

Module 13 - Critical Requirements: Safety, Security, and Privacy

*TOC*

## Program Protection Plan (PPP) and Typical Critical Requirements

TOC

Depending on the type of system being developed, safety, security, and privacy requirements are considered to be among the most critical issues for many software systems.



## Lesson Objectives

TOC

This lesson presents an overview of a Program Protection Plan and critical requirements for software systems.

After completing this lesson, you will be able to:

- Identify the purpose and key components of a Program Protection Plan.
- Describe why critical requirements are important.
- Identify typical critical requirements for software-intensive systems.
- Identify accessibility requirement for electronic information technology.



Objectives



## Key Components of a Program Protection Plan

There are two main components of a Program Protection Plan (PPP) which include:

- Critical Program Information (CPI)
- Mission-Critical Functions and Components

They are the foundations of a PPP and consist of the technology, components, and information that provide mission-essential capability to our defense acquisition programs.

**Select CPI and Mission-Critical Functions and Components to learn more.**



## Knowledge Review

TOC

Which are the foundations of a Program Protection Plan? (Select all that apply)

- Mission-Critical Functions and Components
- Critical Program Information (CPI)
- Intelligence and Counterintelligence (CI) Support

**Check Answer**



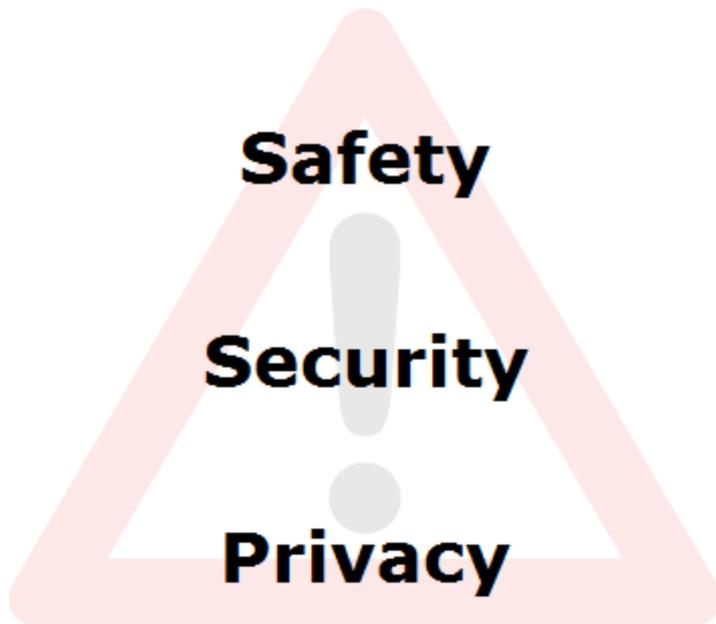
## Predominant Critical Requirements

TOC

Although there are no hard and fast rules, it is generally true that:

- For a [Weapons System](#), system and software **Safety** is among its predominant critical requirements.
- For a [C4I System](#), **Security** issues is among its predominant critical requirements.
- For a [Defense Business System](#), **Privacy** issues is among its predominant critical requirements.

*Select each predominant critical requirement, Safety, Security and Privacy to learn more.*



## Accessibility

TOC

The previous pages detailed the importance of the critical requirements safety, security and privacy. Accessibility is yet another important requirement that must be considered with acquiring and using electronic information technology (EIT). While accessibility may not rise to the level of criticality as safety, security and privacy, it is very important to a growing community of IT users who require assistive technology to work with and access electronic information.

In 1998, Congress amended the Rehabilitation Act of 1973 to require Federal agencies to make their electronic and information technology (EIT) accessible to people with disabilities.

Inaccessible technology interferes with an ability to obtain and use information quickly and easily. Section 508 was enacted to eliminate barriers in information technology, open new opportunities for people with disabilities, and encourage development of technologies that will help achieve these goals.

While there are [exceptions](#) to the applicability to Section 508 for IT systems, when acquiring IT systems, accessibility needs to be added to the list of requirements.

The ability to access and use EIT is the LAW.



## Summary

[TOC](#)

The purpose of the Program Protection Plan (PPP) is to ensure that programs adequately protect their technology, components, and information throughout the acquisition process during design, development, delivery and sustainment.

The two main components of a Program Protection Plan (PPP) are:

- Critical Program Information (CPI)
- Mission-Critical Functions and Components

Among the most critical requirements for many software systems are safety, security, and privacy.

**Select each critical require to review its key points.**

**Safety**

**Security**

**Privacy**

### Safety

A software system is safety-critical if there is a degree of "unacceptable risk" associated with its incorrect operation. Software safety is part of the overall System Safety Program.

