European Extremely Large Telescope (E-ELT) Availability Stochastic Model: integrating Failure Mode and Effect Analysis (FMEA), Influence Diagram and Bayesian Network together

Gianluca Verzichelli[a]

[a]European Southern Observatory (ESO), Karl-Schwarzschild-Strasse 2, Garching, Germany

ABSTRACT

An Availability Stochastic Model for the E-ELT has been developed in GeNIE. The latter is a Graphical User Interface (GUI) for the Structural Modeling, Inference, and Learning Engine (SMILE), originally distributed by the Decision Systems Laboratory from the University of Pittsburgh, and now being a product of BayesFusion, LLC.

The E-ELT will be the largest optical/near-infrared telescope in the world. Its design comprises an Alt-Azimuth mount reflecting telescope with a 39-metre-diameter segmented primary mirror, a 4-metre-diameter secondary mirror, a 3.75-metre-diameter tertiary mirror, adaptive optics and multiple instruments.

This paper highlights how a Model has been developed for an earlier on assessment of the Telescope Availability. It also describes the modular structure and the underlying assumptions that have been adopted for developing the model and demonstrates the integration of FMEA, Influence Diagram and Bayesian Network elements. These have been considered for a better characterization of the Model inputs and outputs and for taking into account Degraded-based Reliability (DBR).
Lastly, it provides an overview of how the information and knowledge captured in the model may be used for an earlier on definition of the Failure, Detection, Isolation and Recovery (FDIR) Control Strategy and the Telescope Minimum Master Equipment List (T-MMEL).

Keywords: Observatory, Telescope, Availability, Reliability, Maintainability, Degradation-Based Reliability, Influence Diagram, Bayesian Network

1. INTRODUCTION

An Availability Stochastic Model of the System under analysis helps an Organization to manage the limited amount of information and uncertainties, that are *physiologically* and unavoidably present at the beginning of a project, in a more efficient manner. This reduces the risk of introducing unrealistic or non-cost effective Reliability, Availability and Maintainability (RAM) requirements into specifications for the definition of the System and procurement of Sub-systems. Furthermore, it improves the development process of the design and allows the simulation of *what-if* scenarios to be performed and evaluated efficiently.

2. BACKGROUND INFORMATION

ESO will face new challenges in the development of the E-ELT Programme concerning RAM and Integrated Logistics Support (ILS). There are several critical RAM and ILS aspects that need to be considered when designing, constructing, assembling, integrating and verifying the E-ELT. Table 1 provides a general overview of them.
It is worth noting that the last item of the Table appears in both columns. Indeed, the fact that a Third Party Certification Authority (or in general a Licensing Body) is not required to operate the Observatory, leaves more

Further author information: (Send correspondence to G. Verzichelli)
G. Verzichelli: E-mail: gverzich@eso.org, Telephone: +49 (0)89 3200 6277

freedom to the Organization for establishing the minimum level of effort to be invested in Design for RAM and ILS during Design & Development. But this, at the same time, opens the door to conflicting opinions on *how much* investment is *enough*. Differently, in those environments where a Certification Authority is required to operate the System, there are certain RAM and ILS activities that are mandatory and thus the required investment for the effort is less prone to be challenged. In the case of the E-ELT Programme, the paramount importance that RAM and ILS activities will have, has been amply recognised from the beginning.

Table 1. List of critical and favorable RAM and ILS aspects for the E-ELT Programme.

Critical	**Favourable**
Procurements with a large number of components (but still not a *mass production*) with 100% duty cycle	Recognition that not every single component needs to be functional to operate the Telescope (DBR)
Many components are custom made	Operations carried out only during nighttime
Remote location: high replenishment time	Preventive Maintenance may be performed daily during day time if required
Harsh operational environment: dust, high solar radiation, etc. Reliability Library still valid?	Telescope is not a safety-critical System but still an expensive one...
Lifetime of 30 years (for some Sub-systems a goal of 50)	Logistic infrastructure already existing: Paranal Observatory
Replace/Repair vs. Replace/Discard policy to be carefully considered for the cost of ownership of the Observatory	Third Party Certification Authority not required
Replace/Repair at the Telescope? in the workshop on site? or at the Original Equipment Manufacturer (OEM)?	
Third Party Certification Authority not required	

