**Self Protecting Suite for F-16**

**System Design Describtion**

Case study made at IHA September 2010

System Engineering

Company F

Kaj N. Nielsen, Kenneth Pihl, Anders A. Poder, Lars Munch

**Index.**

[1. Scope. 3](#_Toc274167982)

[1.1 Identification. 3](#_Toc274167983)

[1.2 System overview. 3](#_Toc274167984)

[1.3 Document overview. 5](#_Toc274167985)

[2. Referenced documents. 5](#_Toc274167986)

[3. System-wide design decisions. 5](#_Toc274167987)

[3.1 Actors 5](#_Toc274167988)

[3.2 Power On/Off 5](#_Toc274167989)

[3.3 Mode select 6](#_Toc274167990)

[3.4 Zerorize 6](#_Toc274167991)

[3.5 Internal Test 6](#_Toc274167992)

[3.6 Thread detected 6](#_Toc274167993)

[3.7 Program update 6](#_Toc274167994)

[3.8 Plane on ground 6](#_Toc274167995)

[4. System architectural design. 7](#_Toc274167996)

[4.1 System components. 7](#_Toc274167997)

[4.2 Concept of execution. 8](#_Toc274167998)

[4.3 Interface design. 8](#_Toc274167999)

[5. Requirements traceability. 10](#_Toc274168000)

[6. Notes. 10](#_Toc274168001)

[7. A. Appendixes. 10](#_Toc274168002)

[8. Niv 1 11](#_Toc274168003)

[8.1 Niv 2 11](#_Toc274168004)

**History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Description** | **Name** | **Version** |
| 28/9 2010 | Document setup made | LMU | 0.1 |
| 5/10 2010 | Paragraph 3 started | KPI | 0.2 |
| 6/10 2010 | Added Power and no selector descriptor | LMU | 0.3 |
|  |  |  |  |
|  |  |  |  |

# Scope.

This section shall be divided into the following paragraphs.

## 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.

This paragraph shall contain a full identification of the system to which this

document applies, including, as applicable, identification number(s), title(s), abbreviation(s),

version number(s), and release number(s).

## 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.



Figure 1

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.

This paragraph shall briefly state the purpose of the system to which

this document applies. It shall describe the general nature of the system; summarize the history

of system development, operation, and maintenance; identify the project sponsor, acquirer, user,

developer, and support agencies; identify current and planned operating sites; and list other

relevant documents.

## Document overview.

This paragraph shall summarize the purpose and contents of this

document and shall describe any security or privacy considerations associated with its use.

# Referenced documents.

This section shall list the number, title, revision, and date of all

documents referenced in this document. This section shall also identify the source for all

documents not available through normal Government stocking activities.

# System-wide design decisions.

## Actors

This paragraph lists all actors who will be using the system. An actor can be anything which creates an input event to the system e.g. a person, a machine or a signal. In the list actors are preceded with the stereotype <*Actor*> and then followed by a brief description.

<*Actor*> **Pilot**.

The pilot will use the system from an operational point of view.

<*Actor*> **Service**.

Service is service personnel who maintains the system, perform test on the system etc.

<*Actor*> **ECU**.

The Electronic Control Unit is an electronic device providing information from the pod.

<*Actor*> **AMC**.

The Aircraft Mission Computer provides info from the aircraft system.

<*Actor*> **Zerorize**.

Zerorize is an electrical signal.

<*Actor*> **System**.

The system itself can initiate actions.

<*Actor*> **TestSystem.**

The test system can program, download configuration files and perform test sequences.

## Power On/Off

Actors: <*Actor*> **Pilot;** <*Actor*> **Service**

When the CCU is powered on it will initialize itself and run a selftest. After initialization and selftest it will power up the rest of the system and then enter standby state.

If plane on ground signal is off, the state will change to armed state.

## Mode select

<*Actor*> **Pilot;** <*Actor*> **Service**

Mode select has only effect in armed state. When state changes from not armed to armed the system will enter an armed internal state (manual, semi automatic, automatic) depending on the position of mode select.

## Zerorize

<*Actor*> **Zerorize**.

This is handled under security.

