Abstract:

The Seeker 400 UAS is the second full military aviation certification program in the history of a South African product. Its main predecessor was the Rooivalk. On Rooivalk the certification exercise began well after the actual product had been developed and took some 15 years to complete.

Under contract, Seeker 400 will be developed with Certification included. This paper states the specifications and guidelines imposed by Certification on the Seeker 400 program. It assimilates these requirements into the programme’s system engineering process and compares them to the company standards. Findings are presented on what the contemporary international aviation standards require; the associated shortfalls in the company standards; and conclusions as to its impact on the day to day system engineering process are made. Certification requirements address the three levels of design; system, sub-system and line replaceable unit (LRU). Certification evidence is required through all stages of the development process. The outcome of the evaluation is represented in Figure 1.

Introduction:

The Client’s contract requires Military Type Certification of the Seeker 400 UAS system through the Military Aviation Board (MAB). The advantage of having a type certified operational system is that the Client is assured a system which has been designed to and in accordance with contemporary international standards and best practices. This reduces the client’s overall risk in procurement and increases the client’s confidence in their own product.

If Seeker 400 Certification is not taken into account in this development phase, the “back certification” exercise that will be required in future would be a costly exercise as experienced on the Rooivalk program. A lot of knowledge regarding the standards for certification was gleaned from the Rooivalk program, and with the aid of the certification officer from Rooivalk, Seeker 400 is now able to position itself in providing the required “evidence” to internationally certify once the qualification of Seeker 400 is complete.

The benefits to Denel Dynamics in certifying its Seeker 400 system is that it increases the selling power to a broader base of clients who specify certified systems. Further it grants Denel Dynamics the opportunity to review its internal company standards and reflect on their viability in the international domain.

Predictions are that civil aviation certification of Unmanned Aerial Vehicles’ (UAVs), in segregated airspace, is some ten years away due to;
a lack of regulations and standards,
a lack of technology such as sense and avoid,
a lack of historical evidence of the safety of operations, ref [1].

In the event that the skies were to be opened to UAV’s the Type Certified Seeker 400 system, with minor effort, is in a much better position to be phased into such an environment.

Currently the Seeker 400 Certification Plan has been approved by the certification board and the Type Acceptance Master Compliance Book, at the end of the program, shall verify a baseline that complies to:
- a tailored version of Stanag 4671 with regard general design and airworthiness requirements,
- functional and performance criteria as identified in the Contract with the client,
- selected aspects of the URS.
- software developed in accordance with RTCA 178B,
- and hardware meeting environmental and electromagnetic compatibility based on MIL-STD 810E and MIL-STD 461C respectively.

Figure 1 – Seeker 400 System Engineering Process shall be used as a basis for explaining the methodology followed on the Seeker 400 project to obtain final product certification

**System Aspects of Certification:**

Certification at system level hinges on safety and qualification proof. Denel Dynamics’ definition for the design phase is “...to produce the design documentation necessary to demonstrate a system that fully meets the user requirements, that may be engineered to full-scale production, and is capable of being supported in the field.” Ref [7]

According to the System Engineering Handbook v3.1 of 2006 – paragraph 8.10 Certification is a verification method along with inspection, analysis, demonstration and testing, ref [8].

According to Denel Dynamics, qualification is verification proof that a product will meet the Client’s operational requirements. Certification is concerned with verifying that the process was followed as defined in the company standards.

Certification is planned for at the beginning of a Development Cycle similar to the PM, SE, Safety, QA and CM Plans with a Type Acceptance Master Compliance Book at the end of the Development Cycle verifying that the product has been designed and qualified according to the actions as specified in the Certification Plan.

The Compliance Book will be presented to the Military Aviation Board. The MAB will scrutinise the compliance book at Technical Qualification Workgroups, and if satisfied with the content, issue a Military Type Certificate for the product.