2.1 E-ELT Top Level RAM Requirements

Without prejudice of providing a compendium of all the E-ELT requirements related to RAM and ILS herein, it is important to recall for completeness the top level requirement related to the availability of the Telescope and that cites as follows:

> *Over a period of one year, no more than 3% of the time (10% in the first year of operation), when weather conditions permit science operations, shall be lost due to technical failures of the System.*

3. THE MODEL

3.1 Overview

A Top Level view of the model at its highest level is depicted on Figure 1. It is possible to identify the core of the model itself (*100_E-ELT*), the Availability (*E-ELT Availability*) and Unavailability (*E-ELT Unavailability*) computation blocks, the parameters for selecting the Severity Level to be considered (*Sev_Level...*), the ones for selecting the type of Availability to be computed (*A_...*) and finally inputs related to the hours (*Hours Considered)* and days (*Days Considered)* to be considered for the simulation.

The presence of an arrow indicates that there is a mathematical relationship amongst two elements: for instance, the arrow starting in the model element *100 E-ELT* and ending in the model element *E-ELT Availability*, indicates that the first *influences* the second by means of a mathematical relationship that needs to be defined within the model element *E-ELT Availability*.

The numerical value computed by the model element *E-ELT Availability* is directly compared with the requirement quoted in Section 2.1.

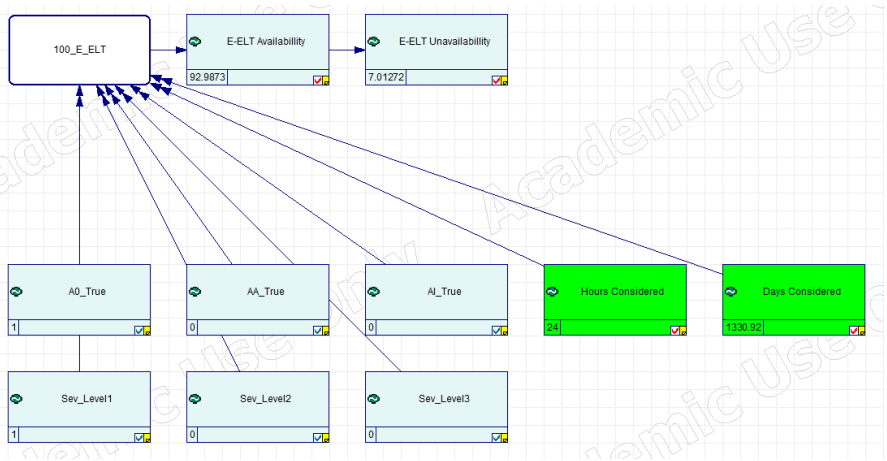

Figure 1. Top Level view of the Model.

3.2 Model Development

The Model has been developed following a modular approach. The latter has been systematically adopted for building the entire network of model elements. These and their hierarchy have been extracted directly from the Product Breakdown Structure (PBS) stored in the Requirements Database DOORS®. Then, using a comma-separated values (CSV) file and a Scripting Language (SL), the entire network of model elements has been created in GeNIE, see also Figure 2.
This approach – given the large amount of model elements to be included – has saved a considerable amount of time to the model developer and has diminished the risk of errors and inconsistencies enormously.

