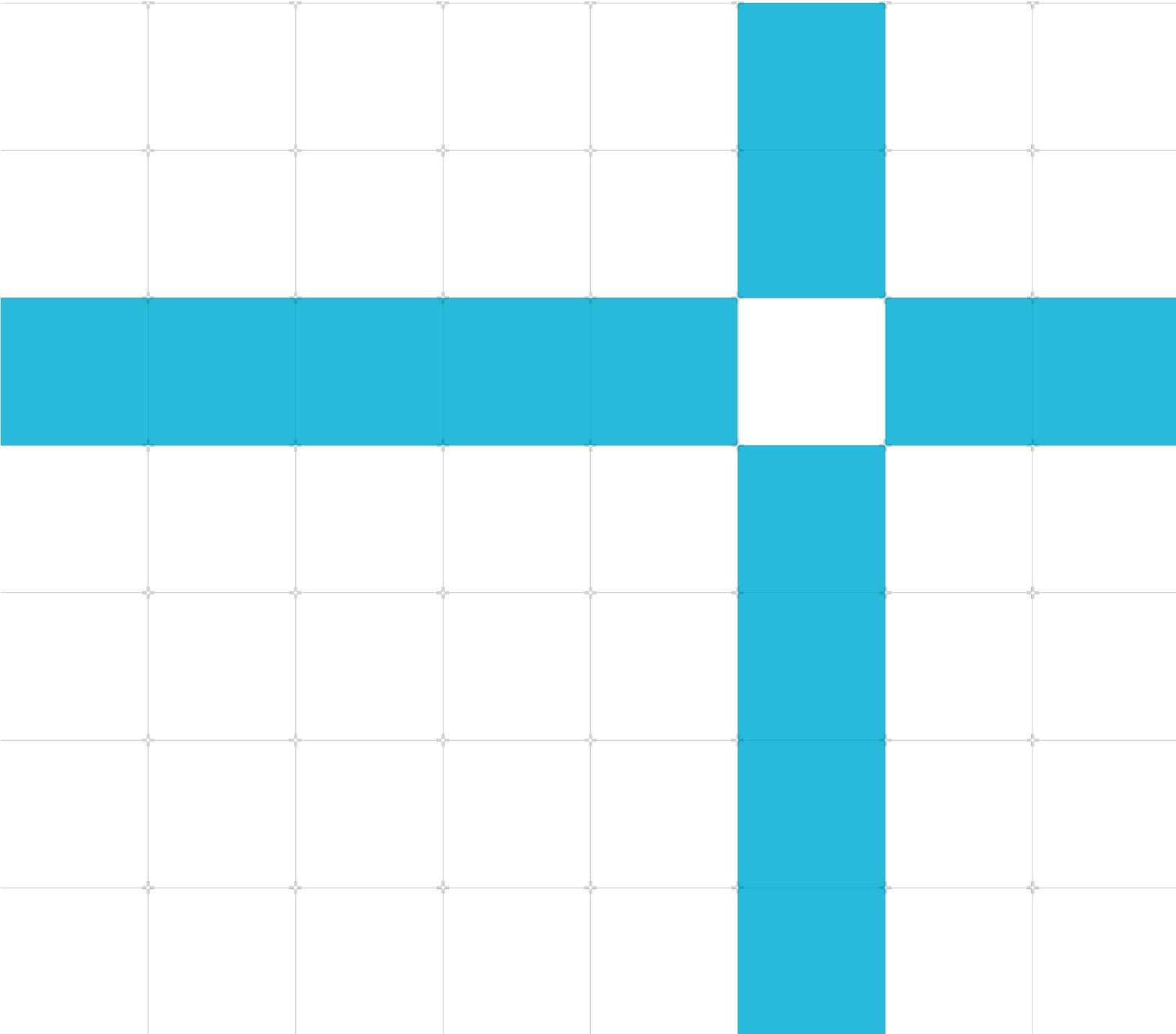




# Before debugging on Armv8-A

[Non-Confidential]  
Copyright ©[2019 Arm Limited (or its affiliates).  
All rights reserved.