Developers often use analytical methods such as such as Fault Tree Analysis (FTA) and Failure Modes, Effects and Criticality Analysis (FMECA) to help perform safety analysis. Safety is the number one design concern for Weapons systems software.

## Summary, Cont.

In the MLS environment, a system's security operations are characterized according to user clearances and security levels of the data either processed or transferred by the system. The four modes, defined by DoD, are:

- Dedicated security mode: least difficult of the four security modes of operation
- System High security mode: somewhat difficult compared to the other modes of operation
- Partitioned security mode: moderately difficult
- Multilevel security mode: most difficult of the four modes of operation

Finally, another important requirement to factor in when dealing with any EIT is accessibility. Accessibility may not rise to the level of criticality as safety, security and privacy; however, it is very important to a growing community of IT users who require assistive technology to work with and access electronic information.

While there are exceptions to the applicability to Section 508 for IT systems, when acquiring IT systems, accessibility needs to be added to the list of requirements. The ability to access and use EIT is the LAW.



Lesson Completion

[TOC](#)

You have completed the content for this lesson.

To continue, select another lesson from the Table of Contents on the left.

If you have closed or hidden the Table of Contents, click the Show TOC button at the top in the Atlas navigation bar.

## Critical Program Information (CPI)

TOC

[Critical Program Information \(CPI\)](#) should be thought of as the technological "crown jewels" of the program.

The United States gains military advantages from maintaining technology leads in key areas, so we must protect them from compromise in the development environment and on fielded systems.

CPI may include:

- Classified military information
- Controlled Unclassified Information (CUI)
- Commercial-off-the-Shelf (COTS) technology



## Critical Program Information (CPI), Cont.

TOC

CPI determination is done with decision aids and Subject Matter Experts (SMEs). As general guidance, PMs should identify a component as CPI if:

- Critical technology components will endure over its lifecycle
- A critical component which supports the warfighter is difficult to replace
- A capability depends on technology that was adjusted/adapted/calibrated during testing and there is no other way to extrapolate usage/function/application
- The component was identified as CPI previously and the technology has been improved or has been adapted for a new application
- The component contains a unique attribute that provides a clear warfighting advantage (i.e. automation, decreased response time, a force multiplier)
- The component involves a unique method, technique, application that cannot be achieved using alternate methods and techniques
- The component's performance depends on a specific production process or procedure
- The component affords significant operational savings and/or lower operational risks over prior doctrine, organization, training, materiel, leadership and education, personnel, and facilities (DOTMLPF) methods
- The Technology Protection and/or Systems Engineering (SE) Team recommends that the component is identified as CPI
- The component will be exported through Foreign Military Sales (FMS)/Direct Commercial Sales (DCS) or International Cooperation

## Mission-Critical Functions and Components

Mission-critical functions are those functions of the system being acquired that, if corrupted or disabled, would likely lead to mission failure or degradation.

Mission-critical components are primarily the elements of the system (hardware, software, and firmware) that implement critical functions.

Mission-critical functions and components are equal in importance to Critical Program Information (CPI) with respect to their inclusion in comprehensive program protection, its planning (documented in the PPP), and its execution.

Efforts to identify mission-critical functions and components and their protection must begin early in the lifecycle and be revised as system designs evolve and mature.

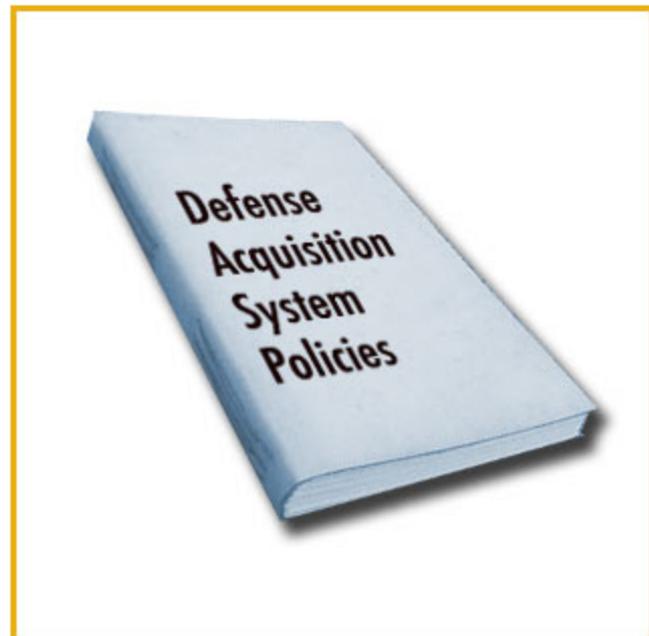


## Systems Safety Analysis

Defense Acquisition System policies encourage PMs to: identify and evaluate system safety and health hazards, define risk levels, and manage all hazards associated with development, use, and ultimate disposal of the system. Various plans are required and safety related issues are formally evaluated at selected milestones.