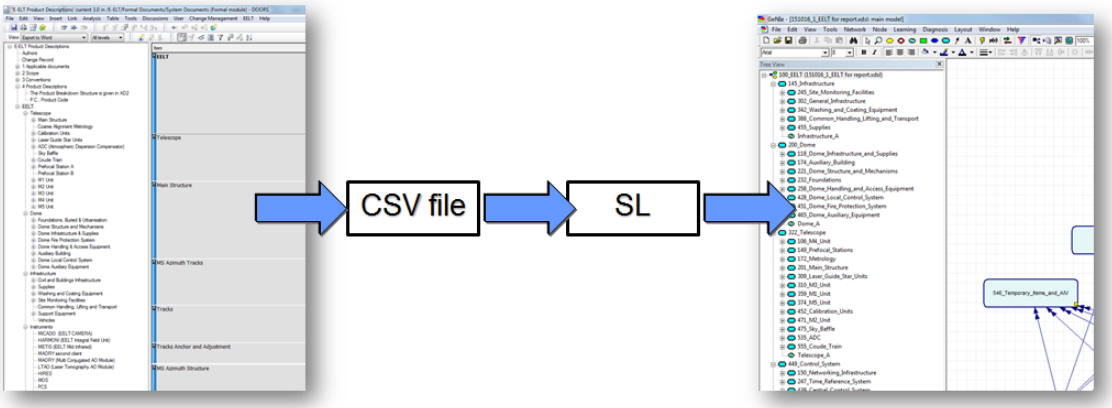

Figure 2. Model development: from DOORS® to GeNIE.

Product Codes have been also retained for an easy browsing and traceability, e.g. the label *322* used in DOORS for the Telescope, has become *322_Telescope* in GeNIE, similarly the label *200* for the Dome in DOORS, has become *200_Dome* in GeNIE.

The next very important step for the model developer has been to validate the hierarchical relationships and the contribution to the overall Telescope Availability.
For the sake of completeness and traceability, when a model element did not contribute to the Telescope Availability, has been left in the model, has been identified by a specific color coding, and has provided 100% of its Availability: an example of this kind of model element is the item *546_Temporary_Items_and_AIV*, which

includes all temporary items needed during Assembly, Integration & Verification (AIV), but not required when the Observatory is at steady state conditions, see Figure 3.

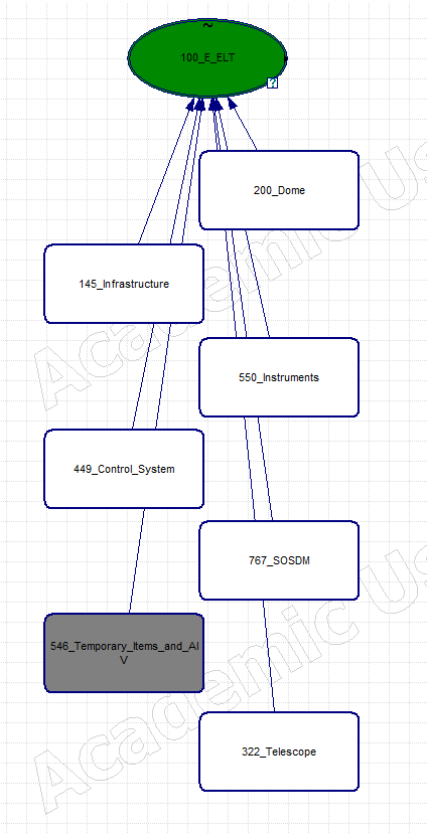

Figure 3. Model Block *100_E-ELT*.

3.3 Module Description

The Module that has been used as the basis for building the entire network of model elements is depicted in Figure 4. In this specific case, it has been instantiated for the model element *451_Dome_Fire_Protection_System*. The block includes all the inputs required to perform the computations explained in Section 3.6, and the output which is the Availability of this specific module. Again the arrows indicates the *influence* amongst the various elements.

3.4 Computational Features

The main computational features that have been included in the model are as follows:

- Parallel Systems: n Sub-systems arranged in a parallel configuration;
- Series Systems: n Sub-systems arranged in a series configuration;
- m *out of* n Systems. Where n is the number of parallel, identical Sub-systems and the System is *down* if there are m or more Sub-systems down.

