#

CIP File Integrity

Table of contents

Revision History

Revision No	Date	Change description	Author	Reviewed by
001	2021-09-03	Draft file integrity document	Venkat P	To be reviewed by CIP Security WG members
002	2021-11-25	Added TODO reference	Yasin U	Reviewed by CIP Security WG

---

1. Objective

The primary objective of this document is to explain about how file integrity for CIP deliverables is achieved.

2. Scope

Scope of this document is to meet IEC-62443-4-1 SM-6 (File Integrity) security requirement. This document will explain about how file integrity of CIP deliverables can be verified by CIP users.

As currently primary deliverable of CIP is reference source code and meta data maintained in various gitlab repositeries, this document covers about the same.

3. File Integrity of Source Code

CIP users can use gitlab tool called git-fsck for verifying integrity of CIP source code, script, meta data after downloading locally to ensure the artifacts downloaded are same as in gitlab repo.

git-fsck is git feature to verifiy the connectivity and validity of the source code objects that may be corrupted during download or usage.

Following steps can be followed to confirm integrity of source code, scripts, meta data. this example is considering isa-cip-core gitlab repo, similar steps would work with any other gitlab repo.

```
$ git clone https://gitlab.com/cip-project/cip-core/isar-cip-core.git
$ cd isar-cip-core
$ git fsck –full
```

If it doesn't print any warnings then there is no corruption or integrity issues in the downloaded source code.

4. File Integrity of Images

CIP members plan to release evaluation images in future which would be available for some of the CIP supported reference hardwares.

This section would be updated once CIP evaluation images are available to download.

5. References

1. More about git-fsck https://git-scm.com/docs/git-fsck
2. Future TODOs https://gitlab.com/cip-project/cip-security/iec_62443-4-x/-/issues/27