The standard system engineering Vee model indicates the three major layers of the project (Figure 1); the first layer is the deliverable system, which includes the Unmanned Aerial Vehicle and the Ground Control Station. The second layer is the sub-system functional areas which are made up of line replaceable units (LRU’s) such as the communications and flight control functional areas. The lowest layer is the line replaceable units which make up the system.

The User Requirement Specification captured the needs of the user as defined at the beginning of the programme; this was largely based on the current Seeker II design with upgrades to the airframe and eliminating obsolescence. From this the System Specification was generated which will form the input document to the verification process at system level. The requirements at system level will largely involve Flight Testing. It is planned that two flight test series will be conducted under the development phase. The first flight test series will verify flight control within the entire flight envelope, and the second flight test series will
verify the payloads included for surveillance. The results will be captured in a Flight Test Report. All the results from flight tests along with the evidence from the low level testing that was performed will be captured in a Qualification Report which will prove verification of the System Specification. Due to time and cost constraints on the program, qualification to Mil-Spec810E was only required within the operational envelope of the LRU’s and not to end of life. This will be an input to the Certification Compliance Book along with the additional flight tests that may be performed to address any outstanding verification proof not adequately addressed by qualification.

The Safety Analysis followed both a top down and bottoms up approach. In the top down approach a Classification of Hazardous Events was compiled which list all possible top level unwanted events applicable to the UAS. A fault tree analysis was performed on each of the events identified in the hazards analysis. At system level the fault tree analysis will serve as inputs to the ‘certification evidence’ required by the certification board.

In the bottoms up approach two safety analyses paths were followed, one for the hardware and one for software analysis. FMECA’s were performed on the hardware configuration items. Denel’s company standards do not require the safety case to classify hardware components to criticality levels as dictated by RTCA 254 but rather classifies the characteristics of the components according to DOD-STD-2101 to ensure that those items identified as critical follow strict monitoring and acceptance testing during the production phase. This FMECA also flows into the Reliability Centred Maintenance which identifies what preventive maintenance is required for ensuring safe operation of the system through its life cycle.

Functional FMECA and Software Safety Assessments were performed on software CSCI’s. These were identified for their criticality as specified in RTCA 178B and treated accordingly.

**Sub-System Aspects of Certification:**

At a sub-system level the bulk of the work hinges on integration of the LRU’s into functional areas such as avionics, communications, propulsion etc. This extensive exercise is not defined by any company standard. It can be more defined by a spiral design method. Interface, test, evaluate and provide feedback into hardware and software design update until the functional area performs as specified in the higher level development specifications. In this phase there is very little documentation and a lot of time spent on implementation. Due to the complexity of and varied nature of this phase, company standards and international standards do not specify a process to be followed apart from the normal configuration management process. Similarly, the certification plan does not dictate evidence to be provided. What will be recorded on the programme will be HILs simulations and ground tests performed on the functional areas to satisfy outstanding requirements verification that was not gleaned from the lower level LRU tests. One of the problems currently experienced which could possibly be addressed in a company standard is the method of informing the lower level designers of any integration issues that may arise in their particular design. The integration engineer has no means of providing feedback on findings to the design engineers. For the production LRU’s this is easily done using the internal PRACAS and ECP process. At development integration process there is no formal baseline for any of the LRU’s. Thus the programme is adopting an informal notification process via a web based database alerting process designers to particular integration issues that have to be resolved. If this process is successful it could possibly be used as an input to the company standard.
**Software Aspects of Certification:**

Certification requires that RTCA 178B guidelines be followed in the life cycle of the software development. On Seeker 400 firmware is defined as software rather than hardware and the processes followed on firmware are in line with the software design process.

