**Missile Warning System**

**System Requirement Specification**

Index

[1. Scope 3](#_Toc273118120)

[1.1 Identification 3](#_Toc273118121)

[1.2 System overview 3](#_Toc273118122)

[1.3 Document overview 5](#_Toc273118123)

[2. Referenced documents 5](#_Toc273118124)

[2.1 Input to requirements 5](#_Toc273118125)

[2.2 Standards 5](#_Toc273118126)

[3. 3. Requirements. 6](#_Toc273118127)

[3.1 Required states and modes. 6](#_Toc273118128)

[3.2 3.2 System capability requirements. 8](#_Toc273118129)

[3.2.1 Engaging / Disengaging The System 8](#_Toc273118130)

[3.2.2 The system will detect a threat, decide and react accordingly 8](#_Toc273118131)

[3.2.2.1 Detection of a threat 8](#_Toc273118132)

[3.2.2.1.1 Detection of a threat is done by the MWS. 8](#_Toc273118133)

[3.2.2.2 The Threat is processed by the Threat Response Subsystem 8](#_Toc273118134)

[3.2.2.2.1 Pattern matching the threat 8](#_Toc273118135)

[3.2.2.3 Reaction to the Thread 9](#_Toc273118136)

[3.2.2.3.1 The kind of threat and the direction of the threat is displayed 9](#_Toc273118137)

[3.2.2.3.2 The kind of threat is announced through the audio cue system in the intercom. 9](#_Toc273118138)

[3.2.2.3.3 The Countermeassure program 9](#_Toc273118139)

[3.2.3 Other functional requirements 9](#_Toc273118140)

[3.2.3.1 CCU 10](#_Toc273118141)

[3.2.3.2 POD 10](#_Toc273118142)

[3.2.4 Performance requirements 11](#_Toc273118143)

[3.2.4.1 CCU 11](#_Toc273118144)

[3.3 System external interface requirements. 11](#_Toc273118145)

[1. 3.3.1 Interface identification and diagrams. 12](#_Toc273118146)

[2. Interface A (Interface to Aircraft Mission Computer. 12](#_Toc273118147)

[3.3.1 CCU 12](#_Toc273118148)

[3.3.2 POD 13](#_Toc273118149)

[3. 3.3.x (Project-unique identifier of interface). 13](#_Toc273118150)

[3.4 3.4 System internal interface requirements. 14](#_Toc273118151)

[3.5 3.5 System internal data requirements. 15](#_Toc273118152)

[3.6 3.6 Adaptation requirements. 15](#_Toc273118153)

[3.7 3.7 Safety requirements. 15](#_Toc273118154)

[3.8 3.8 Security and privacy requirements. 15](#_Toc273118155)

[3.9 3.9 System environment requirements. 15](#_Toc273118156)

[4. Temperature. 15](#_Toc273118157)

[5. Acceleration. 16](#_Toc273118158)

[3.10 3.10 Computer resource requirements. 16](#_Toc273118159)

[6. 3.10.1 Computer hardware requirements. 16](#_Toc273118160)

[7. 3.10.2 Computer hardware resource utilization requirements. 16](#_Toc273118161)

[8. 3.10.3 Computer software requirements. 16](#_Toc273118162)

[9. 3.10.4 Computer communications requirements. 16](#_Toc273118163)

[3.11 3.11 System quality factors. 17](#_Toc273118164)

[3.12 3.12 Design and construction constraints. 17](#_Toc273118165)

[10. Weight. 17](#_Toc273118166)

[11. Mounting. 17](#_Toc273118167)

[12. MWS. 17](#_Toc273118168)

[13. Power. 17](#_Toc273118169)

[14. Coverage against missile threats. 17](#_Toc273118170)

[3.13 3.13 Personnel-related requirements. 18](#_Toc273118171)

[3.14 3.14 Training-related requirements. 18](#_Toc273118172)

[3.15 3.15 Logistics-related requirements. 18](#_Toc273118173)

[3.16 3.16 Other requirements. 18](#_Toc273118174)

[3.17 3.17 Packaging requirements. 18](#_Toc273118175)

[3.18 3.18 Precedence and criticality of requirements. 18](#_Toc273118176)

[4. 4. Qualification provisions. 18](#_Toc273118177)

[5. 5. Requirements traceability. 22](#_Toc273118178)

[6. 6. Notes. 23](#_Toc273118179)

[7. A. Appendixes. 24](#_Toc273118180)

**History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Description** | **Name** | **Version** |
| 17-09-2010 | Initial document | kpi | 1 |
| 18-09-2010 | Format requirements to heading 1 | kpi | 2 |
| 23-9-2010 | Strukture from SSS-DID put in. Paragraph 3.8, 3.9 and 3.12 is updated. | LMU | 3 |

# Scope

## Identification

This document describes a self protection suite for the F-16 combat aircraft used by the Royal Danish Air Force. The protection suite incorporates a pod for mounting under the left wing and an intelligent cockpit control unit for controlling the system. In the pod is mounted a Missile Warning System (MWS) which gives input to the cockpit control unit. The cockpit control unit controls the dispensing of flares and chaffs from the pod. The solution shall provide warning upon detection of missile threats and be able to automatically dispense payloads in response.

The MWS will be provided as Government Furnished Equipment (GFE) and be physically installed by Company F.

## System overview

The system is a self protection suite for a F-16 combat aircraft , it shall protect the aircraft against missile attacks. The system consists of 2 main systems:

* Cockpit Unit, which communicate with the systems in the POD and Aircraft Mission Computer. Has also an interface to the aircraft intercom system and an interface for the user to control the system.
* POD, which holds magazines for flares and chaffs and what is needed for firing them of, plus the MWS system.



