DESIGN FOR RELIABILITY AND SAFETY: CHALLENGES AND OPPORTUNITIES IN HYDROGEN MOBILITY ASSETS

Hernandez Bello, J.
Systems Engineering Department
Shell Hydrogen, 150 North Dairy Ashford, Houston, TX 77079, USA.
email: Juan.Hernandez@Shell.com

ABSTRACT

Safety and reliability are important performance attributes of any engineered system where human-machine interactions are present. However, they are usually approached as afterthoughts or, in some cases, unintended consequences of the system design and development process that must be addressed and verified in subsequent design stages. In plain words, safety and reliability are often seen as constraints that add layers of complexity and extra costs to the minimum functional system of interest.

No longer. Shell Hydrogen is embedding the Design for Reliability and Safety approach to engineer our products and assets in such a way that safety and reliability are at the core of a concurrent engineering process throughout the system lifecycle. This has been achieved in practice by leveraging systems, reliability, and safety engineering methods along with the experience and expertise of Shell Hydrogen, original equipment manufacturers, and system integrators in designing, building and operating hydrogen assets for mobility applications.

The challenges in implementing this approach are many, ranging from access to historical data on equipment and component safety and reliability performance, to lack of standardization in the industry when dealing with hydrogen related hazards. In this paper we will describe the approach in more detail, some of our early successes and failures during deployment, and the continual improvement journey that lies ahead.

1.0 BACKGROUND

Safety is at the core of Shell's values and remains a priority for every asset, facility, or project regardless of what phase of development they are in. This is equally certain for Hydrogen Mobility where the hazards and their impact to people and the environment should not be underestimated.

As per Shell HSSE and SP (Health, Safety, Security, Environment and Social Performance) framework [1], Shell Hydrogen is required to:

1) establish and maintain an effective Hazards and Effects management process;

2) identify HSSE and SP Hazards and document their effects on people, assets, the community and the environment;

3) assess all the risks of identified hazards for worse-case credible scenarios; and

4) manage those risks based on criticality by elimination, reduction by substitution, and/or implementation of controls and recovery measures.

All of this while demonstrating that risks have been reduced to ALARP (As Low As Reasonably Practicable) [2] as per pre-defined criteria.

To comply with the HSSE and SP framework Shell Hydrogen has developed a bespoke standard for Hazards and Effects Management Process, HEMP [3], to provide a structured manner for the identification, assessment, and mitigation of HSSE and SP risks to ALARP. According to the HEMP standard process safety reviews shall be conducted for new assets and for modifications to existing assets. These process safety reviews include, but are not limited to, Process Hazard Analysis, HAZID, HAZOP, LOPA and DSR (Desktop Safety Review).

Shell is a buyer and operator of Hydrogen Refueling Station (HRS) equipment, distribution trailers, and loading facility equipment, which are designed and manufactured as per Shell specifications and requirements as detailed in the Basis for Design (BFD) document. Usually, those suppliers offer a successful history of deployment and operation. However, Shell has identified gaps in compliance to its standard design and engineering practices for system performance and reliability. These gaps have prompted Shell to co-develop, along with its suppliers, a new generation of state-of-the-art technologies. The challenge is how to manage the risks of owning and operating a hydrogen refueling network when the customer, solution space, and industry standards are in a state of flux.

Shell Hydrogen applies Systems Engineering methodology to manage such risks. At its core, the purpose of Systems Engineering is to deal with risks such as “the risk of not delivering what the customer wants and needs, the risk of late delivery, the risk of excess cost, and the risk of negative unintended consequences” [4]. Shell Hydrogen uses both qualitative and quantitative reliability and risk methods to assess the degree to which the risk of these unintended consequences has been attenuated.

2.0 RESIDUAL RISK TOLERABILITY AND ALARP

Meeting the Tolerability criteria includes, but is not limited to, meeting industry codes and standards, Shell standards and HSSE premises for assets. These criteria may also include stakeholder expectations. Tolerability assumes that all identified barriers from threat to consequence are valid and are functioning as intended. In HEMP [3] the tolerability criteria for residual risk of those incident scenarios resulting in people consequences is defined. For scenarios where there is a potential of multiple fatalities the first course of action is to eliminate the impact on people either through relocation of personnel or relocation of equipment. In case relocation is not a practicable option the tolerability criteria establish the maximum number of occurrences per year for the assessed scenario.

One way to quantitatively assess the residual risk of the consequences is using Layers of Protection Analysis (LOPA) where every single barrier is considered independent as illustrated in the Bow Tie example shown in figure 1 below.

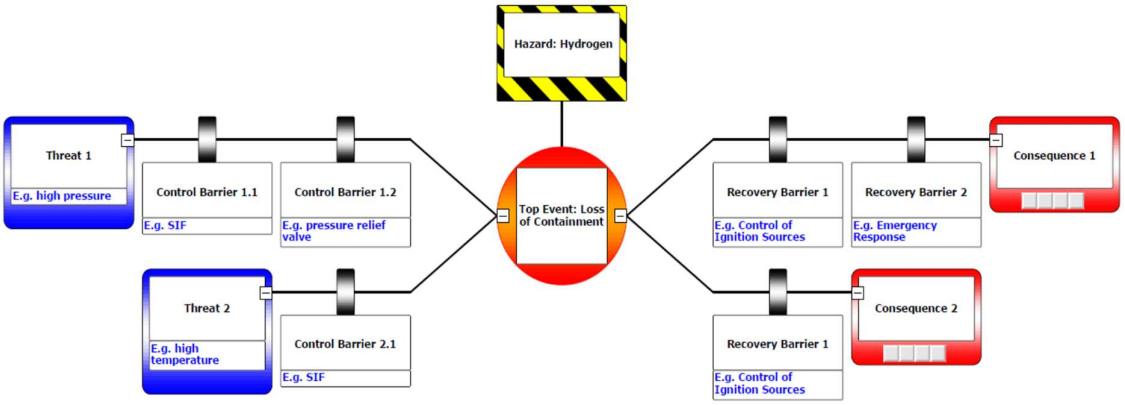

Figure 1. Bow tie for Hydrogen loss of containment scenario

According to LOPA residual risk is calculated as:

$$\text{Residual risk} = \text{IEF} \times P_e \times (PFD_1 \times PFD_2 \times \ldots \times PFD_n) \times P_c \quad (1)$$