**UAV Software:**

Currently the company processes allow for software metric tools such as Understand for C and PC-Lint to ensure the coding standard is followed. In addition requirements coverage of the software requirements specifications will be achieved with the software test descriptions and custom software test environments shall be written. The abovementioned software artefacts will allow the code to be qualified to Level C. The safety analysis has revealed safety critical functionality within the code (RTCA Level A) for some LRU’s within the aircraft. The company processes do not prescribe or suggest any means of obtaining statement coverage, decision coverage or modified decision coverage which needs to be proven for Level A code. Additionally, Level A code has to be verified by means of independence. The programme has decided to achieve this objective by employing an independent contractor to test the relevant CSCI’s in CANTATA. This will achieve both independence and all required level of coverage testing. This also provides the Engineering department with an opportunity to evaluate the Level A certification process and may help in defining company standards for future projects. Currently each programme has its own Certification Officer who advises on an informal method of achieving adequate code coverage to get that project certified by the certification board. This may appease both the current client and the current certification board, but may limit the potential clients who require more rigorous certification adherence to the RTCA guidelines. The current method of certifying to Level A code also has overall cost and time implications for each programme since each programme ‘re-invents’ the wheel.

Due to time constraints on the programme the safety assessments on the software were performed in parallel with the actual hardware and software design, and thus the analysis is unable to influence the architecture of the hardware or software. By implication, this means that any function found to be Level A makes the entire code safety critical and has a severe time and cost implication on the testing and verification of the software. It is advisable that the company find a standard to address this to ensure reduced cost and time spent in the verification cycle of its programmes.

The company software documentation set, to be delivered per CSCI, is perfectly matched to address RTCA certification evidence, except for the PSAC and the SAS. The company standard has been updated to satisfy this requirement.

**Ground Control Station Software:**

Denel Dynamics is traditionally a missiles company with embedded high performance processors where code is written in embedded C format. The Ground Control Station code is written in a Windows Operating System environment. Seeker II, the predecessor of Seeker 400, has been safely operating within this environment for the past fifteen years. None of the incidents that have taken place have in any way shown this operational environment to be unsafe. With the current Certification requirements to RTCA levels the programme is obliged to prove this to the Certification Board. This has posed a problem to the UAV programme since no company standards for software address the verification process of a windows environment. In the greater South African industrial context it is difficult to find development houses that have experience with certifying these environments. Individual professionals around South Africa have worked on international programmes where Windows Environments had to be certified to RTCA levels. These professionals advised that the
Windows Environment can only achieve RTCA 178B Level D certification with international Certification Boards. The programme has presented its plan to certify the GCS code to Level D to the Certification Board with some additional actions for Level C. These actions include that Software Standards for requirements, design and coding in a Windows Environment shall be written and adhered to. It is also difficult to find developers who have worked in this environment within Denel Dynamics since they are all familiar with the C environment.

**Hardware Aspects of Certification:**

The Certification Plan has enforced that Mil-Std 810E for environmental and Mil-Std 461E and Mil-Std 464A at component and subsystem level electromagnetic compatibility be verified, but do not need to verify this using the RTCA 254 guidelines for hardware aspects of certification. One product specification will be written on the program and that is for the entire system.

**UAV Hardware:**

For the development phase of Seeker 400 a mix of advanced development models and engineering design models have been used, the final baseline will be converted into a pre-production model without industrialisation.

The current hardware design process within Denel begins with the development specification for that sub-system. This then gets designed as a mechanical or electronic item of hardware as indicated in Figure-1. The standard drawings are generated with associated BOMs and assembly drawings etc. The program does not dictate explicitly that hardware requirements specifications be written, but in cases of complex design, it will be included. Detail design documents required for hardware is typically included in the doc 705 system (in military terms the “old blue book”). The developers have not been mandated to keep such a file for their development. Where certification requires design proof to answer specific Stanag requirements, it will be extracted from the data pack with the help of the designer and issued as a report.

The verification process for hardware will be threefold. Performance shall be verified by acceptance test reports which are traceable to the development specification for that item. The environmental requirements will be qualified based on an environmental specification which has been written for the programme and is based on Mil-Std 810E. The electromagnetic requirements have been captured in an EMC/EMI specification and addresses both the Mil-Std 464 and Mil-Std 461 for line replaceable units and system level requirements. The specific tailored environmental and electromagnetic tests that have been included have been approved by the Certification Board.