Missiles shall be detected by the MWS that are provided as a GFE equipment and mounted by Company F. When missile attacks are detected information is sent to the cockpit control unit, which depending on the mode it is in will react on the information and is able to react by dispensing flares and chaffs according to the program chosen. By the interface to the aircraft intercom system audio cues and warnings can be provided.

The system has a number of different users depending on what is done and where:

* On ground the system can be maintained by technicians that update SW and control the system
* Ground personnel shall be able to mount it and, when ready for takeoff, arm it.
* The pilot shall use the system, by choosing an appropriate program and depending on program chosen, consent dispense when missile attacks are detected.
* After dispensing has happened maintenance has to be done again to fill up the magazines again with flares and chaffs.

Other relevant documents for this system are:

* Technical description of MWS system. Document number xxx
* Mechanical description of MWS system. Document number xxx
* User handbook of MWS system. Document number xxx

## Document overview

This document shall describe all the Systems Requirements for the Self Protection System for the F-16 combat aircraft and the development of the system shall be based on this document, when the system fulfil the requirements in this document the requirement of the Royal Danish Air Force is fulfilled.

This document must only be used in the project group by Company F and project group and other personal at The Royal Danish Air force that are cleared to have access to this project.

# Referenced documents

# Input to requirements

|  |  |  |
| --- | --- | --- |
| **ID** | **Name** | **Description** |
| TC1 | Terma case.pdf | Document received from TERMA at IHA 3/9 2010 |
| TCC1 | Terma case comments v1.pdf |  |
| TCM1 | Terma case meeting 17 9 2010 at IHA v1.pdf |  |
| TCQA1 | Terma case questions and answers v1.pdf Answers received at consultation meeting at IHA 17/9 2010 room 517. |  |

# Standards

|  |  |
| --- | --- |
| **Standard** | **Description** |
| DM30p | NATO dispenser magazine type contains the complete details about the magazines physical constructions and interface, |
| FP42f | MIL standard 1600-2-9 v12.45 - F-16 POD standard contains complete specification about requirements for POD manufacturing, including size, weight, material, shape, etc. |
| FE16d | F-16 EW standard contains the requirements and test procedures required to have a new system approved on an F-16. |
| PM11b | F-16 POD mounting standard includes specifications on how a POD shall safely be mounted to an F-16 aircraft. |
| DF14b | NATO dispenser threat format specify the protocol to use when exchanging threat data with the F-16 aircraft mission computer. |
| GFE | The complete specification of the Government Furnished Equipment that is the MWS. |
| FBIT12c | F-16 subsystem BIT standard indicate how a subsystem shall test its internal status to comply with the F-16 operational standard. |
| ACTv2 | Separate document excluded due to the fact that it is not important for the process. |
| AMM32f | Aircraft maintenance manual contains details about how removable parts on aircraft shall be located and labeled. |
| SDS23v | DOD sensitive data standard specify how sensitive data must be stored, and also how the decryption key must be stored. |
| DWS12g | DOD data wipe specification dictates how sensitive data must be wiped from different media. |
| MIL-1553B | Military standard for a redundant communication protocol. The MIL-1553B is pure master-slave(s), and can have 1 Bus Controller (BC) and a number of Remote Terminals (RT). Only the BC can initiate communication, so if two RTs are to communicate it must be programmed into the BC. The MIL-1553B specify polling frequencies of up to 50Hz, meaning that a given package (e.g. status information) can be requested (and thereby sent) with a minimum interval of 20ms. |

# 3. Requirements.

## Required states and modes.

R-X : The system shall be able to work in 2 different System states: Armed and Disarmed.

INFO:

* Armed: In this state the system is able to react on information from the MWS system and depending on which mode it is set to by the pilot (Manuel, Semi automatic or automatic from UR 12) it will react according to the mode. But for security reasons there shall also be a “plane on ground” mode, where firing of chaffs and flares are disabled.

INFO:

* Disarmed: in this state it shall be impossible to fire flares or chaffs even though the MWS system of any reason gives a warning against missile attack. In this state shall it also be possible to update SW in the MWS.

R-X : The system state shall power up as Disarmed

R-X : The System state Shall change from Disarmed to Armed when all of the following conditions are met(ANDED):

1. The Safety pin is to be removed before flight.
2. The plane is off ground

R-X : The System state Shall change from Armed to Disarmed when one of the following conditions are met(ORED):

1. The Safety pin is inserted after flight.
2. The plane is off ground



INFO : The Threat Response Subystem : When the AMC receives information about threats that are detected by the MWS, This subsystem will determine the response with respect to automatic semiautomatic or manual dispensing of chaffs and flares according to a Countermeasure program.

R-X : In Systemstate Armed the behaviour of the Thread respose subsystem shall be influenced by the mode (Manuel, Semi automatic, Automatic or Plane on Ground)

R-X: Changing between the modes : Manuel, Semi automatic or Automatic shall be chosen by the position of a selector switch in the cockpit.

R-X: Changing mode to “Plane on Ground” from any state of Manual , Semi automatic or Automatic shall happen when the plane is on ground.

R-X: Changing mode from “Plane on Ground” to any state of Manual , Semi automatic or Automatic shall happen when the plane is off ground and the safety pin is removed. The mode shall be chosen by the position of a selector switch in the cockpit.

LMU: Her skal vi have noget ind omkring hvor vi ellers behandler states og modes.