## Internal Test

<*Actor*> **Service**, <*Actor*> **System**.

The internal test is initiated by the system every 15 minutes. The test can also be initiated by ground personnel.

## Thread detected

<*Actor*> **ECU**.

When the system is acknowledge about a missile attack from the MWS, the system will display the direction of the thread in body frame format on the AMC within 20ms and initiate an audible sound on the intercom within 20ms.

## Program update

<*Actor*> **TestSystem;** <*Actor*> **Service**

The system software can be updated via a connector on the CCU. When the connecter is plugged in the system can be reset by an external system. The external system can load new software or a new configuration file into the system.

## Plane on ground

<*Actor*> **AMC**

When the aircraft is on ground the plane on ground signal is active low so that the system cannot be armed by a defect wire.

## Power consumption 28Vdc in pod

The PCU used to convert from 115Vac to 28Vdc in the pod can as maximum deliver 250W. At the same time UR-20 in the doc ref TBD required dispensing 2 payloads at the same time, but looking on the power analyse below:

Dispensing 2 payloads at the same time.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Number | Consumption 28Vdc [W] | Consumption 115Vac [W] | Total for components@28Vdc [W] | Total for components@115Vac [W] |
| ECU | 1 | 85 | 100 | 85 | 100 |
| DSS's | 4 | 3 | 0 | 12 | 0 |
| Dispensing | 2 | 126 | 0 | 252 | 0 |
| Total |  |  |  | **349** | 100 |
|  |  |  |  |  |  |
| Total Power consumption from 28Vdc and 115Vac | | | |  | 449 |

Shows that the power consumption on the 28Vdc in the pod is above 250W.

When reducing to only dispense 1 payload each time reduce power consumption to:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Number | Consumption 28Vdc [W] | Consumption 115Vac [W] | Total for components@28Vdc [W] | Total for components@115Vac [W] |
| ECU | 1 | 85 | 100 | 85 | 100 |
| DSS's | 4 | 3 | 0 | 12 | 0 |
| Dispensing | 1 | 126 | 0 | 126 | 0 |
| Total |  |  |  | **223** | 100 |
|  |  |  |  |  |  |
| Total Power consumption from 28Vdc and 115Vac | | | |  | 323 |

223W is well below the maximum of 250W.

UR-20 was by agreement with Terma at SRR meeting at IHA changed to SR-53 in SRD, which says that the system shall be able to dispense 2 payloads in 40msec. By changing it to this requirement reduced the power use on the 28Vdc to 223W, well below the 250W.

## Magazine selector

Each DSS can control 2 magazines and it is possible to add a control line that could select between the 2 magazines. But there are no requirements on this part of the system, so the system design sketched below show no selector for selecting magazine 1 or 2. The decision is to leave out the selector signal and the reasons for leaving out the selector signal are:

* No requirements state anything about the ability the select magazine 1 or 2.
* No requirements require that only Chaffs or flares shall be dispensed.
* Leaving out the selector make it a more simple system with less timing issues.

So when a DSS get the order to dispense it will start with the first payload in magazine 1, then the second one and it will continue so until every payloads in magazine 1 is used. After all payloads in magazine 1 are used then it will dispense the first payload in magazine 2 and continue so until the last payload in magazine 2 is used.



## Safety

To prevent that chaffs or flares can be fired at times where it can be dangerous to other users, ground personal and other people or things in the surrounding a hardware safety interlock is build into the system. This safety interlock prevent that the DSS’s get a firing signal for any chaffs or flares as long as the safety interlock is activated. Further more the CCU is always monitoring the “Plane On Ground” signal which is received as data on the bus from the AMC and as long this signal is logical high, indicating the plane is not in the air the CCU may not give a signal for firing chaffs or flares even though the MWS gives a missile warning.

## Security

For security reasons the CCU is monitoring a zeroize signal from the aircraft if this signal goes logical high the self protection suite shall erase sensitive data in the system. If the signal goes to a high level the CCU will send a zeroize signal to the ECU in the MWS to start the erasure of sensitive data there and also start to erase its own sensitive data.

