Protecting Microelectronics

Welcome

Protecting Microelectronics

Introduction

[Tiffany] Microelectronics are utilized to ensure the integrity of military systems in the Department of Defense, or DOD. They are used to support nearly all DOD activities such as communications. However, there are variations in the use and importance of each device.

This short considers what microelectronic are, DOD's microelectronic needs, existing threats, vulnerabilities, and associated reporting requirements.

I'm Tiffany, one of the DOD System Security Engineers here. I will walk you through the key topics, such as microelectronics and existing threats. Bradley, a DOD Facility Security Officer, or FSO, will discuss the remaining topics in this short.

Key Topics:

- Defining microelectronics
- What are the existing threats?
- Key vulnerabilities
- Indicators of compromise
- Reporting requirements

Learning Objective:

- The learner will be able to define microelectronics and recognize the associated threats and vulnerabilities.

Defining Microelectronics

Let's get started by defining microelectronics.

Microelectronics is a subfield of electronics that support nearly all DOD activities, enabling capabilities such as the global positioning system, radar, command and control, and communications.

There are many types of microelectronics, but the three most commonly discussed in terms of defense are: Application Specific Integrated Circuits, or ASICs, Field Programmable Gate Arrays, or FPGAs, and Systems on Chips, or SoCs.

Application Specific Integrated Circuits (ASICs)

ASICs are an integrated circuit customized for a specific function and not general-purpose use.

ASICs are used throughout Defense, communications, and industrial sectors.

Some examples include consumer electronics, communications equipment, and space systems when radiation- hardened.

Rollover text: Radiation hardening: The process of making electronic components and circuits resistant to damage or malfunction caused by high levels of ionizing radiation, especially for environments in space, around nuclear reactors or during nuclear accidents or nuclear warfare.

Field Programmable Gate Arrays (FPGAs)

FPGAs are integrated circuits designed to be configured by either a customer or a designer after manufacturing. This is how it gets the name field programmable. FPGAs are applicable all throughout Defense, communications, and industrial sectors.

Here are some examples: Aeronautics, communications, imagery systems, and space systems when radiation-hardened.

Rollover text: Radiation hardening: The process of making electronic components and circuits resistant to damage or malfunction caused by high levels of ionizing radiation, especially for environments in space, around nuclear reactors or during nuclear accidents or nuclear warfare.

Systems on Chips (SoCs)

SoCs are integrated circuits utilizing many or all components of a computer or electronic device. SoCs can be used for a wide variety of computing functions. Some examples include mobile computing devices such as tablets, smartphones, and embedded systems.

Unfortunately, securing access to the leading-edge microelectronics can be a challenge due to potential targeting and threats from U.S. adversaries.

Protecting Microelectronics

Now that we know what microelectronics are, let's talk about why they need protection. Microelectronics security is vital due to potential targeting and threats from our adversaries and other emerging challenges.

Electronics and the subcategory of microelectronics are among the most targeted on the Industrial Base Technology List. Further, the sophistication of U.S. adversaries, who might target military or dual-use electronic components, emphasize the need for continuous training on the microelectronics security framework.

Several policies guide the protection of microelectronics. Department of Defense Instruction, or DODI, 5200.44 - Protection of Mission Critical Functions to Achieve Trusted Systems and Networks, or TSN, requires that DOD manage risks to the supply and security of certain microelectronic components.

DODI 5000.83, "Technology and Program Protection, or TAPPS, to Maintain Technological Advantage" maintains TAPPs, Science and Technology, or S&T protection, and Program Protection Plans, or PPPs. This policy will manage activities to protect and enable technological innovation for present and future warfighting capabilities and programs.

Lastly, DOD Directive, or DODD, 5137.02, Under Secretary of Defense for Research and Engineering states the DOD must provide specific protections—including detecting, avoiding, and mitigating potential threats—based on a component's military importance or criticality.

Security needs vary based on use and importance of each device, changes in supply, supply chain, demand, the emergence of new threat actors, and availability of effective threat countermeasures. However, no single security solution can provide complete protection for the full range of critical components.

Knowledge Check 1

Which of the following correctly defines microelectronics?

○ An electronics agency that supports nearly all DOD activities
○ A program that supports nearly all DOD activities
○ A subfield of electronics that supports nearly all DOD activities
○ A type of threat that impacts DOD activities

Knowledge Check 2

Security needs can vary based on: (Select all that may apply).

- ○ Design of the device
- ○ Location of the device
- ○ New threat actors
- ○ Use and importance of each device

Threats

To ensure the confidentiality, integrity, and availability of its microelectronics, the DOD must consider and contend with several potential risks.