## 3.2 System capability requirements.

## Engaging / Disengaging The System

R-X : Controlling power on/off, for the dispensing system and the MWS shall be done by a secured switch Mil.Grade.xyz inside the cockpit

INFO : This will power up or down the system to a known state

R-X : When turning on power a maximum of 5 seconds will last before the system is fully operational

R-X : When turning off power a maximum of 2 seconds will last before the system is fully closed down

## The system will detect a threat, decide and react accordingly

INFO: The system will detect a threat using the MWS , compare this to already known threat patterns and act accordingly. With respect to system states.

## Detection of a threat

## Detection of a threat is done by the MWS.

INFO : When the AMC receives information about threats that are detected by the MWS, the kind of threat and the direction (body frame format) is transmitted

## The Threat is processed by the Threat Response Subsystem

INFO :: When the AMC receives information about threats that are detected by the MWS the Threat Response Subsystem is triggered

INFO : About the Threat Response Subsystem. When the AMC receives information about threats that are detected by the MWS, this subsystem will determine the response with respect to automatic semiautomatic or manual dispensing of chaffs and flares according to a Countermeasure program.

## Pattern matching the threat

INFO : A thread pattern is a certain number of threads attacking the aircraft from certain angles

R-X : The Threat Response Subsystem shall be able to store 100 Threat patterns

R-X : All data concerning the Threat patterns shall be handled by the winXYZapplication. This includes programming configuration uploading or downloading to the Threat response system

R-X : When the Threat Response Subsystem automatically chooses a countermeasure program, it shall be done by matching the stored Thread patterns with the actual threat pattern and finding the best match using the mathematical zyx procedure

R-X : All data concerning the mathematical zyx procedure shall be handled by the winXYZapplication. This includes programming configuration uploading or downloading to the Threat response system

## Reaction to the Thread

INFO : Three reactions are relevant :Visible on display, hearable via Audio cue system and automatic chaff flare dispensing.

## The kind of threat and the direction of the threat is displayed

R-X : When the AMC receives information about threats that are detected by the MWS, the kind of threat and the direction (body frame format) shall be displayed in the cockpit within 20 milliseconds from AMC is receiving the threat info

## The kind of threat is announced through the audio cue system in the intercom.

R-X : When the AMC receives information about threats that are detected by the MWS, the cockpit unit shall play an audio cue on the aircrafts audio system.

R-X : when a threat is detected the Audio Cue System shall be signalled to start within 20 milliseconds from AMC is receiving the threat info

R-X : The audio cue played in case of a threat shall be an indication of threat type (e.g. “Missile”), location (e.g. “4 o’clock”) and elevation (e.g. “low”), as specified by the audio queue table *ACTv2*.

## The Countermeassure program

INFO : A Countermeassure Program is a preprogrammed sequence of dispensing chaffs and or flares in certain directions with a certain timing

R-X : When the Threat Response Subsystem is in the manual mode, the threads shall be heard and seen by the pilot but he himself must manually select and execute a Countermeasure program

R-X : When the Threat Response Subsystem is in the Semiautomatic mode a countermeasure program shall be chosen by the system and executed but only upon consent from the pilot

R-X : When the Threat Response Subsystem is in the Automatic mode a countermeasure program shall be chosen by the system and executed

## Other functional requirements

|  |  |
| --- | --- |
| **REQ ID** | **Requirement** |
| FR-12 | The systems shall comply with all F-16 EW standards for EMC and data bus load as specified by the F-16 EW standard *FE16d*. |

## CCU

|  |  |
| --- | --- |
| **REQ ID** | **Requirement** |
| FR-12 | The systems shall comply with all F-16 EW standards for EMC and data bus load as specified by the F-16 EW standard *FE16d*. |
| FR-20 | The ECU shall perform the built in test that is supported by this Government Furnished Equipment (*GFE*). |
| FR-21 | The cockpit unit shall perform an internal built-in test of its internal subsystems and HW, as specified by the F-16 subsystem BIT standard *FBIT12c*. |
| FR-23 | The cockpit unit shall request status information from the ECU every 20ms. |
| FR-24 | The ECU shall report the status information available for this Government Furnished Equipment (*GFE*). |
| FR-26 | The cockpit unit shall play an audio cue on the aircrafts audio system when a threat is detected. |
| FR-27 | The audio cue played in case of a threat shall be an indication of threat type (e.g. “Missile”), location (e.g. “4 o’clock”) and elevation (e.g. “low”), as specified by the audio queue table *ACTv2*. |
| FR-31 | The cockpit unit shall keep all sensitive data in an encrypted format as specified by the DOD sensitive data standard *SDS23v*. |
| FR-32 | The cockpit unit shall erase the decryption key using the DOD data wipe specification *DWS12g*. |