This section shall be divided into paragraphs as needed to

present system-wide design decisions, that is, decisions about the system’s behavioral design

(how it will behave, from a user’s point of view, in meeting its requirements, ignoring internal

implementation) and other decisions affecting the selection and design of system components.

If all such decisions are explicit in the requirements or are deferred to the design of the system

components, this section shall so state. Design decisions that respond to requirements

designated critical, such as those for safety, security, or privacy, shall be placed in separate

subparagraphs. If a design decision depends upon system states or modes, this dependency

shall be indicated. Design conventions needed to understand the design shall be presented or

referenced. Examples of system-wide design decisions are the following:

a. Design decisions regarding inputs the system will accept and outputs it will produce,

including interfaces with other systems, configuration items, and users (4.3.x of this DID

identifies topics to be considered in this description). If part or all of this information is

given in Interface Design Descriptions (IDDs), they may be referenced.

b. Design decisions on system behavior in response to each input or condition, including

actions the system will perform, response times and other performance characteristics,

description of physical systems modeled, selected equations/algorithms/rules, and

handling of unallowed inputs or conditions.

c. Design decisions on how system databases/data files will appear to the user (4.3.x of this

DID identifies topics to be considered in this description). If part or all of this information

is given in Database Design Descriptions (DBDDs), they may be referenced.

d. Selected approach to meeting safety, security, and privacy requirements.

e. Design and construction choices for hardware or hardware-software systems, such as

physical size, color, shape, weight, materials, and markings.

f. Other system-wide design decisions made in response to requirements, such as selected

approach to providing required flexibility, availability, and maintainability.

# System architectural design.

This section shall be divided into the following paragraphs to

describe the system architectural design. If part or all of the design depends upon system states

or modes, this dependency shall be indicated. If design information falls into more than one

paragraph, it may be presented once and referenced from the other paragraphs. Design

conventions needed to understand the design shall be presented or referenced.

Note: For brevity, this section is written in terms of organizing a system directly into Hardware

Configuration Items (HWCIs), Computer Software Configuration Items (CSCIs), and manual

operations, but should be interpreted to cover organizing a system into subsystems,

organizing a subsystem into HWCIs, CSCIs, and manual operations, or other variations as

appropriate.

## System components.



This paragraph shall:

a. Identify the components of the system (HWCIs, CSCIs, and manual operations). Each

component shall be assigned a project-unique identifier. Note: a database may be

treated as a CSCI or as part of a CSCI.

b. Show the static (such as "consists of") relationship(s) of the components. Multiple

relationships may be presented, depending on the selected design methodology.

c. State the purpose of each component and identify the system requirements and systemwide

design decisions allocated to it. (Alternatively, the allocation of requirements may

be provided in 5.a.)

d. Identify each component’s development status/type, if known (such as new development,

existing component to be reused as is, existing design to be reused as is, existing design

or component to be reengineered, component to be developed for reuse, component

planned for Build N, etc.) For existing design or components, the description shall provide

identifying information, such as name, version, documentation references, location, etc.

e. For each computer system or other aggregate of computer hardware resources identified

for use in the system, describe its computer hardware resources (such as processors,

memory, input/output devices, auxiliary storage, and communications/network equipment).

Each description shall, as applicable, identify the configuration items that will use the

resource, describe the allocation of resource utilization to each CSCI that will use the

resource (for example, 20% of the resource’s capacity allocated to CSCI 1, 30% to CSCI

2), describe the conditions under which utilization will be measured, and describe the

characteristics of the resource:

1) Descriptions of computer processors shall include, as applicable, manufacturer name

and model number, processor speed/capacity, identification of instruction set

architecture, applicable compiler(s), word size (number of bits in each computer word),

character set standard (such as ASCII, EBCDIC), and interrupt capabilities.

2) Descriptions of memory shall include, as applicable, manufacturer name and model

number and memory size, type, speed, and configuration (such as 256K cache

memory, 16MB RAM (4MB x 4)).

3) Descriptions of input/output devices shall include, as applicable, manufacturer name

and model number, type of device, and device speed/capacity.