The safety analysis for the hardware was performed using a mix of functional and physical FMECAs, not so much to influence the hardware design process, as this was already too late, but rather to define critical hardware components within the system to utilise in the classification of characteristics and the reliability of both the LRU hardware and system as a whole. This will ensure the safe manufacture of the system and improve the operational life cycle of the product.

**Ground Control Station Hardware:**

The philosophy adopted for hardware within the Ground Control Station is to use as much commercial off the shelf (COTS) hardware as possible. This is to eliminate the obsolescence problems experienced with the Seeker II hardware and also reduce the overall development time of the system. Those line replaceable units that have been developed “in house” will go through the typical development and verification cycle as for the UAV hardware. The COTS
items shall be tested in its installed environment for performance, environmental and electromagnetic requirements to ensure that the components preform, at an integrated level, as defined in the development specification. Certification requires that the COTS configuration items have at least a Certificate of Conformance from the supplier as evidence that the hardware performs its intended function.

**Conclusion:**

At the end of the development cycle, the client will receive a system that has been military type certified. The MAB is not able to certify for the Civil Aviation Environment. Currently nowhere in the world is civil UAV certification being granted. Three reasons are cited for this: a lack of regulations and standards, the lack of adequate sense and avoid technology and the lack of historical evidence of safety of operations. It is perceived that type certifying UAVs for the civil environment is still a good ten years hence.

**References:**

5. MIL-STD 461E, *Requirements for the control of electromagnetic interference characteristics of subsystems and equipment*, August 1999

**Bibliography:**

Andrea Kuhn has been working as a Systems Engineer on various programmes within Denel Dynamics for the past five years. She holds a BSc Aeronautical Engineering and began work within Denel Dynamics as an Aerodynamicist. She also is the only female UAV pilot to have flown deployments for the high speed target drone, SKUA for the Brazilian Air Force.

Prior to her Aeronautical studies, she was working on construction sites and holds a Civil Engineering Diploma.
Figure 1 - Seeker 400 System Engineering Process

SEEKER 400 SYSTEM ENGINEERING PROCESS, BASED ON VEE MODEL

FOR CERTIFICATION EVIDENCE

TIME

2011 2012 2013 2014

CERTIFICATION PLAN

STANAG WITH EDITION 2

COMPLIANCE BOOK

DAR + FBG

PRODUCT SPEC (C-SPEC)

FLIGHT TESTING +

FLIGHT TEST REPORTS +

SYSTEM QUALIFICATION

FUNCTIONAL INTEGRATION, FAULT REPORTING AND
GROUND TESTING, AND

SOFTWARE IN THE LOOP SIMULATIONS

MODELING

RECOGNIZED

RECEIVED

SRS (SOFTWARE REQUIREMENTS SPECIFICATION)

ACCETANCE TEST INSTRUCTIONS/RESULTS

SOFTWARE TEST DESCRIPTIONS/RESULTS

LOW LEVEL QUALIFICATIONS

HARDWARE & SOFTWARE DESIGN DOCUMENT

SOFTWARE DEVELOPMENT FILE

HARDWARE + SOFTWARE BUILD

SUB-SYSTEMS

SOFTWARE REQUIREMENTS

FUNCTIONAL AREA

DEVELOPMENT SPECS

(AR-SPEC'S)

(HARDWARE)

PSAC

RECOGNIZED

RECEIVED

SRS (SOFTWARE REQUIREMENTS SPECIFICATION)

ACCETANCE TEST INSTRUCTIONS/RESULTS

SOFTWARE TEST DESCRIPTIONS/RESULTS

LOW LEVEL QUALIFICATIONS

HARDWARE & SOFTWARE DESIGN DOCUMENT

SOFTWARE DEVELOPMENT FILE

HARDWARE + SOFTWARE BUILD

SUB-SYSTEMS

SOFTWARE REQUIREMENTS

FUNCTIONAL AREA

DEVELOPMENT SPECS

(AR-SPEC'S)