## POD

|  |  |
| --- | --- |
| **REQ ID** | **Requirement** |
| FR-1 | The POD shall contain three dispenser magazine mounts.  INFO: These shall henceforth be named first, second and third. |
| FR-2 | The POD’s first dispenser magazine mount shall physically be located before the second and third dispenser magazine mount relative to the nose of the plane. |
| FR-3 | The POD’s first dispenser magazine mount shall support forward dispensing. |
| FR-4 | The POD’s first dispenser magazine mount shall support two magazines. |
| FR-5 | The POD’s second dispenser magazine mount shall physically be located before the third dispenser magazine mount relative to the nose of the plane. |
| FR-6 | The POD’s second dispenser magazine mount shall support leftwards dispensing. |
| FR-7 | The POD’s second dispenser magazine mount shall support four magazines. |
| FR-8 | The POD’s third dispenser magazine mount shall support downwards dispensing. |
| FR-9 | The POD’s third dispenser magazine mount shall support two magazines. |
| FR-11 | The POD shall comply with all F-16 requirements for aerodynamics and radar reflections as specified by the F-16 POD standard *FP42f*. |
| FR-13 | The POD shall be mounted under the left wing. |
| FR-20 | The ECU shall perform the built in test that is supported by this Government Furnished Equipment (*GFE*). |
| FR-24 | The ECU shall report the status information available for this Government Furnished Equipment (*GFE*). |
| FR-28 | The POD shall include a safety pin that prevents the dispenser from firing. |
| FR-29 | The POD safety pin shall be clearly labelled and accessible by aircraft maintenance crew as specified by the aircraft maintenance manual *AMM32f*. |
| FR-39 | The POD shall supply the status of the following LRUs:   * The Sensors * The ECU   INFO: The Magazines and DSS are not seen as LRUs and also do not have status reporting capabilities.  INFO: It is assumed that the ECU has the ability to deliver this information. |
| FR-44 | The status reported by the POD as a whole shall be:   1. POD internal temperature 2. ECU operational status (OK, ERROR)   INFO: It is assumed that the ECU has the ability to deliver this information.  INFO: It is assumed that the ECU has a temperature sensor inside the POD and is able to deliver its reading on the data bus. |

## Performance requirements

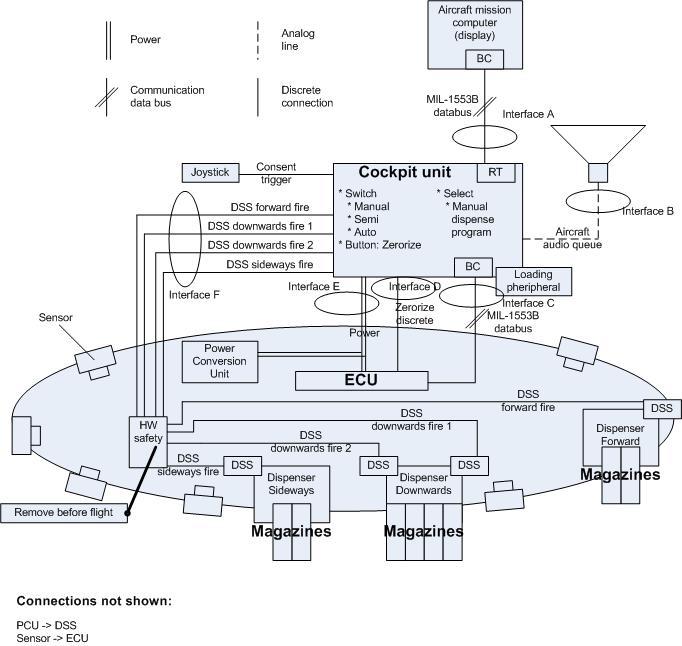
## CCU

|  |  |
| --- | --- |
| **REQ ID** | **Requirement** |
| FR-16 | The cockpit unit shall forward the threat data received from the MWS within 20ms. |
| FR-19 | The cockpit unit shall request the performance of a built in test by the ECU every 15 minutes. |
| FR-22 | The cockpit unit shall forward the built in test results to the aircraft mission computer with a maximum latency of 1 second from receiving the results. |
| FR-25 | The cockpit unit shall forward the status of the individual subsystems and LRUs; ECU, POD and aircraft unit to the aircraft mission computer with a maximum latency of 100ms from receiving the information.  INFO: The Magazines and DSS are not seen as LRUs and also do not have status reporting capabilities. |
| FR-34 | When the erasing of sensitive data procedure is initiated, the cockpit unit shall erase its sensitive data decryption key within 100ms. |

## System external interface requirements.

This paragraph defines the requirements on the interfaces between the system and externals parts.

### 3.3.1 Interface identification and diagrams.



Oversigtstegning der viser de forskellige interfaces mellem Cockpit Control Unit og AMC samt Intercom.

### Interface A (Interface to Aircraft Mission Computer.

This interface shall make it possible to communicate with the AMC. Information will both be from AMC to the system and from the system to the AMC.

## CCU

|  |  |
| --- | --- |
| **REQ ID** | **Requirement** |
| FR-15a | The cockpit unit shall communicate with the aircraft mission computer via the planes main MIL-1553B data bus. |
| FR-15b | The cockpit unit shall forward all threat data received from the MWS to the aircraft mission computer in body frame format. |
| FR-17 | The cockpit unit shall use the NATO dispenser threat format *DF14b* to forward threat data to the aircraft mission computer. |
| FR-30 | The cockpit unit shall receive an input discrete which when set to logic 0 shall trigger the erasing of sensitive data procedure. |
| FR-47 | The cockpit unit shall include a consent button to use with semi-automatic dispensing. |

## POD

|  |  |
| --- | --- |
| **REQ ID** | **Requirement** |
| FR-10 | The POD shall support standard NATO dispenser magazines type *DM30p*. |
| FR-14 | The POD shall be mounted by two T-hooks as specified by the F-16 POD mounting standard *PM11b*. |

Skal interface i vingen mellem pod og kabler fra CCU’en beskrives her eller under interne interfaces??.