4) Descriptions of auxiliary storage shall include, as applicable, manufacturer name and

model number, type of storage, amount of installed storage, and storage speed.

5) Descriptions of communications/network equipment, such as modems, network

interface cards, hubs, gateways, cabling, high speed data lines, or aggregates of these

or other components, shall include, as applicable, manufacturer name and model

number, data transfer rates/capacities, network topologies, transmission techniques,

and protocols used.

6) Each description shall also include, as applicable, growth capabilities, diagnostic

capabilities, and any additional hardware capabilities relevant to the description.

f. Present a specification tree for the system, that is, a diagram that identifies and shows the

relationships among the planned specifications for the system components.

## Concept of execution.

This paragraph shall describe the concept of execution among the

system components. It shall include diagrams and descriptions showing the dynamic relationship

of the components, that is, how they will interact during system operation, including, as applicable,

flow of execution control, data flow, dynamically controlled sequencing, state transition diagrams,

timing diagrams, priorities among components, handling of interrupts, timing/sequencing

relationships, exception handling, concurrent execution, dynamic allocation/deallocation, dynamic

creation/deletion of objects, processes, tasks, and other aspects of dynamic behavior.

## Interface design.

This paragraph shall be divided into the following subparagraphs to

describe the interface characteristics of the system components. It shall include both interfaces

among the components and their interfaces with external entities such as other systems,

configuration items, and users. Note: There is no requirement for these interfaces to be

completely designed at this level; this paragraph is provided to allow the recording of interface

design decisions made as part of system architectural design. If part or all of this information is

contained in Interface Design Descriptions (IDDs) or elsewhere, these sources may be

referenced.

### Interface identification and diagrams.

The system has a number interfaces, some internal, some external, some mecanical and some are software interfaces. Below is a sketch showing some the interfaces. The mechanical interface used to mount the pod on the wing and software interfaces are not shown here.



Figure TBD - Interface A, E, F G and H are interfaces to external parts/systems.

This paragraph shall state the project-unique

identifier assigned to each interface and shall identify the interfacing entities (systems,

configuration items, users, etc.) by name, number, version, and documentation references, as

applicable. The identification shall state which entities have fixed interface characteristics (and

therefore impose interface requirements on interfacing entities) and which are being developed

or modified (thus having interface requirements imposed on them). One or more interface

diagrams shall be provided, as appropriate, to depict the interfaces.

### Interface A (CCU to Aircraft Intercom).

To interface the Cockpit Control Unit to the aircraft intercom system the interface will follow the interface described in audio interface for intercom in the F16: FAII-34G.

### Interface B (CCU to Safety Switch).

Between the cockpit control unit and the pod there are 6 discrete wires, used for various signals:

* 4 of them for controlling the firing chaffs and flares using the 4 DSS’. Logical high is firing command. Pins used:
  + No 1: DSS Forward fire
  + No 2: DSS Downward fire 1
  + No 3: DSS Downward fire 2
  + No 4: DSS Backward fire
* 1 for controlling the power switch in pod. Logical High level Power Switch ON
  + No 5: Power Switch
* 1 is a spare wire.
  + No 6: Spare

At the Cockpit control unit is used an EDWC7f connector for the discrete wires, the same connector is used at the pod.

### Interface C (CCUto Power Switch in pod).

To control the power in the pod there is a controllable power switch in the pod. Through interface C this control signal is feed from Cockpit Control Unit to the power switch. Connections, connector and levels are described in [Interface B (Cockpit Control Unit to Safety Switch).](#_Interface_B_(Cockpit) as the two interfaces use the same connector.

### Interface D (CCU to ECU).

This interface is used for the communication between the CCU and ECU. Communication is done via the MIL-1553B data bus which defines signal levels, baud rate, data bit and every other parameter needed for setting up the communication on a MIL-1553B data bus. Connector used is an EDC29b connector.

Data on the bus will be command and data for controlling the MWS and getting data from it. Commands and data formats are described in the MWS-CD document and will not be described further here. TBD Data and commands that shall be sent to the ECU are data like:

* Aircraft attitude.
* Aircraft Heading.
* Aircraft altitude.
* GPS data.
* Commands for starting ECU Built in self test.