Although software plays a key part in the functionality of today's defense systems, it is just one part of an overall system. A systems perspective that identifies systems-level safety hazards as described in MIL-STD 882E, DoD Standard Practice for System Safety.

At the systems level, a Systems Safety Analysis is used to describe the formal processes used by systems and safety engineers to identify, evaluate, and control hazards in a total system context.



TOC

## System Safety Program

Software safety is part of the overall System Safety Program. The System Safety Program includes the application of system safety engineering techniques to software.

The purpose of the safety program is to ensure and verify that:

- The software design includes positive measures to enhance system safety
- Errors have been eliminated or controlled to an acceptable level of risk



TOC

## Safety-Critical Software

A software system is considered safety-critical if there is some degree of "unacceptable risk" associated with the incorrect operation of that system. Examples of unacceptable risk include:

- Loss of human life
- Severe equipment damage
- Damage to the environment



TOC

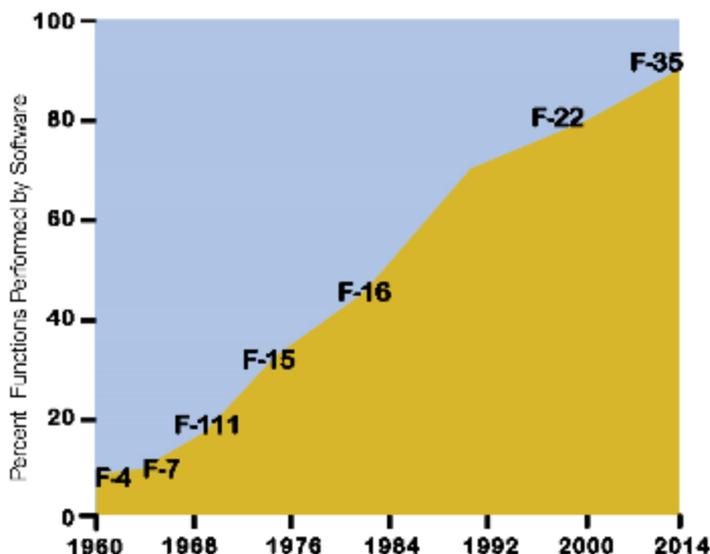
## Software Safety

As weapons systems become increasingly complex and dependent on software, software safety is a growing concern.

Increasing dependence on software to control safety-critical functions is also critical throughout the civilian sector in areas such as:

- Air traffic control
- Ship navigation
- Mass transit
- Medical equipment
- Nuclear power plant operation

Select the image for an enlarged view.



D

TOC

## Software Safety and Design

The roots of software safety are formed early in the requirements analysis and design phase of the software development process. Remember that:

- Misunderstandings or poor oversight during requirements analysis or design can lead to safety-critical faults or errors.
- Software safety is a design activity, not an afterthought. Safety cannot be "tested in" after a system is developed.
- The Systems Engineering process must drive software safety activities.

[D](#)

## Analytical Methods

Developers frequently use analytical methods when performing System Safety Analysis. Examples of these methods include:

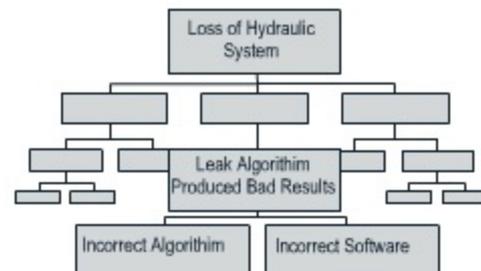
- Fault Tree Analysis (FTA) and
- Failure Modes, Effects, and Criticality Analysis (FMECA)

*Select each analytical method to learn more.*

[FTA](#)[FMECA](#)

Fault Tree Analysis (FTA) starts with a particular undesirable event and provides an approach for analyzing the causes of this event.

## Fault Tree Analysis



TOC

## Examples of Safety Plans

A system-level safety program can be developed from a set of standard tasks that typically are needed to manage program safety.

This set of standard tasks is then tailored to the project and forms the basis for a project-specific System Safety Program System Safety Program

Details are typically found in the project's System Safety Program Plan (SSPP) or its equivalent. For software safety issues only, a separate Software Safety Plan (SSP) can be prepared.