### 3.3.x (Project-unique identifier of interface).

3.3.2 Beskrivelse af og krav til interface mellem CCU og AMC.

3.3.3 Beskrivelse af og krav til interface mellem CCU og Intercom.

This paragraph (beginning with 3.3.2) shall identify

a system external interface by project-unique identifier, shall briefly identify the interfacing entities,

and shall be divided into subparagraphs as needed to state the requirements imposed on the

system to achieve the interface. Interface characteristics of the other entities involved in the

interface shall be stated as assumptions or as "When [the entity not covered] does this, the

system shall...," not as requirements on the other entities. This paragraph may reference other

documents (such as data dictionaries, standards for communication protocols, and standards for

user interfaces) in place of stating the information here. The requirements shall include the

following, as applicable, presented in any order suited to the requirements, and shall note any

differences in these characteristics from the point of view of the interfacing entities (such as

different expectations about the size, frequency, or other characteristics of data elements):

a. Priority that the system must assign the interface

b. Requirements on the type of interface (such as real-time data transfer, storage-andretrieval

of data, etc.) to be implemented

c. Required characteristics of individual data elements that the system must provide, store,

send, access, receive, etc., such as:

1) Names/identifiers

a) Project-unique identifier

b) Non-technical (natural-language) name

c) DoD standard data element name

d) Technical name (e.g., variable or field name in code or database)

e) Abbreviation or synonymous names

2) Data type (alphanumeric, integer, etc.)

3) Size and format (such as length and punctuation of a character string)

4) Units of measurement (such as meters, dollars, nanoseconds)

5) Range or enumeration of possible values (such as 0-99)

6) Accuracy (how correct) and precision (number of significant digits)

7) Priority, timing, frequency, volume, sequencing, and other constraints, such as whether

the data element may be updated and whether business rules apply

8) Security and privacy constraints

9) Sources (setting/sending entities) and recipients (using/receiving entities)

d. Required characteristics of data element assemblies (records, messages, files, arrays,

displays, reports, etc.) that the system must provide, store, send, access, receive, etc.,

such as:

1) Names/identifiers

a) Project-unique identifier

b) Non-technical (natural language) name

c) Technical name (e.g., record or data structure name in code or database)

d) Abbreviations or synonymous names

2) Data elements in the assembly and their structure (number, order, grouping)

3) Medium (such as disk) and structure of data elements/assemblies on the medium

4) Visual and auditory characteristics of displays and other outputs (such as colors,

layouts, fonts, icons and other display elements, beeps, lights)

5) Relationships among assemblies, such as sorting/access characteristics

6) Priority, timing, frequency, volume, sequencing, and other constraints, such as whether

the assembly may be updated and whether business rules apply

7) Security and privacy constraints

8) Sources (setting/sending entities) and recipients (using/receiving entities)

e. Required characteristics of communication methods that the system must use for the

interface, such as:

1) Project-unique identifier(s)

2) Communication links/bands/frequencies/media and their characteristics

3) Message formatting

4) Flow control (such as sequence numbering and buffer allocation)

5) Data transfer rate, whether periodic/aperiodic, and interval between transfers

6) Routing, addressing, and naming conventions

7) Transmission services, including priority and grade

8) Safety/security/privacy considerations, such as encryption, user authentication,

compartmentalization, and auditing

f. Required characteristics of protocols the system must use for the interface, such as:

1) Project-unique identifier(s)

2) Priority/layer of the protocol

3) Packeting, including fragmentation and reassembly, routing, and addressing

4) Legality checks, error control, and recovery procedures

5) Synchronization, including connection establishment, maintenance, termination

6) Status, identification, and any other reporting features

g. Other required characteristics, such as physical compatibility of the interfacing entities

(dimensions, tolerances, loads, plug compatibility, etc.), voltages, etc.

## 3.4 System internal interface requirements.

Oversigttegning der viser interfaces mellem CCU og MWS/ECU, samt CCU og DSS’er.

|  |  |
| --- | --- |
| **REQ ID** | **Requirement** |
| FR-18a | The ECU shall communicate with the cockpit unit via a dedicated *MIL-1553B* data bus. |
| FR-18b | The ECU shall forward threat data to the cockpit unit in NATO dispenser threat format *DF14b*. |
| FR-46 | The cockpit unit shall display the LRU status received from the POD as indicated by the LRU status display specification. |
| FR-45 | The POD LRU status shall be reported in the POD status format specified under interfaces.  INFO: This interface is specified by the ECU (GFE). |

## 3.5 System internal data requirements.

Interface CCU og MWS/ECU.

Interface CCU og DSS’er.

## 3.6 Adaptation requirements.

Ikke relevant for os

## 3.7 Safety requirements.

POD safety PIN

## 3.8 Security and privacy requirements.

R-X: The system shall be able to erase sensitive data upon input from a discrete signal from aircraft.

R-X: The cockpit unit shall keep all sensitive data in an encrypted format as specified by the DOD sensitive data standard SDS23v.

R-X: The cockpit unit shall erase the decryption key using the DOD data wipe specification DWS12g.

R-X: When the erasing of sensitive data procedure is initiated, the POD erase sensitive data discrete shall be set within 10ms.

R-X: When the erasing of sensitive data procedure is initiated, the cockpit unit shall erase its sensitive data decryption key within 100ms.

Krav og beskrivelse af zeroize signal/mulighed.

## 3.9 System environment requirements.

This paragraph shall specify the environment in which the system must operate.

### Temperature.

R-x: The pod structure shall be operational at temperatures of 95 ̊C on the outer skin and of 102 ̊C on the leading edge for 25 minutes.

R-x: The pod structure shall be operational at temperatures of 134 ̊C on the outer skin and of 151 ̊C on the leading edge for 3 minutes.