## Before debugging on Armv8-A

Copyright © 2019 Arm Limited (or its affiliates). All rights reserved.

Release information

Document history

Issue	Date	Confidentiality	Change
01			

## Non-Confidential Proprietary Notice

This document is protected by copyright and other related rights and the practice or implementation of the information contained in this document may be protected by one or more patents or pending patent applications. No part of this document may be reproduced in any form by any means without the express prior written permission of Arm. No license, express or implied, by estoppel or otherwise to any intellectual property rights is granted by this document unless specifically stated.

Your access to the information in this document is conditional upon your acceptance that you will not use or permit others to use the information for the purposes of determining whether implementations infringe any third party patents.

THIS DOCUMENT IS PROVIDED "AS IS". ARM PROVIDES NO REPRESENTATIONS AND NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, NON-INFRINGEMENT OR FITNESS FOR A PARTICULAR PURPOSE WITH RESPECT TO THE DOCUMENT. For the avoidance of doubt, Arm makes no representation with respect to, and has undertaken no analysis to identify or understand the scope and content of, patents, copyrights, trade secrets, or other rights.

This document may include technical inaccuracies or typographical errors.

TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT WILL ARM BE LIABLE FOR ANY DAMAGES, INCLUDING WITHOUT LIMITATION ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES, HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF ANY USE OF THIS DOCUMENT, EVEN IF ARM HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

This document consists solely of commercial items. You shall be responsible for ensuring that any use, duplication or disclosure of this document complies fully with any relevant export laws and regulations to assure that this document or any portion thereof is not exported, directly or indirectly, in violation of such export laws. Use of the word "partner" in reference to Arm's customers is not intended to create or refer to any partnership relationship with any other company. Arm may make changes to this document at any time and without notice.

If any of the provisions contained in these terms conflict with any of the provisions of any click through or signed written agreement covering this document with Arm, then the click through or signed written agreement prevails over and supersedes the conflicting provisions of these terms. This document may be translated into other languages for convenience, and you agree that if there is any conflict between the English version of this document and any translation, the terms of the English version of the Agreement shall prevail.

The Arm corporate logo and words marked with ® or ™ are registered trademarks or trademarks of Arm Limited (or its affiliates) in the US and/or elsewhere. All rights reserved. Other brands and names mentioned in this document may be the trademarks of their respective owners. Please follow Arm's trademark usage guidelines at <http://www.arm.com/company/policies/trademarks>.

Copyright © [2019 Arm Limited (or its affiliates). All rights reserved.

Copyright © 2019 Arm Limited (or its affiliates). All rights reserved.

[Non-Confidential]

Arm Limited. Company 02557590 registered in England.

110 Fulbourn Road, Cambridge, England CB1 9NJ.

(LES-PRE-20349)

## Confidentiality Status

This document is Non-Confidential. The right to use, copy and disclose this document may be subject to license restrictions in accordance with the terms of the agreement entered into by Arm and the party that Arm delivered this document to.

Unrestricted Access is an Arm internal classification.

## Web Address

[www.arm.com](http://www.arm.com)

# Contents

<b>1 Overview</b> .....	<b>5</b>
1.1 Before you begin .....	5
<b>2 Different types of debug</b> .....	<b>6</b>
2.1 External debug.....	6
2.2 Self-hosted debug.....	6
2.3 Invasive debug .....	7
2.4 Non-invasive debug.....	7
<b>3 Target types</b> .....	<b>9</b>
<b>4 Program being debugged</b> .....	<b>10</b>
<b>5 Target state</b> .....	<b>12</b>
5.1 Core or processor is powered down.....	12
5.2 Core or processor is held in reset .....	12
5.3 Core or processor is in a different security state .....	12
5.4 Core or processor is in a different Exception level.....	13
<b>6 Initializing a target</b> .....	<b>15</b>
6.1 Powering up or taking a core or processor out of reset.....	15
6.2 Unlocking scan chains or devices .....	15
6.3 Multiplexed signals .....	15
6.4 Missing connectors .....	16
<b>7 Check your knowledge</b> .....	<b>17</b>
<b>8 Related information</b> .....	<b>18</b>
<b>9 Next steps</b> .....	<b>19</b>

# 1 Overview

This guide describes concepts that are useful to know before debugging an Armv8-A processor. To illustrate these concepts, we mention debuggers, for example GDB and the Arm Debugger, which is part of Arm Development Studio.