The related equations for the Parallel, Series and m *out of* n System configurations respectively are given in Eq. 1, 2 and 3 (assuming that all the Sub-systems are identical):

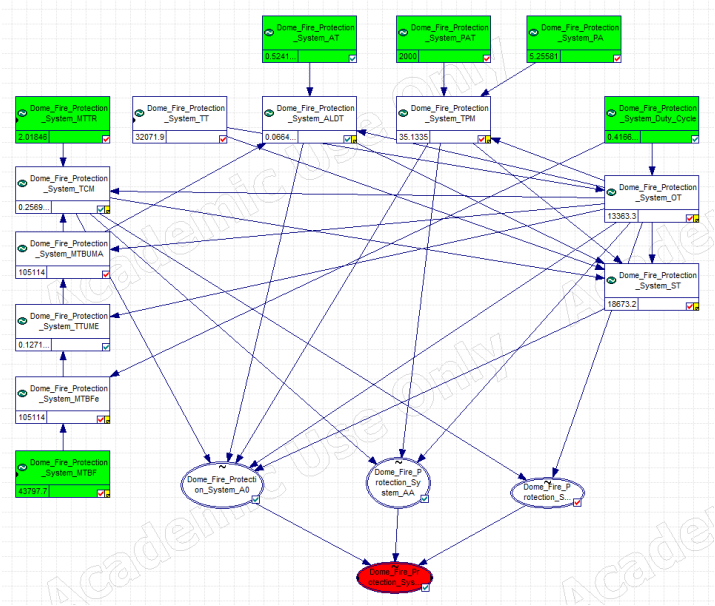

Figure 4. Overview of a Module.

$$A_{Parallel} = 1 - (1 - A)^n \tag{1}$$

$$A_{Series} = A^n \tag{2}$$

$$A_{m\ out\ of\ n} = 1 - \frac{n!}{m! \cdot (n-m)!} \cdot (1 - A)^m \tag{3}$$

The model capability of computing the *Minimal Cut Set* is currently under investigation. A minimal cut set is a combination of intact Sub-systems that causes a System to be functional in the sense of the specified scenario. *Minimal* means that a cut set contains only as many intact Sub-systems as are necessary for the System to be functional. Redundant Systems are characterised by the existence of several minimal cut sets for a specified scenario. By nature, a minimal cut sets analysis considers only two states per Sub-system: *intact* or *failed*.

The majority of the inputs and parameters have been characterized with a stochastic statistical distribution (most of the time either a Gauss or a Gamma distribution have been used). Thus also the outputs of the model yield a stochastic characterization. See for example how the Mean Time Between Failures (MTBF) or the time of an intervention from Paranal have been characterized in Figure 5 and 6, respectively.

3.5 Time Breakdown

The overall Time Breakdown adopted in the Model, is given is Figure 7. The Total Time (TT) is given adding the *Up Time* and the *Down Time*. The *Up Time* is computed adding the Operating Time (OT) and the Standby Time (ST), whilst the *Down Time* is computed adding the *Active Time*, made by the Time for Preventive Maintenance (TPM) and the Time for Corrective Maintenance (TCM), and the *Delay Time*, made by Administrative and Logistics Down Time (ALDT).
The *Off Time* does not apply to Availability Analysis because during this time, System operation is not required. Storage, transportation and overhaul maintenance periods are examples of Off Time.

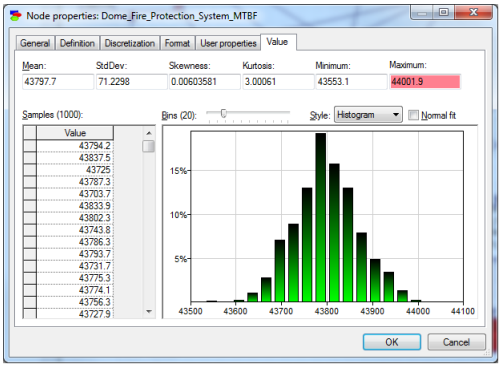

Figure 5. MTBF characterization (Gauss Distribution, values expressed in hours).