(HARDWARE)

UNIT TESTING & INSPECTION

PSAC

RECOGNIZED

RECEIVED

SRS (SOFTWARE REQUIREMENTS SPECIFICATION)

ACCETANCE TEST INSTRUCTIONS/RESULTS

SOFTWARE TEST DESCRIPTIONS/RESULTS

LOW LEVEL QUALIFICATIONS

HARDWARE & SOFTWARE DESIGN DOCUMENT

SOFTWARE DEVELOPMENT FILE

HARDWARE + SOFTWARE BUILD

SUB-SYSTEMS

SOFTWARE REQUIREMENTS

FUNCTIONAL AREA

DEVELOPMENT SPECS

(AR-SPEC'S)

(HARDWARE)

TESTING & INSPECTION

PSAC

RECOGNIZED

RECEIVED

SRS (SOFTWARE REQUIREMENTS SPECIFICATION)

ACCETANCE TEST INSTRUCTIONS/RESULTS

SOFTWARE TEST DESCRIPTIONS/RESULTS

LOW LEVEL QUALIFICATIONS

HARDWARE & SOFTWARE DESIGN DOCUMENT

SOFTWARE DEVELOPMENT FILE

HARDWARE + SOFTWARE BUILD

SUB-SYSTEMS

SOFTWARE REQUIREMENTS

FUNCTIONAL AREA

DEVELOPMENT SPECS

(AR-SPEC'S)

(HARDWARE)

INTEGRATION & TESTING

PSAC

RECOGNIZED

RECEIVED

SRS (SOFTWARE REQUIREMENTS SPECIFICATION)

ACCETANCE TEST INSTRUCTIONS/RESULTS

SOFTWARE TEST DESCRIPTIONS/RESULTS

LOW LEVEL QUALIFICATIONS

HARDWARE & SOFTWARE DESIGN DOCUMENT

SOFTWARE DEVELOPMENT FILE

HARDWARE + SOFTWARE BUILD

SUB-SYSTEMS

SOFTWARE REQUIREMENTS

FUNCTIONAL AREA

DEVELOPMENT SPECS

(AR-SPEC'S)

(HARDWARE)

INTEGRATION & TESTING

PSAC

RECOGNIZED

RECEIVED

SRS (SOFTWARE REQUIREMENTS SPECIFICATION)

ACCETANCE TEST INSTRUCTIONS/RESULTS

SOFTWARE TEST DESCRIPTIONS/RESULTS

LOW LEVEL QUALIFICATIONS

HARDWARE & SOFTWARE DESIGN DOCUMENT

SOFTWARE DEVELOPMENT FILE

HARDWARE + SOFTWARE BUILD

SUB-SYSTEMS

SOFTWARE REQUIREMENTS

FUNCTIONAL AREA

DEVELOPMENT SPECS

(AR-SPEC'S)

(HARDWARE)

INTEGRATION & TESTING

PSAC

RECOGNIZED

RECEIVED

SRS (SOFTWARE REQUIREMENTS SPECIFICATION)

ACCETANCE TEST INSTRUCTIONS/RESULTS

SOFTWARE TEST DESCRIPTIONS/RESULTS

LOW LEVEL QUALIFICATIONS

HARDWARE & SOFTWARE DESIGN DOCUMENT

SOFTWARE DEVELOPMENT FILE

HARDWARE + SOFTWARE BUILD

SUB-SYSTEMS

SOFTWARE REQUIREMENTS

FUNCTIONAL AREA

DEVELOPMENT SPECS

(AR-SPEC'S)

(HARDWARE)

INTEGRATION & TESTING

PSAC

RECOGNIZED

RECEIVED

SRS (SOFTWARE REQUIREMENTS SPECIFICATION)