At the end of this guide, you should be able to:

- Understand the differences between external, self-hosted, invasive, and non-invasive debug.
- Apply the correct target and application considerations when working with a debugger.
- Understand the state of the target when it is connecting to a debugger.
- Understand that some target initialization may be necessary before establishing a debug connection.

## 1.1 Before you begin

This guide assumes that you are familiar with the following guides:

- [Exception model](#)
- [Memory model](#)

## 2 Different types of debug

The Armv8-A architecture can support two types of debug: external debug and self-hosted debug. Two types of debug operation can be performed: non-invasive debug and invasive debug.

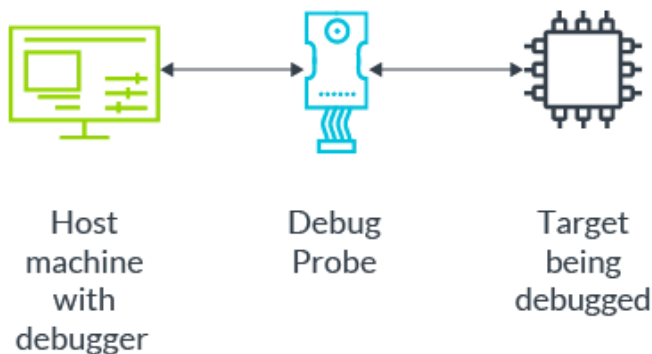
We will describe external and self-hosted debug, and invasive versus non-invasive debug. We are providing an overview only, and do not provide detail about how to program an Armv8-A processor to use any particular type of debug.

### 2.1 External debug

External debug occurs when the debugger is external to the processor being debugged. For example, external debug is taking place if a debugger that is running on a host machine is debugging an Armv8-A processor that is available on a separate development board. Another example of external debug is a debugger that is running on one processor and debugging another processor on the same SoC.

External debug is usually used when doing chip validation and bring-up, or when working with bare-metal environments. Generally, external debug relies on a physical connector, for example JTAG, or Serial Wire Debug (SWD) on the target being debugged.

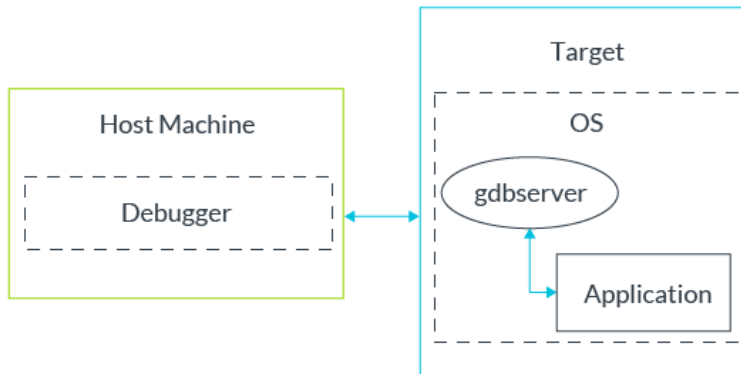
External debug also requires a debug adapter to be connected between the target being debugged and the host machine running the debugger. The following diagram shows the debug adapter connection between a host machine running a debugger and a debug target:



### 2.2 Self-hosted debug

Self-hosted debug occurs when the debugger and the software being debugged run on the same processor. A good example is gdbserver, which is used for Linux application debug. Gdbserver is a program that runs alongside a Linux application, and allows a debug environment like GDB or the Arm Debugger to debug the application.

