National Security Agency
Cybersecurity Technical Report

DoD Microelectronics: Field Programmable Gate Array Level of Assurance Quick Start Guide

October 2023

U/OO/208512-23
PP-23-3453
Version 1.0

This cybersecurity technical report (CTR) was created in collaboration with the JFAC Hardware Assurance labs:

- National Security Agency
- Air Force Research Lab (AFRL) RYDT
- Naval Surface Warface Center (NSWC) Crane
- Army Development Command (DEVCOM)/AVMC

For additional information, guidance, or assistance with this document, please contact the Joint Federated Assurance Center (JFAC) at JFAC_HWA@radium.nscs.mil.

Notices and history

Document change history

Date	Version	Description
October 2023	1.0	Initial Publication

Disclaimer of warranties and endorsement

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.

Publication information

Author(s)

National Security Agency
Cybersecurity Directorate
Joint Federated Assurance Center

Contact information

Joint Federated Assurance Center: JFAC_HWA@radium.ncsc.mil
Cybersecurity Report Feedback / General Cybersecurity Inquiries: CybersecurityReports@nsa.gov
Defense Industrial Base Inquiries and Cybersecurity Services: DIB_Defense@cyber.nsa.gov
Media inquiries / Press Desk: Media Relations, 443-634-0721: MediaRelations@nsa.gov

Purpose

This document was developed in furtherance of NSA's cybersecurity missions. This includes its responsibilities to identify and disseminate threats to National Security Systems, Department of Defense information systems, and the Defense Industrial Base, and to develop and issue cybersecurity specifications and mitigations. This information may be shared broadly to reach all appropriate stakeholders.

Contents

Tables

Quick start guide purpose

This quick start guide for the NSA Field Programmable Gate Array (FPGA) Levels of Assurance (LoA) guidance provides users with an outline of how to apply the LoA Best Practice Guides to their programs. While comprised of nine documents in total, the LoA series does not require all the volumes for its application. Users need only read and apply the guidance found in, at most, two documents. Other documents in the series address the methods used to develop the guidance, advice on how to replicate this process for other types of microelectronic devices, and include definitions. Users only need to concern themselves with:

- The appropriate level best practice guide
- The accompanying third-party intellectual property (IP) review guide

The following table lists the nine LoA documents and their purposes:

Table 1: Level of Assurance best practice guidance Documents

Document	Purpose
DoD Microelectronics: Field Programmable Gate Array Overall Assurance Process	Background
DoD Microelectronics: Levels of Assurance Definitions and Applications	Background
DoD Microelectronics: Field Programmable Gate Array Best Practices – Threat Catalog	Background
DoD Microelectronics: Field Programmable Gate Array Level of Assurance 1 Best Practices	**Guidance LoA1**
DoD Microelectronics: Third-Party IP Review Process for Level of Assurance 1	**Guidance LoA1**
DoD Microelectronics: Field Programmable Gate Array Level of Assurance 2 Best Practices	**Guidance LoA2**
DoD Microelectronics: Third-Party IP Review Process for Level of Assurance 2	**Guidance LoA2**
DoD Microelectronics: Field Programmable Gate Array Level of Assurance 3 Best Practices	**Guidance LoA3**
DoD Microelectronics: Third-Party IP Review Process for Level of Assurance 3	**Guidance LoA3**

Quick start steps

Overview

The application of the LoA guidance consists of the following four simple steps:

1. Determine the appropriate level of assurance for the top-level system.
2. Determine the appropriate level of assurance for the FPGA device(s).
3. Select the appropriate best practice guide.
4. Apply the guidance.

1. Determine the appropriate LoA for the top-level system

The first step in applying the LoA guidance identifies the appropriate LoA for the top-level system in which the FPGA will operate, a determination made by the program based on the potential national-level impact caused by the failure or subversion of the top-level system. This determines the highest possible level of assurance for the FPGA device.

The FPGA device should not be protected at a level higher than the system in which it operates. A U.S. Government (USG) person with authority over the program should select the appropriate LoA for the overall program using the criteria in the following table:

Table 2: Top-level system LoA criteria as determined by national impact

Level of Assurance	Typical Criteria
	If the system fails, USG capability will be reduced in a meaningful way. If the system is subverted, it can cause harm to U.S. personnel, property, or interests. However: • Essential operational capabilities for the DoD will remain available even during a system failure.
	If the system fails, the consequences will be grave. If the system is subverted, it can cause serious harm to U.S. personnel, property, or interests. However: • Essential operational capabilities for the DoD may be degraded during a system failure, and

Level of Assurance	Typical Criteria
	• Redundant capabilities can be brought online as part of a continuity of operations plan, and • The failure of the system will not cause cascade effects across many DoD or allied systems.
	If the system fails, the consequences will be extremely grave. If the system is subverted, it can cause exceptionally grave harm to U.S. personnel, property, or interests. A failure or subversion of this system: • May represent an existential risk to the USG, and • May cascade across many DoD systems in a way that impacts total operational readiness in an immediate way, and • Will interrupt essential operational capabilities of the DoD.

Select the top-level LoA. This now represents the highest level at which the FPGA device can be protected.

2. Determine the appropriate LoA for the FPGA device(s)

The second step determines the appropriate LoA for each FPGA device in the sub-system. The device LoA is based upon the device's criticality to the system in which it operates. This criticality is determined during the program's Trusted Systems and Networks (TSN) analysis required by the Program Protection Plan. The program's TSN analysis determines the assignment of a level of criticality commensurate with the consequence to the sub-system of the component's failure. The following table lists the TSN levels of criticality and the corresponding LoAs:

Table 3: TSN criticality and corresponding Levels of Assurance

TSN Criticality	Description	LoA Mapping
Level I: Total Mission Failure	Failure that results in total compromise of mission capability	LoA3

TSN Criticality	Description	LoA Mapping
Level II: Significant / Unacceptable Degradation	Failure that results in unacceptable compromise of mission capability or significant mission degradation	LoA2
Level III: Partial / Acceptable	Failure that results in partial compromise of a mission capability or partial mission degradation	LoA1
Level IV: Negligible	Failure that results in little or no compromise of mission capability	N/A; Although LoA1 mitigations are recommended

Although components can receive a lower LoA than the system, a component cannot receive a higher LoA than the system. For example, an LoA1 system cannot require LoA3 components.

Program analysts can refer to the following table to determine the appropriate LoA for a given component having determined the TSN criticality level.

Table 4: Mapping critical components to Levels of Assurance

System LoA	TSN Criticality of Component to the System			
	Negligible	Partial / Acceptable	Significant / Unacceptable	Total Mission Failure
LoA 1	N/A	LoA 1	LoA 1	LoA 1
LoA 2	LoA 1	LoA 1	LoA 2	LoA 2
LoA 3	LoA 1	LoA 2	LoA 3	LoA 3

Determine the LoA for each FPGA device in the sub-system.

3. Select the appropriate best practice guide

After identifying the device LoA, the user can download the appropriate best practice guide and its accompanying IP review guide from the NSA website, https://www.nsa.gov/Press-Room/DoD-Microelectronics-Guidance/. Each best practice guide is complete and does not require information or support of the lower-level guides. That is, for LoA3, the user does not also need LoA2 and LoA1 documents.

4. Apply the guidance

Each best practice guide contains all the guidance necessary to mitigate threats at the intended level. In addition to the mitigation details, the documents include a checklist that users can use to track the chosen options, a glossary, and contact information for help or questions.