loglevel changes for printk messages are applied.

e) It cannot contain any "trivial" fixes in it (spelling changes, whitespace cleanups, etc).
Certainly not enforced. There is preference to taking patches from mainline with no changes.
CIP Kernel Team Contribution to Upstream Statistics (Retrieved 25th, Oct 2019)

Embedded Linux Conference Europe 2019
CIP Members Patches Review Participation

Review CIP Member Patches

Kernel 4.4

[cip-dev] [PATCH 4.4-cip] ARM: dts: socfpga: Rename socfpga_cyclone5_de0_{sockit, nano_soc}  Jan Kiszka
[cip-dev] [PATCH 4.4-cip] ARM: dts: socfpga: Rename socfpga_cyclone5_de0_{sockit, nano_soc}  Nobuhiro Iwamatsu

Kernel 4.19

[cip-dev] [PATCH 4.19.y-cip 0/4] Add USB support  Biju Das
[cip-dev] [PATCH 4.19.y-cip 0/4] Add USB support  Pavel Machek
[cip-dev] [PATCH 4.19.y-cip 0/4] Add USB support  Pavel Machek
Feature Backported Patches Statistics in CIP Kernel

- CIP kernel 4.4: 617 patch commits
- CIP kernel 4.19: 436 patch commits
CIP SLTS Real-time Support

CIP SLTS+PREEMPT_RT (will be separately maintained by CIP members)
• CIP kernel tree based on linux-stable-rt and patches from CIP SLTS
• Validation will be done by CIP
CIP SLTS Real-time Support

• CIP has become a Gold Member of the Real Time Linux Project

• What’s next
  • Work together with the RTL Project

• More information
  • https://wiki.linuxfoundation.org/realtime/rtl/start
## CIP SLTS Kernel Release Policy

<table>
<thead>
<tr>
<th>Release regularly</th>
<th>Release on demand</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release <strong>4.19 twice a month</strong> and <strong>4.4 once a month</strong> (Effective June, 2019)</td>
<td>It depends on critical bug/ security fix</td>
</tr>
<tr>
<td>• Kernel 4.19</td>
<td></td>
</tr>
<tr>
<td>• second and fourth Fridays of the month</td>
<td></td>
</tr>
<tr>
<td>• Kernel 4.4</td>
<td></td>
</tr>
<tr>
<td>• second Friday of the month</td>
<td></td>
</tr>
<tr>
<td>Release <strong>4.19-rt twice a month</strong> and <strong>4.4-rt once every two months</strong> (Effective Nov, 2019)</td>
<td>Ditto</td>
</tr>
</tbody>
</table>

**Note:** Difficult to estimate actual release date because of number of patches depends on each stable release
CIP Kernel and Real-time Kernel Release Statistics

- v4.4-cip
- v4.4-cip-rt
- v4.19-cip
- v4.19-cip-rt

![Bar Chart]

- 2017: v4.4-cip (15), v4.4-cip-rt (3), v4.19-cip (0), v4.19-cip-rt (0)
- 2018: v4.4-cip (14), v4.4-cip-rt (0), v4.19-cip (0), v4.19-cip-rt (0)
- Total (Retrieved 27th, Oct): v4.4-cip (38), v4.4-cip-rt (25), v4.19-cip (12), v4.19-cip-rt (3)
- Total estimated in 2019: v4.4-cip (42), v4.4-cip-rt (26), v4.19-cip (16), v4.19-cip-rt (5)
Introduction to "cip-kernel-sec"

- This project tracks the status of security issues, identified by CVE ID, in mainline, stable, and other configured branches.
The Maintenance Scope of "cip-kernel-sec" – “cip-kernel-config”

• The security issues are determined to be fixed base on kernel configurations provided by CIP members
CVE Issue Format - Supported by CIP

Issue Format - YAML
CVE Issue Format – Unsupported by CIP

description: 'IB/mlx5: Fix leaking stack memory to userspace'
references:
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-20855
- https://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=0625b4ba1a5d4703c7fb01c497bd6c156908af00
- https://github.com/torvalds/linux/commit/0625b4ba1a5d4703c7fb01c497bd6c156908af00
comments:
    Debian-bwh: |
        Introduced in Linux 4.17 by commit 41d902cb7c32 "RDMA/mlx5: Fix
definition of mlx5_ib_create_qp_resp".
introduced-by:
    mainline: [41d902cb7c326d711674977763c4b30df87611bc]
fixed-by:
    mainline: [0625b4ba1a5d4703c7f001c497bd6c156908af00]
ignore:
    linux-4.19.y-cip: No member enables the mlx5_ib driver
    linux-4.19.y-cip-rt: No member enables the mlx5_ib driver
    linux-4.4.y-cip: No member enables the mlx5_ib driver
    linux-4.4.y-cip-rt: No member enables the mlx5_ib driver
Introduction to "classify-failed-patches"

• This project tracks the status of failed patches, and classifies patches into “applied” and “ToApply” types.
Introduction to "classify-failed-patches"

Applied patches

```
[APPLIED] arm64: Disable unhandled signal log messages by default
56b57bd26b5b0d353ae7f7b7c41ee18ffed963 arm64: Disable unhandled signal log messages by default

[APPLIED] ARC: hide unused function umx_hdr_alloc
4d28512bf54e4566bf65e800c003c6f81040b0 ARC: hide unused function umx_hdr_alloc

[APPLIED] btrfs: Ensure replaced device doesn't have pending chunk allocation
986543fcf50c8a3e681be44ac42dc498fe25ab34 btrfs: Ensure replaced device doesn't have pending chunk allocation
[APPLIED] btrfs: Ensure replaced device doesn't have pending chunk allocation
986543fcf50c8a3e681be44ac42dc498fe25ab34 btrfs: Ensure replaced device doesn't have pending chunk allocation
[APPLIED] btrfs: Ensure replaced device doesn't have pending chunk allocation
986543fcf50c8a3e681be44ac42dc498fe25ab34 btrfs: Ensure replaced device doesn't have pending chunk allocation
[APPLIED] btrfs: Ensure replaced device doesn't have pending chunk allocation
986543fcf50c8a3e681be44ac42dc498fe25ab34 btrfs: Ensure replaced device doesn't have pending chunk allocation
```