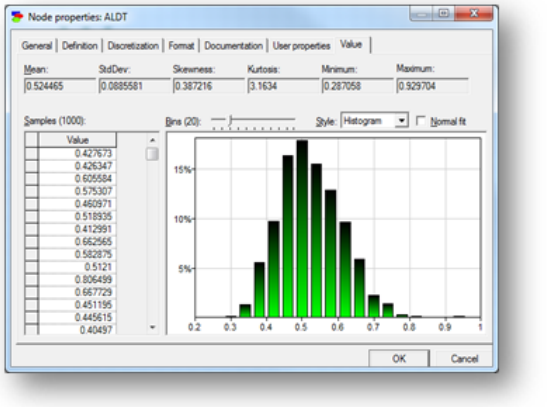

Figure 6. Intervention Time from Paranal (Γ Distribution, values expressed in hours).

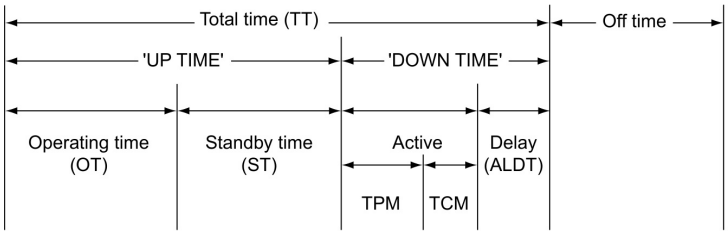

Figure 7. Time Breakdown Overview.

3.6 Types of Availability

Three different types of Availability are considered in the model and all of them are available for computation:

- Inherent Availability, see eq. 4;
- Operational Availability, see eq. 5;
- Achieved Availability, see eq. 6.

$$A_{IA} = \frac{MTBF}{MTBF + MTTR} \tag{4}$$

$$A_{OA} = \frac{OT + ST}{OT + ST + TPM + TCM + ALDT} \tag{5}$$

$$A_{AA} = \frac{OT}{OT + TCM + TPM} \tag{6}$$

The Model user can select any of the three types of Availability at one time by selecting a certain boolean value. The three different types of Availability are important because each of them is needed considering the scope of the analysis that the user has to perform. For instance, when dealing with requirements to be implemented in a contractual environment, by means of a Technical Specification document, all the elements related to the administrative and logistics delays are not relevant for the Contractors. These in fact have to be considered only by ESO: indeed the Contractor is not responsible for dealing with such matters but only for the purely technical ones related to the product that it within the scope of its responsibility.
Nevertheless it is important for ESO to have a clear understanding of the overall E-ELT Availability considering all the factors: the ones for which the Contractor is accountable and the ones for which ESO is accountable. For this reason, the three types of Availability can be all computed in the Model.

3.7 Degraded-based Reliability

DBR has been considered in the E-ELT Programme for maximising Observatory Availability and reduction of development costs. DBR has been introduced in the Technical Specifications of the various procurements, considering three different levels of Severity to which then correspond three different values of MTBF. The three types of Severity are defined as follows:

Severity 1: Loss of Observation: the Telescope is not operational;

Severity 2: Observation is possible but with a degradation of performance;

Severity 3: all other types of consequences.

The model is capable of computing the E-ELT Availability considering the three different types of Severity. This is done by selecting a specific boolean value, see also Section 3.

3.8 Example of Results

An example of results for the expected Inherent Availability of the E-ELT is given in Figure 8. The mean value is equal to 97.06%, whilst the maximum and the minimum are equal to 96.58% and 97.46% respectively and the standard deviation is equal to 0.14. The Skewness and the Kurtosis values are equal to -0.04 and 2.99 respectively. Skewness is a measure of the asymmetry of the distribution – for a standard normal distribution, skewness is zero – negative values indicate data that are skewed left (left tail is long relative to the right tail). Kurtosis is a measure of the peakedness of a distribution (for standard normal distribution is zero), positive values indicates a *peaked* distribution and negative indicates a *flat* distribution.

As it possible to note, see also Figure 9, with the current values used in the model, there is circa a 70% chance that the E-ELT is compliant with respect to the requirement given in Section 2.1. The values used in the model are currently being reviewed and an improvement of the Inherent Availability is expected.