This diagram shows how gdbserver interacts with an Operating System (OS) application and a debugger:



Even though the debugger attached to gdbserver usually runs off-target, gdbserver is still classed as self-hosted debug.

Self-hosted debug is usually used with debugging applications that are running under an OS, or when physical debug connectors are not available.

## 2.3 Invasive debug

When using invasive debug, the act of debugging changes the processor state in a subtle way. For example, when a breakpoint is set using a debugger, the processor stops when the breakpoint is hit, and the timing of the program being debugged changes.

Some familiar debug methods are invasive debug methods. These include stepping through code, viewing memory, setting breakpoints and watchpoints, and viewing registers.

Usually, the subtle changes introduced using invasive debug techniques do not affect the general execution of the program. However, some bugs, for example problems related to timing, might be sensitive to these subtle changes. This means that invasive debug techniques are not suitable for investigating this type of bug.

## 2.4 Non-invasive debug

In contrast to invasive debug, non-invasive debug does not change the processor state in any way.

For example, generating and collecting trace data from a target will usually not affect the processor, so trace is usually classified as non-invasive debug. Other operations that are usually classified as non-invasive debug are use of the Performance Monitoring Unit (PMU) and performing Program Counter (PC) sampling.





# 3 Target types

When debugging, it is important to consider the capabilities and relevancy of the target. Sometimes a target, during the development cycle, bears only a cursory resemblance to the final SoC design. This means that areas like speed, functionality, or performance might differ between earlier targets and the final design.

Here is a list of different targets that you might work with during a project, and some things to remember about each of them:

- RTL simulation or emulation
  - Accurate model of the processor but not a complete representative of the final design.
  - Debugging is very slow.
- FPGA
  - Can be true to final design.
  - Debugging is faster than RTL simulation, but slower than final target.
  - May require more steps to establish a debug connection.
- Software model
  - Can be true to layout of final design, but not necessarily timing accurate.
  - There may be aspects of the model which do not function the same way that the hardware functions.
  - Debugging is faster than RTL simulation, but slower than an FPGA.
  - Need to consider whether the model is functionally accurate or timing accurate.
- Development board
  - If built in-house, the target is similar to, or the same as, the final design. If built by a third party, the target is only similar to the final design.
  - May require more steps to establish a debug connection.
  - Debugging is faster than a model.
- Final silicon
  - The target is the final design.
  - May not have physical connectors for debugger connection.
  - Debugging is faster.
  - Typically available late in project development.

# 4 Program being debugged

Before debugging, another thing to consider is the type of program that is being debugged. The image being debugged determines the level of complexity for both the debug operations and the information that you obtain from a debugger.

Here is a list of different types of programs that you might work with, and some things to remember about each of them:

- Bare-metal and boot code
  - Directly uses the architectural features of a processor
  - Usually contains a mix of source and assembly files
  - Usually less overhead when performing debug operations
  - Easy to determine the order of execution
  - Debug information is usually not complex
  - Program memory layout is usually easy to understand
  - Memory map generally does not change during execution
  - Usually has one execution thread
  - May cross multiple Execution levels (ELs)
- OS kernel
  - Directly uses the architectural features of a processor
  - Usually contains a mix of source and assembly files
  - Harder to determine the order of execution
  - Debug information is usually more complex
  - Program memory layout is more complex
  - Memory map can change during execution
  - May have more than one execution thread
- OS application and OS module or driver
  - More difficult to see how processor architecture features are used
  - Usually made up of source files
  - May rely on library for which you do not have the source code
  - Harder to determine the order of execution
  - Debug information is usually very complex
  - Program memory layout is very complex
  - Memory map can change during execution
  - Usually has more than one execution thread
  - Usually requires the debugger to have some awareness of the OS being used



# 5 Target state

On connection to a target, the debugger shows the current state of the processor. Because of the way that the architecture is configured, the processor is probably just coming out of reset in Secure EL3 when you halt the debugger. However, your SoC might not do this.