**Select SSPP and SPP below to view their respective outlines.**

### System Safety Program Plan

### Software Safety Plan



TOC

## Knowledge Review

What ensures and verifies that the software design includes positive measures to enhance system safety.

Software Safety Program

FMECA

FTA

Check Answer



## Security

TOC

In some systems, all sensitive information is protected at the highest classification for data contained in that system. If one piece of data is **TOP SECRET**, then the entire system is classified at that level.

Although the easiest to implement, this approach results in over-classification of data, over-clearing of personnel, redundancies, and inefficiencies.

To overcome these problems, technologies based on Multilevel Security (MLS) can be used. MLS allows users with different clearances to simultaneously process different classifications of data.

```

000 11101 101010100 00011 01101010 0010010 0100 1111 1110
CLEARANCEREQUIRED01010001010 114001010 TOP SECRET
00100 000 00000 0010 00101 111 1100 010 10100 101010011
0100 10 110 001011 PASSWORD 010110 10101001 0111 101 001
000101 010 010100101 1010 01001010 100011000 110 000 00 1
001 01010 010 1110 010101010 1011 0 1000 10 101010 011 11
100 10101000 101010100 0010 1010100 101010010 111 10001
110101 001 11001001 010 000010 TOP SECRET10101 100 0101
00 1010 101 001010 010 1010100 00011010 11110 000001010 100
001010 101 TOP SECRET01 01010 00010000 10 01010 11
10010100 00 011101 111 01010 1000001 10110 CLEARANCE
REQUIRED1111 11101010 001110 1100001010 001 01011 10010
100 10111001 1001 00000 000000 0100010 11111100 010 10100
101010 0110 100TOP SECRET1010 101110 00000101 01 10 10101
00101 1110100 10001010100 101001 011 01001001010 100
0110001100 000 00010 101001011100 101010101 01101 000 1
01010 101011001 0101000 1010 10100001 0101 PASSWORD1 00
10111 10001 010 1001110 010010100 00010 101 001001 0101
011000 1010 0101010 1001 010010101 01000 010 10111100 0
0 00101 010001 010 10111010101 011111001 0010 001010 001
10110 PASSWORD 11110010100 01 11 01 1110 1010100000 11
011 010100010 0100100111111 1010100 01 11 010 000101 000
1010 1110010100 101110011 001000000000 00 01 00010 1 1111
100010 10 1001010 10011010001 011000 10 110 101011 000 00 0
10101 101010 10 0101111010 010 0010 101 00101 001 0110 1 0
010 01010 10001 10 0011000 00001 010 101 0010 11100101 01 010
10110 100 01010101010 1110010 10100 0101 01 0100 00101
0101001 01010 01 0111 10001 PASSWORD001001010000001 010
1 001001 01 01 011 000101 001 010101 0010 100 10101 010000
011 0 CLEARANCE REQUIRED000010 1010111 0101 010 11 11 10
010 01 00011101 0101 0101 001 110100 11001 100000 11
011110 1010100000 1101 10101001001 001001 TOP SECRET 00
011 PASSWORD10001010 11 100 10 10 010111 001100 100 00 0

```

## Security Modes of Operation

In the MLS environment, a system's security operations are characterized according to user clearances and security levels of the data either processed or transferred by the system. The user and environmental characteristics can be used to establish a spectrum of modes of MLS operations. The modes have increasing security capabilities but become technologically more complex.

*Select the tabs to learn more about each security mode.*

**Dedicated**

System High

Partitioned

Multi-Level

In the Dedicated Security Mode:

- All users with access to the system have both the appropriate security clearance and need-to-know access for all classified information contained in the system.
- Controls that restrict all aspects of the systems are established.
- Controls conform to those required for the protection of the highest classification category contained in the system.
- Is the least difficult to implement of the four security modes of operation.



TOC

## Knowledge Review

What is the level of difficulty for partitioned?

- Somewhat difficult
- Most difficult
- Moderately difficult

Check Answer



## Privacy

Some of the earliest applications of computers were for business applications such as payroll, personnel management, tax processing and supply management.

In the beginning people realized these types of IT systems, databases containing sensitive personnel information, required special protection.

Unlike the cumbersome paper records these early systems replaced, it was far easier to exchange information and quickly compromise vast amounts of personnel information.

These concerns are even more relevant in today's highly-networked systems which are subjected to a variety of computer security and hacking attacks.

Any type of DoD IT system that directly or indirectly processes personal-type data needs to take special steps to address privacy concerns. For these types of systems, privacy is almost always a critical requirement.

To address this issue, so-called Privacy Laws were passed in an attempt to ensure protection of essential information.