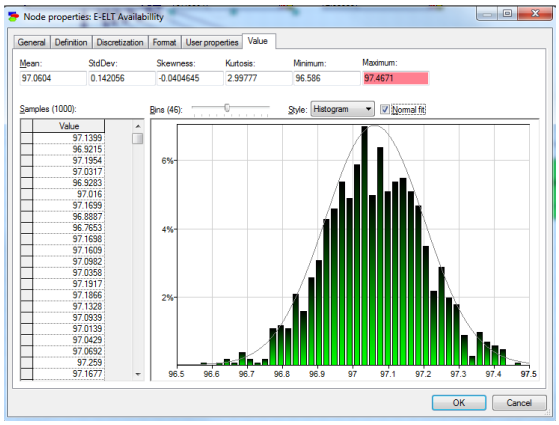

Figure 8. Example of results for the Inherent Availability (Histogram with 46 bins).

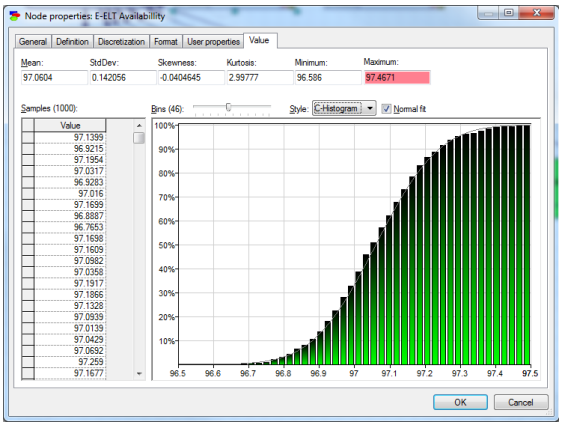

Figure 9. Example of results for the Inherent Availability (Cumulative Histogram).

4. EMBEDDING FMEA

Generally the values of MTBF that are found in the Reliability Data Libraries or in the Product Sheets of the Manufacturer, refer to an average value which somehow encompasses all the failure modes of the item under consideration.

In order to enhance and refine the evaluation of the MTBF and the Mean Time to Repair or Replace (MTTR), FMEA is embedded in the Model. All the known failure modes are taken into account, see an example applied to the Slit Door Structure in Figure 10. For this reason, two additional parameters have been introduced in the model: the *failure mode ratio* α_i and the *repair rate* r_i.

With these two additional parameters, it is possible to refine the computation of the MTBF and MTTR using equations 7 and 8.

$$MTBF_{Slit\_Door\_Structure} = \frac{1}{\lambda_1 \cdot \alpha_1 + \lambda_2 \cdot \alpha_2 + \lambda_3 \cdot \alpha_3 + \lambda_4 \cdot \alpha_4} \tag{7}$$

$$MTTR_{Slit\_Door\_Structure} = \frac{\lambda_1 \cdot r_1 + \lambda_2 \cdot r_2 + \lambda_3 \cdot r_3 + \lambda_4 \cdot r_4}{\lambda_1 + \lambda_2 + \lambda_3 + \lambda_4} \tag{8}$$

5. TELESCOPE MASTER MINIMUM EQUIPMENT LIST

In aviation, a Minimum Master Equipment List (MMEL), is a document approved by the Certification Authority and created specifically to regulate the dispatch of an aircraft type with inoperative equipment. It establishes

Functional Failure	Variable Name	Value [FIT]	Failure Mode Ratio (alpha)
Fail to Open	Lambda_Fail_to_Open	$\lambda_1 = 1000$	$\alpha_1 = 0.4$
Fail to Close	Lambda_Fail_to_Close	$\lambda_2 = 2000$	$\alpha_2 = 0.4$
Stuck Open	Lambda_Stuck_Open	$\lambda_3 = 100$	$\alpha_3 = 0.1$
Stuck Closed	Lambda_Stuck_Closed	$\lambda_4 = 100$	$\alpha_4 = 0.1$
	Total		**1**

Figure 10. Example of failure modes for the Slit Door Structure.

the aircraft equipment allowed to be inoperative under certain conditions for a specific type of aircraft and still provide an acceptable level of safety and thus the capability of flying for the aircraft. The MMEL contains the conditions, limitations and procedures required for operating the aircraft with these items inoperative. An excerpt of a MMEL is shown in Figure 11. Any inoperative item of equipment in the MMEL which would require an operational or maintenance procedure to ensure the required level of safety, is identified by an appropriate symbol in the *Remarks or Exceptions* column of the MMEL. This is normally (O) for an operational procedure and (M) for a maintenance procedure. $(O)(M)$ means both operational and maintenance procedures are required.