The Department of Homeland Security, National Institute of Standards and Technology, and Government Accountability Office, have identified risks and vulnerabilities to securely acquiring DOD electronics. Risks to microelectronics fabrication and assembly have received particular focus within the DOD.

The risks could include loss of sensitive information, introduction of fraudulent products, insertion of malicious hardware or code, failures in quality and reliability, and loss of access to electronic components.

Loss of Sensitive Information

Loss of sensitive information involves the unauthorized removal or theft of sensitive and/or Critical Program Information, or CPI, or Intellectual Property, or IP, from a design, template, or electronic device. Malicious agents can exfiltrate CPI through unauthorized production or theft of sensitive hardware.

In addition to hardware or IP theft, reverse engineering is a threat which includes disassembling the device to determine its underlying structure, function, and composition for the purpose of replicating or defeating the device.

Introduction of Fraudulent Products

Introduction of fraudulent products involves the introduction of counterfeit or unauthorized microelectronics into DOD's supply chain. At best, counterfeit products will not function within the required parameters. At worst, counterfeit products can be a means of espionage or sabotage. Malicious actors could also damage or destroy hardware through heating, leading to unexpected and premature hardware failure.

- Introduction of counterfeit or unauthorized microelectronics
- Destruction or damage to devices
- Includes recycled, defective, relabeled, and cloned devices

Types of attack vectors could include counterfeiting, cloning, or unauthorized production of microelectronic components.

- Counterfeiting or the misrepresentation of an unlawfully reproduced part as being authentic and unmodified.
- Cloning or the creation of an exact copy of a genuine part outside of the control of the authorized manufacturer.
- Unauthorized production of microelectronic components by a legitimate supplier without DOD permission.

Attack Vectors: Attack vectors are any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy assets, information system resources or the information itself

Insertion of Malicious Hardware or Code

Insertion of malicious hardware or code involves the intentional introduction of defects or malicious functions into a photomask or into an individual integrated circuit that could permit unauthorized control of a DOD system.

Types of attack vectors include design alteration and Hardware Trojans. Design alteration includes the modification of a product’s specifications, design documents, or physical design to create system weaknesses. Hardware Trojans involve the addition or bypassing of integrated circuit logic to enable malicious actions.

Photomask: Used to produce a pattern on the integrated circuit which comprise the completed design of the integrated circuit. In other words, a photomask is a special stencil used to create a printed circuit board or integrated circuit.

Failures in Quality and Reliability

Quality issues can include product defects and inadequacies introduced either maliciously or through negligence that lead to system and performance issues.

Reliability issues may not stem from an attack, but can result in hardware failures that compromise DOD electronics requirements such as longevity and temperature range.

Loss of Access to Electronic Components

While not a threat to the component’s function, loss of access, especially in terms of supply chain, risks DOD’s ability to maintain or upgrade critical systems in response to new or shifting dangers.

Types of supply chain threats include obsolescence and supplier loss.

- Obsolescence involves the lack of availability of a particular component. This could be the result of a supplier ceasing production or support of the component due to commercial pressures or new versions.
- Supplier loss involves the inaccessibility of a particular supplier, potentially due to the supplier's closure.

Knowledge Check 3

Match the threat to the correct definition:
a. Obsolescence
b. Hardware Trojan
c. Reverse engineering
d. Cloning

____ Lack of availability of a particular component, potentially as supplier ceases support and production of the component due to commercial pressures or new versions

____ Creation of an exact copy of a genuine part outside of the control of the authorized manufacturer

____ Addition or bypassing of integrated circuit logic to enable malicious actions

____ Determining the underlying structure, function, and composition of a device for the purpose of replicating or defeating the device

Countermeasure – Advanced Integrated Circuits

[Bradley] Tiffany, thanks for addressing the definition and risks associated with microelectronics. I'll take it from here and discuss potential countermeasures and trusted technology.

Although there are many risks involved in the fabrication of microelectronics, leading-edge microelectronics offer specific, military-relevant advantages to DOD and its foreign competitors.

Advanced Integrated Circuits generally offer smaller feature sizes, increased performance, and greater capabilities that are critical in achieving stringent military size, weight, and power, or SWaP, requirements. Despite the complexity of newer integrated circuit technologies, the security threats from reverse engineering, counterfeiting, or cloning are still present in advanced microelectronics. Increased access to leading-edge integrated circuits can also facilitate repeated upgrading of military systems to meet new challenges, risks, or threats.

Countermeasure – Risk Management

Throughout the microelectronics lifecycle, DOD requires the use of risk management techniques to prevent or reduce the likelihood of harmful components entering the supply chain, minimize vulnerabilities, or make threats more difficult to execute, detect compromised microelectronics, and respond to a compromise by mitigating potential consequences.