R-x: The maximum temperature inside the pod shall not be more than 70 ̊C during and test and under normal operation.

### Acceleration.

R-x: The pod structure shall be without any failures after being exposed to a steady state acceleration of 5g fore.

R-x: The pod structure shall be without any failures after being exposed to a steady state acceleration of 2.5g aft.

R-x: The pod structure shall be without any failures after being exposed to a steady state acceleration of 25g up.

R-x: The pod structure shall be without any failures after being exposed to a steady state acceleration of 11g down.

Temperatur

G-påvirkninger

## 3.10 Computer resource requirements.

### 3.10.1 Computer hardware requirements.

### 3.10.2 Computer hardware resource utilization requirements.

### 3.10.3 Computer software requirements.

### 3.10.4 Computer communications requirements.

## 3.11 System quality factors.

## 3.12 Design and construction constraints.

### Weight.

R-x: The total weight of pod shall not exceed 270 kg.

R-x: Weight of complete MWS is 18,2kg.

### Mounting.

R-x: The pod shall be mounted on the aircraft wing with standard T-hooks spaced by 13 inches.

R-x: The pod shall be mounted on the left-hand wing.

### MWS.

R-x: MWS will be provided as a Government Furnished Equipment.

R-x: MWS will physically be mounted by Company F.

### Power.

R-x: Power consumption of the pod shall not exceed 700W.

R-x: Power to the pod is 115VAC 400Hz.

R-x: The MWS requires maximum 85W from a 28VDC power source and a maximum of 100W from a 115VAC 400Hz power source.

R-x: The power required to ignite a payload is up to 126W for a period of up to 20ms.

### Coverage against missile threats.

R-x: The six sensors shall be located to cover all angles which are not shaded by the aircraft.

Weight.

Mounting (Under left wing, T-hooks 13” osv.)

Use of MWS provided as GFE

Optimal coverage against Missi…

This paragraph shall specify the requirements, if any,

that constrain the design and construction of the system. For hardware-software systems, this

paragraph shall include the physical requirements imposed on the system. These requirements

may be specified by reference to appropriate commercial or military standards and specifications.

Examples include requirements concerning:

a. Use of a particular system architecture or requirements on the architecture, such as

required subsystems; use of standard, military, or existing components; or use of

Government/acquirer-furnished property (equipment, information, or software)

b. Use of particular design or construction standards; use of particular data standards; use

of a particular programming language; workmanship requirements and production

techniques

c. Physical characteristics of the system (such as weight limits, dimensional limits, color,

protective coatings); interchangeability of parts; ability to be transported from one location

to another; ability to be carried or set up by one, or a given number of, persons

d. Materials that can and cannot be used; requirements on the handling of toxic materials;

limits on the electromagnetic radiation that the system is permitted to generate

e. Use of nameplates, part marking, serial and lot number marking, and other identifying

markings

f. Flexibility and expandability that must be provided to support anticipated areas of growth