ACCETANCE TEST INSTRUCTIONS/RESULTS

SOFTWARE TEST DESCRIPTIONS/RESULTS

LOW LEVEL QUALIFICATIONS

HARDWARE & SOFTWARE DESIGN DOCUMENT

SOFTWARE DEVELOPMENT FILE

HARDWARE + SOFTWARE BUILD

SUB-SYSTEMS

SOFTWARE REQUIREMENTS

FUNCTIONAL AREA

DEVELOPMENT SPECS

(AR-SPEC'S)

(HARDWARE)

INTEGRATION & TESTING

PSAC

RECOGNIZED

RECEIVED

SRS (SOFTWARE REQUIREMENTS SPECIFICATION)

ACCETANCE TEST INSTRUCTIONS/RESULTS

SOFTWARE TEST DESCRIPTIONS/RESULTS

LOW LEVEL QUALIFICATIONS

HARDWARE & SOFTWARE DESIGN DOCUMENT

SOFTWARE DEVELOPMENT FILE

HARDWARE + SOFTWARE BUILD

SUB-SYSTEMS

SOFTWARE REQUIREMENTS

FUNCTIONAL AREA

DEVELOPMENT SPECS

(AR-SPEC'S)

(HARDWARE)

INTEGRATION & TESTING

PSAC

RECOGNIZED

RECEIVED

SRS (SOFTWARE REQUIREMENTS SPECIFICATION)

ACCETANCE TEST INSTRUCTIONS/RESULTS

SOFTWARE TEST DESCRIPTIONS/RESULTS

LOW LEVEL QUALIFICATIONS

HARDWARE & SOFTWARE DESIGN DOCUMENT

SOFTWARE DEVELOPMENT FILE

HARDWARE + SOFTWARE BUILD

SUB-SYSTEMS

SOFTWARE REQUIREMENTS

FUNCTIONAL AREA

DEVELOPMENT SPECS

(AR-SPEC'S)

(HARDWARE)

INTEGRATION & TESTING

PSAC

RECOGNIZED

RECEIVED

SRS (SOFTWARE REQUIREMENTS SPECIFICATION)

ACCETANCE TEST INSTRUCTIONS/RESULTS

SOFTWARE TEST DESCRIPTIONS/RESULTS

LOW LEVEL QUALIFICATIONS

HARDWARE & SOFTWARE DESIGN DOCUMENT

SOFTWARE DEVELOPMENT FILE

HARDWARE + SOFTWARE BUILD

SUB-SYSTEMS

SOFTWARE REQUIREMENTS

FUNCTIONAL AREA

DEVELOPMENT SPECS

(AR-SPEC'S)

(HARDWARE)

INTEGRATION & TESTING

PSAC

RECOGNIZED

RECEIVED

SRS (SOFTWARE REQUIREMENTS SPECIFICATION)

ACCETANCE TEST INSTRUCTIONS/RESULTS

SOFTWARE TEST DESCRIPTIONS/RESULTS

LOW LEVEL QUALIFICATIONS

HARDWARE & SOFTWARE DESIGN DOCUMENT

SOFTWARE DEVELOPMENT FILE

HARDWARE + SOFTWARE BUILD

SUB-SYSTEMS

SOFTWARE REQUIREMENTS

FUNCTIONAL AREA

DEVELOPMENT SPECS

(AR-SPEC'S)

(HARDWARE)

INTEGRATION & TESTING

PSAC

RECOGNIZED

RECEIVED

SRS (SOFTWARE REQUIREMENTS SPECIFICATION)

ACCETANCE TEST INSTRUCTIONS/RESULTS

SOFTWARE TEST DESCRIPTIONS/RESULTS

LOW LEVEL QUALIFICATIONS

HARDWARE & SOFTWARE DESIGN DOCUMENT

SOFTWARE DEVELOPMENT FILE

HARDWARE + SOFTWARE BUILD