We will now describe some common states that the target might be in upon connection:

## 5.1 Core or processor is powered down

Some targets contain hardware elements (for example switches), firmware, boot code, or an OS that power down certain cores or processors unless steps are taken. Also, cores or processors that are not being used for execution, or that have not been used recently, may be powered down by the power controller or OS of the SoC.

Processors contain hardware called debug logic, which allows you to see and configure the debug setup and operation for the processor. Because the debug logic and the processor logic are usually in different power domains, the processor logic might be powered up, while the debug logic is powered down.

Some debuggers cannot connect to powered down logic. If a debugger connection is successful, you probably cannot do much with the debugger until the core, processor, or debug logic is powered up.

## 5.2 Core or processor is held in reset

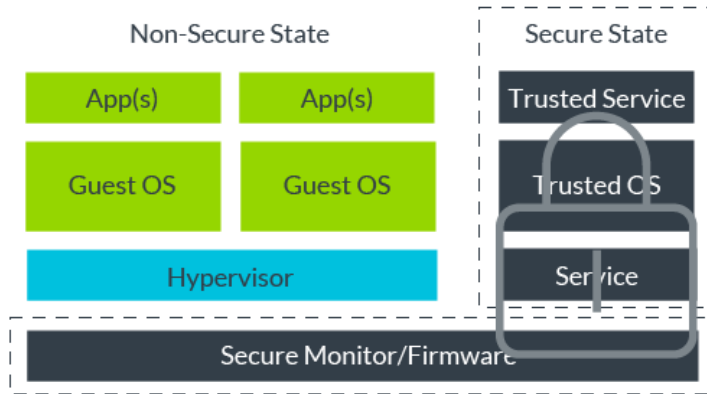
Some targets contain hardware elements, firmware or boot code that hold a core or processor in reset unless steps are taken. Also, some SoCs contain a reset controller or processor that must be configured to release another core or processor from reset.

Some debuggers cannot connect to cores or processors that are held in reset. If a connection is successful, debug operations cannot be performed until the core or processor is released from reset.

## 5.3 Core or processor is in a different security state

An Armv8-A architecture processor or core can have two security states, Secure state and Non-secure state. If the Secure state is implemented, privileged or secret information for the SoC is stored or handled via the Secure state. This means that, after a certain point in the development cycle of an SoC, the hardware or software will lock untrusted users out of the Secure state. This step is taken to prevent access to the protected data in the Secure state.

This diagram shows hardware or software locking a user out of the Secure state:



If you try to connect a debugger to an SoC that uses this operational model, then the debugger will only allow you to connect to the Non-secure state.

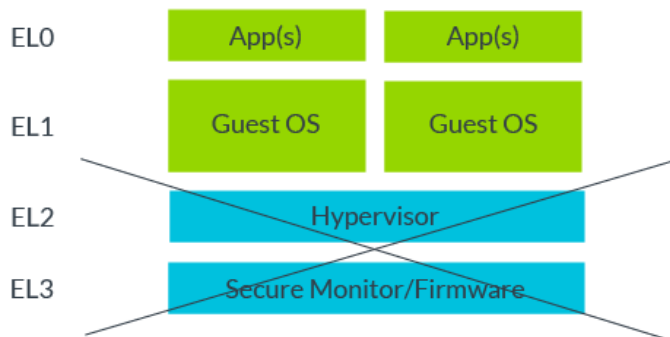
## 5.4 Core or processor is in a different Exception level

There are two common reasons why EL3 is not entered when connecting a debugger to a target.

The first reason is that the Exception level is not implemented.

In the Armv8-A architecture, certain Exception levels are optional. In some Armv8-A processor or core implementations, an Exception level is not accessible because it is not present in the design.