To be Applied Patches

```
[TOAPPLY] inet: update the IP ID generation algorithm to patch 355b98553780b646ed97ad801a619ff898471b92 standards.

[TOAPPLY] scsi: ufs: Fix RX_TERMINATION_FORCE_ENABLE define value

[TOAPPLY] inet: update the IP ID generation algorithm to patch 355b98553780b646ed97ad801a619ff898471b92 standards.

[TOAPPLY] ib/hfil: Failed to drain send queue when QP is put into error state

[TOAPPLY] arm64: mm: Ensure tail of unaligned instr is reserved

[TOAPPLY] fs/proc/task_mmu.c: fix uninitialized variable warning

[TOAPPLY] tpm: Fix the type of the return value in calc_tpm2_event_size()

[TOAPPLY] block: bio_map_user_iov should not be limited to BIO_MAX_PAGES

[TOAPPLY] clk: ingenic/jz4725bs: Fix parent of pixel clock

[TOAPPLY] iucv:pixd: Add Hygon Dhyana SMBus support

[TOAPPLY] ity: serial_core, add -install
```
Testing
CIP Testing Talk at CIP Mini Summit

• Thursday in CIP Mini Summit
  • 8:00 – 13:00 @ Lyon Convention Centre

Testing Architecture Overview

- **lava-docker**
  - LAVA Master Scheduler
  - LAVA Worker Platform manager
  - LAVA Worker Platform manager

- **gitlab-cloud-ci**
  - AWS EC2
  - Kubernetes pods

- **linux-cip-ci**
  - GitLab CI/CD Pipeline manager

- **AWS S3**
  - Artifact storage

- **Reference Platforms**

Embedded Linux Conference Europe 2019 37
**Summary**

- **Routine tasks**
  - The frequency of CIP kernel release
    - The kernel of
      - 4.4 will be released at least once and 4.19 will be released at least twice every month
      - 4.4-rt will be released at least once every two months and 4.19-rt will be released at least twice a month
  - Failed patch tracker
  - Linux kernel CVE tracker

- **Occasional tasks**
  - Build up kernel and rt-kernel testing
  - Define and update the wiki for kernel maintenance scope
Weekly Regular Online Meeting

• CIP IRC weekly meeting – Every Thursday UTC (GMT) 09:00

<table>
<thead>
<tr>
<th>US-West</th>
<th>US-East</th>
<th>UK</th>
<th>DE</th>
<th>TW</th>
<th>JP</th>
</tr>
</thead>
<tbody>
<tr>
<td>02:00</td>
<td>05:00</td>
<td>09:00</td>
<td>10:00</td>
<td>17:00</td>
<td>18:00</td>
</tr>
</tbody>
</table>

• Channel:
  * irc:chat.freenode.net:6667/cip

• The meeting will take 30 min although it can be extended to an hour if it makes sense and those involved in the topics can stay. Otherwise, the topic will be taken offline or in the next meeting.
CIP Kernel Workgroup Repository

• CIP Linux kernel & real-time kernel
  • https://git.kernel.org/pub/scm/linux/kernel/git/cip/linux-cip.git

• CIP Linux kernel CVE tracker
  • https://gitlab.com/cip-project/cip-kernel/cip-kernel-sec

• CIP Linux kernel failed patches tracker
  • https://gitlab.com/cip-project/cip-kernel/classify-failed-patches
Contact Information and Resources

To get the latest information, please contact:

• CIP Mailing List: cip-dev@lists.cip-project.org

Other resources

• Twitter: @cip_project
• CIP Web Site: https://www.cip-project.org
• 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
CIP Talks at ELCE, CIP Mini Summit, and ATS

• Today (ELCE)
  • 15:15 @ Tête d'Or 2 (CIP)
    Open Source Projects to Live long and Prosper: Linux for Smart Infrastructure and Industry - Yoshitake Kobayashi, Toshiba Corporation & Urs Gleim, Siemens AG

• Thursday in CIP Mini Summit
  • 8:00 – 13:00 @ Lyon Convention Centre
    • https://www.cvent.com/Events/Register/RegNumConfirmation.aspx?e=66d78d44-9d3c-4c92-85fa-a87ef8e8b62b&_ga=2.224040339.985516515.1571730868-505872952.1553045385

• Thursday in Automated Testing Summit (ATS)
  • 15:10 @ Rhone 3AB (CIP Testing)
    A Guide to CIP Testing - Chris Paterson, Renesas Electronics Europe & Michael Adler, Siemens AG
Please Visit CIP Booth!

Place: FORUM 4/5 Sponsor Showcase

“CIP mini-summit” will be held on Oct. 31th (Thu), but sold out already, thank you!
Join us

CIP for sustainable Smart Cities with Open Source Software
Question?
Thank you
References

• How to make Smart Cities stay smart with Open Source Projects, OSS-J 2019, Yoshitake Kobayashi

• The Activity of the Security Working Group in the CIP Project, OSS-J 2019, Takehisa Katayama

• Debian and Yocto Project based Long-term Maintenance Approaches for Embedded Products, ELCE 2019, Jan Kiszka and Kazuhiro Hayashi