Civil Aviation Authority **(Insert NAA/country)**

MASTER MINIMUM EQUIPMENT LIST

Aircraft -	**Revision No. -** 5	**Page**
Canadair CL600 \ 601 \ 601-3A \ 601-3R \ 604	**Date:** January 06 / 97	29-1

System and Sequence No. Item.	**1.**	**2. Number installed**	**3. Number required for dispatch**	**4. Remarks or Exceptions**
29 – HYDRAULICS				
11-1 Electric Motor Driven Hydraulic Pumps (System 1 and 2)	C	2	1	(M) One may be inoperative provided: a) Affected pump is selected off and is deactivated, and b) Both Engine Driven Hydraulic Pumps are operative.
11-2 Hydraulic Accumulator Pressure Gauges Systems 1, 2, and 3)	C	3	0	(M) All may be inoperative provided accumulator pre-charge is checked using a suitable gauge before the first flight of the day.
11-3 Hydraulic Accumulators (Systems 1,2, and 3)	B	3	1	System 1 and /or System 2 accumulator(s) may be inoperative.
11-4 Engine Driven Hydraulic Pumps	C	2	1	(M) One may be inoperative provided all other hydraulic pumps are operative.
11-5 Hydraulic Heat Exchanger Cooling Fan (600 \ 601 \ 601-3A \ 601-3R)	C	1	0	May be inoperative provided ground operation of hydraulic systems 1 and 2 is limited to 30 minutes when OAT is above 45 degrees C.

Figure 11. Example of Master Minimum Equipment List for an Aircraft.

An approach similar to the one of the MMEL is being considered for the E-ELT Telescope. The level of granularity adopted in the E-ELT may not be necessarily the same of the one of an aircraft MMEL but it has to be tailored to the specific need. Indeed, in this case, the final purpose of a MMEL-like for the E-ELT Telescope (T-MMEL), would be to understand under what conditions there is the capability of *dispatching* the Telescope

for performing observation (similarly to the capability of dispatching an aircraft for flying in case of the MMEL used in aviation).
The information contained in the model, once updated and its granularity increased with the data provided by the various contractors, within their scope of responsibility (example number of items, redundant items, etc.), may be used as first source of knowledge for developing a T-MMEL document for the E-ELT. The process briefly described in Figure 12 should be incremental and evolve with time.

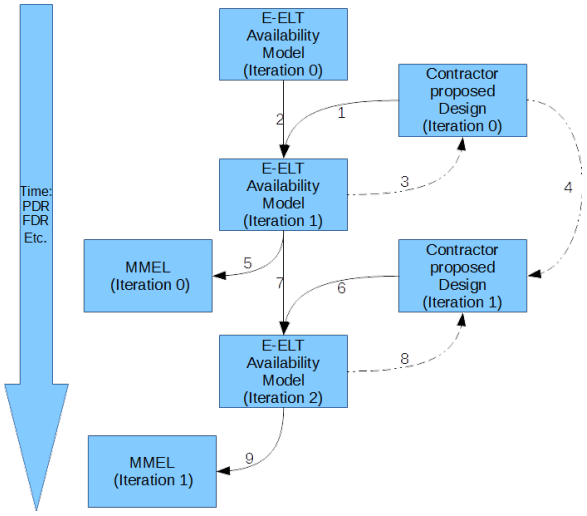

Figure 12. MMEL Development Process Overview (numbers relate to the expected sequence of events, dash-dotted lines represent feedback loop).