This diagram shows a design in which EL3 and EL2 are not implemented:

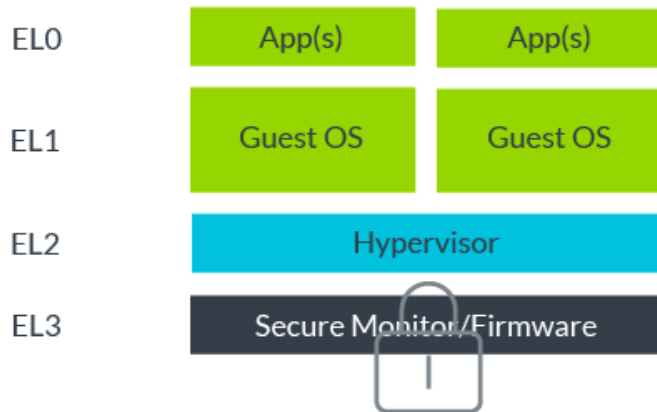


If you connected a debugger to an SoC that uses this operational model, you can only debug Exception levels EL1 and EL0.

The second reason why EL3 is not entered when connecting a debugger to a target is that the hardware or software locks users out of an Exception level.

SoC designs can lock users out of certain Exception levels either through hardware or software. This locking usually occurs late in the development cycle of the SoC, so that unprivileged users cannot access aspects of the code or SoC design.

This diagram shows an SoC in which EL3, which is usually where the secure monitor and firmware reside, is locked:



If you connected a debugger to an SoC that uses this operational model, then you could debug EL2, EL1 and EL0, but not EL3.

# 6 Initializing a target

Some targets require more steps before establishing a debug connection. The exact nature of these steps will depend on the target that you are using. If you are working with an unfamiliar target, look through the user manual for the target, or consult the designers of the target, to determine the requirements for establishing a debug connection.

Here are some of the more common target initialization steps:

## 6.1 Powering up or taking a core or processor out of reset

As explained in **Target state**, there are various reasons why a core or processor might be powered down or held in reset.

Here are some common steps that you can follow to put the core or processor into a better state for debug:

- Perform reads and writes to memory or specific devices
- Modify OS build or run attributes
- Change firmware or target settings
- Manipulate hardware elements, for example switches or SD cards

## 6.2 Unlocking scan chains or devices

Some SoC designers add locking devices or manipulate the debug hardware, so that users without certain information cannot access the debug logic on the target. These locking techniques prevent unprivileged users from debugging the SoC. These techniques are usually implemented late in the SoC development cycle. It is possible that earlier revisions of a target do not require unlocking, but later revisions do.

Here are some common steps that you can use to unlock the debug logic:

- Feed certain patterns into the lock device on the scan chain
- Perform reads and writes to memory and/or specific devices
- Manipulate hardware elements, for example switches or jumpers

## 6.3 Multiplexed signals

Pin space on an SoC is usually limited. This means that less frequently used devices might have their signals multiplexed with other devices on the SoC. For example, the signals of the off-chip trace port, the *Trace Port Interface Unit* (TPIU), might be multiplexed with the *General Purpose I/O* (GPIO) signals.

Here are two common steps that you can follow to demultiplex signals:

- Perform reads or writes to memory or registers

- Manipulate hardware elements, for example switches or jumpers

## 6.4 Missing connectors

Because pin space on an SoC is generally limited, debug output lines on an SoC might be available, but the physical connector is not. If there is pinout space on the PCB, you can overcome this issue by soldering a connector to the board.

In the late stages of the development cycle, the debug socket for an SoC might not be physically available. This might be because the SoC designer does not want users to be able to debug the target, or, or because debug is available through a non-physical method, for example gdbserver. If no socket is available, consult the user manual for the target, or other resources, for example tutorials or community postings.



# 7 Check your knowledge

# 8 Related information

Here are some resources related to material in this guide:

- [Exception model guide](#)
- [Memory model guide](#)
- [Debugger usage guide](#)
- Ask development questions, and find articles and blogs on specific topics from Arm experts at the [Arm community](#).

## 9 Next steps

This guide described concepts that are useful to know before debugging an Armv8-A processor, and explained different types of debugs, target and application considerations, target state, and target initialization.

This guide is the first of two debugging guides for Armv8-A. To learn more, read our guide [Debugger usage on Armv8-A](#).

Error! No text of specified style in document. Error! No text of specified style in document.