The ECU will the other way make it possible for the CCU to get:

* Status information each 20msec.
* Result of Built in self test .
* Thread information in inertial format.

### Interface E ( Power to Power Switch in pod).

To be able to control the power to the pod a controllable power switch in the pod is mounted. Power from the supply in the wing is connected to this power switch through the connector mounted by subcontractor on the pod and not as indicated to the ECU. This wiring is done by the subcontractor which makes the total harness for the pod, so it will not be described further here.

### Interface F (CCU to AMC).

This interface shall make it possible to communicate with the AMC. Information will both be from AMC to the CCU and from the CCU to the AMC. Communication is done via the MIL-1553B data bus which defines signal levels, baud rate, data bit and every other parameter needed for setting up the communication on a MIL-1553B data bus. Connector used is an EDC29b connector.

Data on the bus will be command and data for the status and data communication. Commands and data formats are described in the DF14b which specify the protocol for exchanging threat data with AMC. TBD Data and commands that shall be sent to the CCU are data like:

* Aircraft attitude.
* Aircraft Heading.
* Aircraft altitude.
* GPS data.
* Commands for starting CCU Built in self test.
* Plane On Ground signal.

The CCU will the other way make it possible for the AMC to get:

* Status information.
* Result of Built in self test.
* Thread information in body frame format.

### Interface G (Power to CCU).

The Cockpit Control Unit will be supplied with 28VDC from the aircraft. An EDC22b TBD connector will be used, pin numbers used are:

* No 1: +28Vdc
* No 2: 0Vdc

### Interface H (Zeroize to CCU).

The Cockpit CCU will be given a discrete signal from aircraft. An EDC21b connector will be used, pin no 1 is for the Zeroize signal. A Logical High level of 5V defines zeroize sensitive data. Further description of zerozice can be found in [Security](#_Security) paragraph.

This paragraph (beginning with 4.3.2) shall identify

an interface by project-unique identifier, shall briefly identify the interfacing entities, and shall be

divided into subparagraphs as needed to describe the interface characteristics of one or both of

the interfacing entities. If a given interfacing entity is not covered by this SSDD (for example, an

external system) but its interface characteristics need to be mentioned to describe interfacing

entities that are, these characteristics shall be stated as assumptions or as "When [the entity not

covered] does this, [the entity that is covered] will ...." This paragraph may reference other

documents (such as data dictionaries, standards for protocols, and standards for user interfaces)

in place of stating the information here. The design description shall include the following, as

applicable, presented in any order suited to the information to be provided, 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 assigned to the interface by the interfacing entity(ies)

b. Type of interface (such as real-time data transfer, storage-and-retrieval of data, etc.) to be implemented

c. Characteristics of individual data elements that the interfacing entity(ies) will 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. Characteristics of data element assemblies (records, messages, files, arrays, displays, reports, etc.) that the interfacing entity(ies) will provide, store, send, access, receive, etc., such as:

1) Names/identifiers

a) Project-unique identifier to be used for traceability

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. Characteristics of communication methods that the interfacing entity(ies) will 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. Characteristics of protocols the interfacing entity(ies) will 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 characteristics, such as physical compatibility of the interfacing entity(ies)

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

# Requirements traceability.

This paragraph shall contain:

a. Traceability from each system component identified in this SSDD to the system

requirements allocated to it. (Alternatively, this traceability may be provided in 4.1.)

b. Traceability from each system requirement to the system components to which it is

allocated.

# Notes.

This section shall contain any general information that aids in understanding this

document (e.g., background information, glossary, rationale). This section shall contain an

alphabetical listing of all acronyms, abbreviations, and their meanings as used in this document

and a list of any terms and definitions needed to understand this document.

# A. Appendixes.

Appendixes may be used to provide information published separately for

convenience in document maintenance (e.g., charts, classified data). As applicable, each

appendix shall be referenced in the main body of the document where the data would normally

have been provided. Appendixes may be bound as separate documents for ease in handling.

Appendixes shall be lettered alphabetically (A, B, etc.).

# Niv 1

## Niv 2

### Niv 3

#### Niv 4