Minimize Risk: For minimizing risk in the fabrication phase, available or proposed countermeasures include:

- Use of trusted vendors accredited by the Defense Microelectronics Activity (DMEA); this option is available for applicable systems with trusted workflow requirements.
- Domestic or DOD ownership of suppliers.
- Purchasing sensitive equipment anonymously to conceal a DOD connection.

Detection of Threats: For the detection of threats occurring in the fabrication phase, available or proposed countermeasures include:

- Visual inspection of integrated circuits to spot counterfeit or stressed hardware
- Validation of integrated circuits and photomasks against a known, trusted design
- Electromagnetic or thermal analysis to spot counterfeit or altered hardware

Response to Threats: For the response to threats occurring in the fabrication phase, available or proposed countermeasures include:

- Mandatory reporting of suspected fraudulent products
- Identifying multiple suppliers to allow for switching between component sources
- Maintaining an inventory of spares to combat obsolescence

Knowledge Check 4

Fill in the blank: The visual inspection of integrated circuits to spot counterfeit or stressed hardware in the fabrication phase is referred to as ______________.

○ Risk Mitigation
○ Detection of Threats
○ Response to Threats

Knowledge Check 5

Fill in the blank: Reporting of suspected fraudulent products in the fabrication phase is referred to as a ____________.

○ Risk Mitigation
○ Detection of Threats
○ Response to Threats

Summary

In this short, you have learned about microelectronics terminology, functions, chief threats, vulnerabilities, and countermeasures. Let’s review some key points.

Microelectronics support nearly all DOD activities. DODI 5200.44, DODI 5000.83, and DODD 5137.02 guide communications and protections surrounding microelectronics. Threats to microelectronics could include loss of sensitive information, introduction of fraudulent products, insertion of malicious hardware or code, failures in quality and reliability, and loss of access to electronic components.

Lastly, risk management techniques include the use of trusted vendors, visual inspection of integrated circuits to spot counterfeit hardware, and mandatory reporting of suspected fraudulent products.

For more information on microelectronics, please visit the Course Resources. You may also contact the Defense Counterintelligence and Security Agency (DCSA) or your counterintelligence (CI) Special Agent (CISA) for a security briefing.

Course Conclusion

Congratulations! You have completed the Protecting Microelectronics short.

Answer Key

Knowledge Check 1

Which of the following correctly defines microelectronics?

○ An electronics agency that supports nearly all DOD activities
○ A program that supports nearly all DOD activities
● **A subfield of electronics that supports nearly all DOD activities**
○ A type of threat that impacts DOD activities

Feedback: Microelectronics is a subfield of electronics that support nearly all DOD activities, enabling capabilities such as the global positioning system, radar, command and control, and communications.

Knowledge Check 2

Security needs can vary based on: (Select all that may apply).

○ Design of the device
○ Location of the device
○ **New threat actors**
○ **Use and importance of each device**

Feedback: Security needs can vary based on factors such as new threats actors and use and importance of each device.

Knowledge Check 3

Match the threat to the correct definition:
a. Obsolescence
b. Hardware Trojan
c. Reverse engineering
d. Cloning

_a_ Lack of availability of a particular component, potentially as supplier ceases support and production of the component due to commercial pressures or new versions

_d_ Creation of an exact copy of a genuine part outside of the control of the authorized manufacturer

_b_ Addition or bypassing of integrated circuit logic to enable malicious actions _c_ Determining the underlying structure, function, and composition of a device for the purpose of replicating or defeating the device

Feedback: Obsolescence involves the lack of availability of a particular component, potentially as supplier ceases support and production of the component due to commercial pressures or new versions. Cloning is the creation of an exact copy of a genuine part outside of the control of the authorized manufacturer. Hardware trojans involve the addition or bypassing of integrated circuit logic to enable malicious actions. Lastly, reverse engineering involves determining the underlying structure, function, and composition of a device for the purpose of replicating or defeating the device.

Knowledge Check 4

Fill in the blank: The visual inspection of integrated circuits to spot counterfeit or stressed hardware in the fabrication phase is referred to as ______________.

- Risk Mitigation
- **Detection of Threats**
- Response to Threats

Feedback: The detection of threats countermeasures occurring in the fabrication phase include, but are not limited to, visual inspection of integrated circuits to spot counterfeit or stressed hardware.

Knowledge Check 5

Fill in the blank: Reporting of suspected fraudulent products in the fabrication phase is referred to as a ____________.

- Risk Mitigation
- Detection of Threats
- **Response to Threats**

Feedback: The response to threats countermeasures occurring in the fabrication phase include, but are not limited to, mandatory reporting of suspected fraudulent products.