When the T-MMEL is introduced and developed in the early phases of the design, it inevitably obliges the Designer and the Customer *to talk to each other* in order to carefully select the right level of trade off between the amount of monitored and un-monitored equipments. Indeed a monitored equipment will provide a lower MTTR for the Telescope but also an increase of development and ownership costs.
Furthermore when a T-MMEL document is available during Telescope operation, especially during the initial phases, this may be embedded directly in the Operations Manual and thus it may help to reach a level of maturity of such document much earlier on.
In Figure 13, is depicted an example of T-MMEL for the E-ELT, specifically addressing the inoperability of some M1 Segments versus two types of Observation Modes: Extreme Adaptive Optics (AO) and observations in the rest of AO modes (and seeing-limited). As it is possible to note from Figure 13, in order to perform Observation in Extreme AO Mode, only one M1 Segment is allowed to be inoperative and seven for observations in the rest of AO modes (and seeing-limited).

Compil	G. Verzichelli										
Approved by											
Date	5/17/2016										
						Number required for Observation					
						Extreme AO			Observations in the rest of AO modes (and seeing-limited)		
Parent Code	Parent Description	Child Code	Child Description	Number Installed	Catego	Number required for Observation	Remarks or Exception	Category	Number required for Observation	Remarks or Exception	Cat
322	Telescope	359	M1 Unit								
359	M1 Unit	273	M1 Segment Subunit								
273	M1 Segment Subunit	300	M1 Segment Assemblies								
300	M1 Segment Assemblies	187	M1 Segment	798	TBA	797	TBA	TBA	791	TBA	
187	M1 Segment	3	M1 Segment Polished Blank								

Figure 13. Example of T-MMEL for the E-ELT.

6. FAULT DETECTION, ISOLATION AND RECOVERY

FDIR is an activity that studies the System under analysis and strive to identify after the occurrence of a failure, how the System is isolated and how to recover it, see also Figure 14.
The analysis can provide very important insights for a more mature and earlier on definition of the Central Control System and Local Control Systems FDIR control logics.
The model may be used as the first and primary source of information for developing FDIR control logic strategies at subsystem level and, particularly, at System level.
A process similar to the one depicted in Figure 12 for the MMEL development may be adopted in case of a FDIR definition activity.

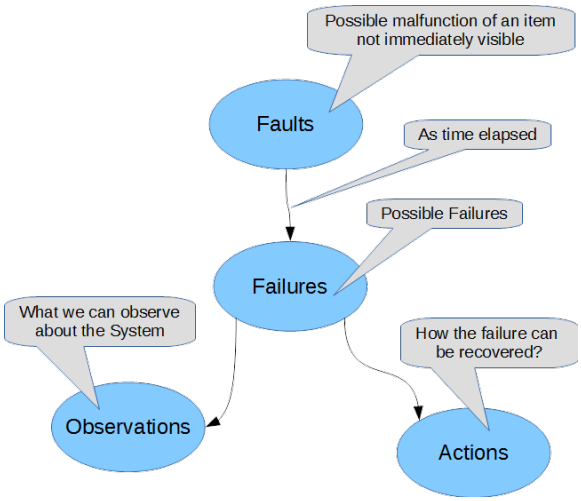

Figure 14. FDIR Process Overview.

7. CONCLUSIONS

A Model for computing the expected Availability of the E-ELT has been presented. The model is used for several purposes depending on the development stages of the Programme:

- In the early phases of the development, it is used to define quantitative achievable and cost effective RAM requirements and for availability budget definition (evaluating several *what-if* scenarios);
- Later on it is adopted as a framework where – as soon as new information related to Contractors detailed design solutions is provided – this is embedded and a refined assessment of the Telescope Availability can be performed;
- Finally, when first reliability and maintainability data become available, either from a Accelerated Life Testing campaign or from field data, the adoption of Bayesian Network allows updating the prior distributions with posterior distributions and thus re-computing the overall Telescope Availability.

The Model also allows the integration of FMEA, Influence Diagrams and Bayesian Network. The implementation of the latter in GeNIE environment with continuous variables is currently under study.