or changes in technology, threat, or mission

## 3.13 Personnel-related requirements.

## 3.14 Training-related requirements.

## 3.15 Logistics-related requirements.

## 3.16 Other requirements.

## 3.17 Packaging requirements.

## 3.18 Precedence and criticality of requirements.

# 4. Qualification provisions.

|  |  |  |
| --- | --- | --- |
| **REQ ID** | **Test description** | **Qualification method** |
| FR-1 | Inspect that the requested dispenser mounts are located on the POD | Inspection |
| FR-2 | Inspect that the first dispenser mount is mounted correctly on the POD. | Inspection |
| FR-3 | Inspect that the first dispenser mount is placed correctly on the POD. | Inspection |
| FR-4 | Inspect that the first dispenser mount can hold 2 magazines. | Inspection |
| FR-5 | Inspect that the second dispenser mount is placed correctly on the POD. | Inspection |
| FR-6 | Inspect that the second dispenser mount is placed correctly on the POD. | Inspection |
| FR-7 | Inspect that the second dispenser mount can hold 4 magazines. | Inspection |
| FR-8 | Inspect that the third dispenser mount is placed correctly on the POD. | Inspection |
| FR-9 | Inspect that the third dispenser mount can hold 2 magazines. | Inspection |
| FR-10 | Inspect that the dispenser mounts support the correct magazine type. | Inspection |
| FR-11 | The POD design and implementation must be verified by a certified third party F-16 POD certifying authority. | Inspection and verification |
| FR-12 | The POD design and implementation must be verified by a certified third party F-16 EW certifying authority. | Inspection and verification |
| FR-13 | Inspect that the POD is mounted correctly. | Inspection |
| FR-14 | Inspect that the POD is mounted correctly. | Inspection |
| FR-15 | Inspect the code and run simulation with a MWS simulator to verify the inertial format to body-frame format conversion. | Code inspection and test |
| FR-16 | Run simulation with a MWS simulator to verify the delay from cockpit unit reception to availability on aircraft mission bus. A simulator of the aircraft mission bus must be set up to poll the cockpit unit as fast as possible. | Test |
| FR-17 | Inspect the code and run simulation with a MWS simulator to verify the threat data format. | Code inspection and test |
| FR-18a | Inspect that the MWS uses a dedicated MIL-1553B data bus. | Inspection |
| FR-18b | Inspect the code and run simulation with a MWS simulator to verify the threat data format. | Code inspection and test |
| FR-19 | Run simulation with a MWS simulator to verify the BIT request interval. | Test |
| FR-20 | Inspect that the supported BIT is requested and run simulation with a MWS simulator to verify the BIT responses. | Code inspection and test |
| FR-21 | Inspect the internal BIT code and run test with test setup (faulty HW) to verify BIT responses. | Code inspection and test |
| FR-22 | Run simulation with a MWS simulator to verify the maximum delay. A simulator of the aircraft mission bus must be set up to poll the cockpit unit as fast as possible. | Test |
| FR-23 | Inspect the status request code time and run test with MWS simulator to verify status request interval. | Code inspection and test |
| FR-24 | Verify that all available status information is placed on the MWS to cockpit unit data bus. | Test |
| FR-25 | Run simulation with a MWS simulator to verify the maximum delay. A simulator of the aircraft mission bus must be set up to poll the cockpit unit as fast as possible. | Test |
| FR-26 | Run simulation with a MWS simulator to verify an audio cue is played. | Test |
| FR-27 | Run simulation with a MWS simulator to verify the correct audio cues are played. | Test |
| FR-28 | Verify that a removable pin exists and that firing is disabled when the pin is present in the POD. | Inspection and test |
| FR-29 | Verify pin design according to standard | Inspection |
| FR-30 | Verify that zerorize button is present on cockpit unit. | Inspection |
| FR-31 | Verify the DOD standard is met with respect to sensitive data storage. | Code inspection |
| FR-32 | Verify the DOD standard is met with respect to decryption key erase. | Code inspection |
| FR-33 | Verify that the POD erase discrete is set within 10ms of depressing the zerorize button. | Test |
| FR-34 | Show that it is probable that the key will be wiped within 100ms. | Code inspection |
| FR-35 | Verify the DOD standard is met with respect to sensitive data storage. | Code inspection |
| FR-36 | Verify that the POD erases its sensitive data decryption key when the POD erase discrete is set. | Test |
| FR-37 | Verify the DOD standard is met with respect to decryption key erase. | Code inspection |
| FR-38 | Show that it is probable that the key will be wiped within 100ms. | Code inspection |
| FR-39 | Verify with MWS simulator that the required status is available and correct. | Test |
| FR-44 | Verify with MWS simulator that the required status is available and correct. | Test |
| FR-45 | Verify with MWS simulator that the required status is available and correct. | Test |
| 46 | Controlling power on/off, for the dispensing system and the MWS shall be done by a secured switch Mil.Grade.xyz inside the cockpit | Observe that the power led in the MWS is turned on and off by controlling the switch in the cockpit |
| 46.1 | When turning on power a maximum of 5 seconds will last before the system is fully operational | Using an oscilloscope and checking the delay from turning on the switch to the “operational led” is on |
|  | When turning off power a maximum of 2 seconds will last before the system is fully closed down | Using an oscilloscope and checking the delay from turning off the switch to the “operational led” is off |
|  | When the AMC receives information about threats that are detected by the MWS, the kind of threat and the direction (body frame format) shall be displayed in the cockpit ,( within 20 milliseconds from AMC is receiving threat info) | Tested on status LEDs. On AMC and MWS using the threadsimulation. |
|  | When the AMC receives information about threats that are detected by the MWS the Threat Response Subsystem shall be triggered ( within 20 milliseconds from AMC is receiving threat info) | Tested on status LEDs. On AMC and MWS using the threadsimulation |
|  | The Threat Response Subsystem shall be in one of three modes : Manual, Semiautomatic, Automatic. The mode shall be chosen by the position of a selector switch | Test that the status LED’s reflect the setting of the appropriate selector switch |
|  | When the Threat Response Subsystem is in the manual mode, the threads shall be heard and seen by the pilot but he himself must select and execute a Countermeasure program | Tested by using the Threat simulator mode of the MWS |
|  | When the Threat Response Subsystem is in the Semiautomatic mode a countermeasure program shall be chosen by the system and executed but only upon consent from the pilot | Tested by using the Threat simulator mode of the MWS |
|  | When the Threat Response Subsystem is in the Automatic mode a countermeasure program shall be chosen by the system and executed | Tested by using the Threat simulator mode of the MWS |
|  | The Threat Response Subsystem shall be able to store 100 countermeasure programs, each of these are configured as being best suited for a given Threat pattern | Tested by using the winXYZapplication to write and read 100 countermeassure programs, and afterwards check by comparision to the originals |
|  | The Threat Response Subsystem shall be able to store 100 Threat patterns | Tested by using the winXYZapplication to write and read 100 Threadpatterns, and afterwards check by comparision to the originals |
|  | When the Threat Response Subsystem chooses a countermeasure program, it shall be done by matching the stored Thread patterns with the actual threat pattern and finding the best match using the mathematical zyx procedure. | Tested by using the Threat simulator mode of the MWS |

# 5. Requirements traceability.

Alle Trace Ids refer to the document *TC1*

|  |  |  |  |
| --- | --- | --- | --- |
| **REQ ID** | **Requirement (short)** | **Trace ID** | **Reference** |
| FR-1 |  | UR-2 |  |
| FR-2 |  | UR-2 |  |
| FR-3 |  | UR-2 |  |
| FR-4 |  | UR-1 |  |
| FR-5 |  | UR-2 |  |
| FR-6 |  | UR-2 |  |
| FR-7 |  | UR-1 |  |
| FR-8 |  | UR-2 |  |
| FR-9 |  | UR-1 |  |
| FR-10 |  | UR-1 |  |
| FR-11 |  | UR-3 |  |
| FR-12 |  | UR-3 |  |
| FR-13 |  | UR-4 |  |
| FR-14 |  | UR-4 |  |
| FR-15 |  | UR-5 |  |
| FR-16 |  | UR-5 |  |
| FR-17 |  | UR-5 |  |
| FR-18a |  | UR-5 |  |
| FR-18b |  | UR-5 |  |
| FR-19 |  | UR-6 |  |
| FR-20 |  | UR-6 |  |
| FR-21 |  | UR-6 |  |
| FR-22 |  | UR-6 |  |
| FR-23 |  | UR-6 |  |
| FR-24 |  | UR-6 |  |
| FR-25 |  | UR-6 |  |
| FR-26 |  | UR-7 |  |
| FR-27 |  | UR-7 |  |
| FR-28 |  | UR-8 |  |
| FR-29 |  | UR-8 |  |
| FR-30 |  | UR-9 |  |
| FR-31 |  | UR-9 |  |
| FR-32 |  | UR-9 |  |
| FR-33 |  | UR-9 |  |
| FR-34 |  | UR-9 |  |
| FR-35 |  | UR-9 |  |
| FR-36 |  | UR-9 |  |
| FR-37 |  | UR-9 |  |
| FR-38 |  | UR-9 |  |
| FR-39 |  | UR-10 |  |
| FR-44 |  | UR-10 |  |
| FR-45 |  | UR-10 |  |
|  |  |  |  |
|  |  |  |  |

# Notes.

## Glossery

|  |  |
| --- | --- |
| Body frame format | Direction of aircraft relative to flight direction |

## Abbriviations

|  |  |
| --- | --- |
| UR | User Requirement |
| FR | Functional Requirement |
| GFE | Government Furnished Equipment |
| MWS | Missile Warning System |
| CCU | Cockpit Control Unit |
| BC | Bus Controller |
| RT | Remote Terminal |
| DSS | Digital Sequencer Switches |
| ECU | Electronic Control Unit |
| PCU | Power Conversion Unit |
| AMC | Aircraft Mission Computer |
| DOD |  |
| EMC |  |
| LRU |  |

# A. Appendixes.

Appendix A:

Her kan Terma Case RTM.XLS placers.

**Explanation:**

|  |  |
| --- | --- |
| Threat Response Subystem | When the AMC receives information about threats that are detected by the MWS, This subsystem will determine the response with respect to automatic semiautomatic or manual dispensing of chaffs and flares according to a Countermeasure program. |
| Countermeasure program | A preprogrammed sequence of dispensing chaffs and or flares in certain directions with a certain timing |
| Thread pattern | A thread pattern is a certain number of threads attacking the aircraft from certain angles |

|  |  |  |  |
| --- | --- | --- | --- |
| Requirement continued | TestMethod | Trace | Completion |
| 1. Controlling power on/off, for the dispensing system and the MWS shall be done by a secured switch Mil.Grade.xyz inside the cockpit | Observe that the power led in the MWS is turned on and off by controlling the switch in the cockpit | UR-11 | TBR |
| * 1. When turning on power a maximum of 5 seconds will last before the system is fully operational | Using an oscilloscope and checking the delay from turning on the switch to the “operational led” is on | UR-11 indirect | TBR |
| * 1. When turning off power a maximum of 2 seconds will last before the system is fully closed down | Using an oscilloscope and checking the delay from turning off the switch to the “operational led” is off | UR-11  Indirect | TBR |
| 1. When the AMC receives information about threats that are detected by the MWS, the kind of threat and the direction (body frame format) shall be displayed in the cockpit ,( within 20 milliseconds from AMC is receiving threat info) | Test ???? | UR7 | TBR |
| 1. When the AMC receives information about threats that are detected by the MWS the Threat Response Subsystem shall be triggered ( within 20 milliseconds from AMC is receiving threat info) |  |  |  |
| 1. The Threat Response Subsystem shall be in one of three modes : Manual, Semiautomatic, Automatic. The mode shall be chosen by the position of a selector switch | Test that the status LED’s reflect the setting of the appropriate selector switch | UR12 | TBR |
| * 1. When the Threat Response Subsystem is in the manual mode, the threads shall be heard and seen by the pilot but he himself must select and execute a Countermeasure program | Tested by using the Threat simulator mode of the MWS | UR13 | TBR |
| * 1. When the Threat Response Subsystem is in the Semiautomatic mode a countermeasure program shall be chosen by the system and executed but only upon consent from the pilot | Tested by using the Threat simulator mode of the MWS | UR14 | TBR |
| * 1. When the Threat Response Subsystem is in the Automatic mode a countermeasure program shall be chosen by the system and executed | Tested by using the Threat simulator mode of the MWS | UR15 | TBR |
| 1. The Threat Response Subsystem shall be able to store 100 countermeasure programs, each of these are configured as being best suited for a given Threat pattern    1. All data concerning the countermeasure programs shall be handled by the winXYZapplication. This includes programming configuration uploading or downloading to the Threat response system |  | UR21 |  |
| 1. The Threat Response Subsystem shall be able to store 100 Threat patterns    1. All data concerning the Threat patterns shall be handled by the winXYZapplication. This includes programming configuration uploading or downloading to the Threat response system |  | UR21 |  |
| 1. When the Threat Response Subsystem chooses a countermeasure program, it shall be done by matching the stored Thread patterns with the actual threat pattern and finding the best match using the mathematical zyx procedure.    1. All data concerning the mathematical zyx procedure shall be handled by the winXYZapplication. This includes programming configuration uploading or downloading to the Threat response system |  | UR15 |  |