Where:

IEF is initiating event frequency, i.e., how often would the initiating event occur.

P_e is enabling probability

PFD is probability of failure on demand of a barrier, i.e., the probability that a barrier will not work when needed.

P_c is conditional probability

The challenge we have faced when assessing Hydrogen refuelling systems is that the application of LOPA for residual risk assessment, while useful, is limited as the criteria for application of the tool is not totally fulfilled [5]. Some control and recovery barriers are non-independent as they have common causes of failures and, in some instances, they also fulfil double functionality such as safeguarding and process control. This has resulted in the need for alternative quantitative and semi-quantitative risk assessment techniques, such as Fault Tree Analysis (FTA) and Failure Modes and Effects Analysis (FMEA) that, as part of the Design for Reliability and Safety (R&S) process, aim at ensuring that the system design complies with the tolerability criteria and the residual risks are reduced to ALARP.

3.0 DESIGN FOR RELIABILITY AND SAFETY (R&S)

The traditional split between safety and reliability in the industrial organizations as well as in international standardization makes it hard to properly handle the tight links between them: improving safety generally undermines reliability and vice versa. For instance, adding safety barriers without

reliability considerations is likely to lead to system architectures subject to spurious safety actions. Then the safety is achieved to the detriment of the reliability of the system of interest.

Design for R&S is a concurrent engineering approach that considers safety and reliability attributes as desired and intended system emergences. The objective is not having to compromise one for the sake of the other. This is achieved by defining R&S objectives for the different use cases of the system of interest that, in turn, are meant to be translated into clear system requirements. These requirements are to be managed via verification activities throughout the subsequent phases of the system development. This is to be reflected into the project execution plan as well as in the contracts with suppliers and partners.

The phases of the design for R&S process and how it fits within the system development process are depicted in figure 2 below.

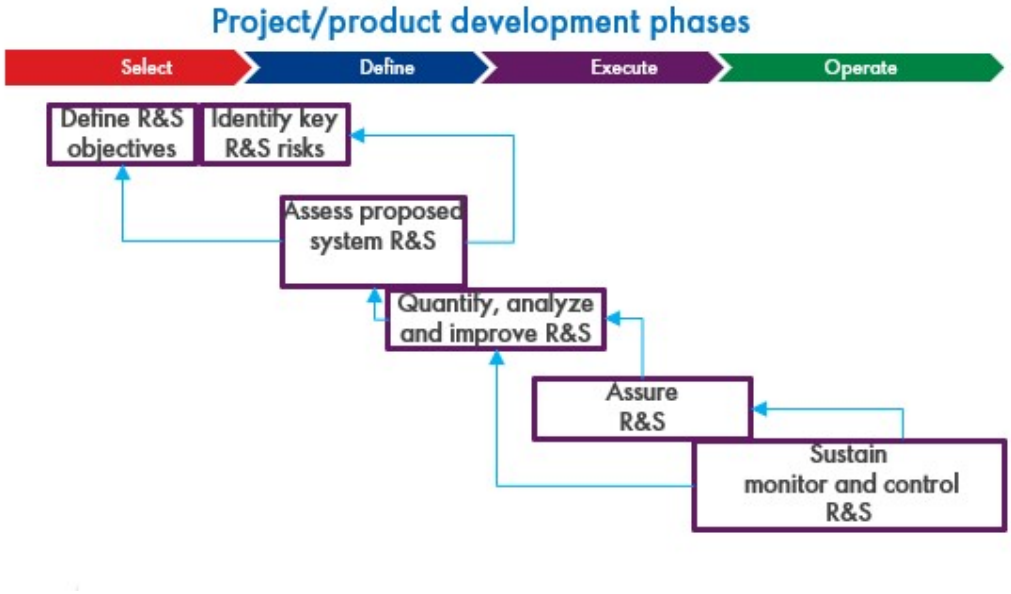

Figure 2. Design for Reliability and Safety (R&S) process

The R&S objectives derive from the user needs and the operating context. The identification of R&S risks is achieved by well-known processes such as HAZID, HAZOP, DSR, FMEA, etc., and the assessment of those risks is an iterative process that will result in improvements to initial system architecture and design. Depending on the complexity of the system additional quantitative risk assessment techniques are employed such as QRA, FTA, system RAM modelling and simulation. Those assessments can take place either before the design is frozen (end of Define phase), in which the value can be higher as potential improvements can be implemented without major schedule or cost impact, or after that as part of the assurance and verification process. Monitoring and control start with the commissioning of the system and continues throughout its useful operating life. Finally, the continuous improvement process of collecting data and feeding it back in reverse cascade mode to all the steps of the process constitutes the backbone of the approach. This is achieved by processes such as FRACAS

(Failure Report and Corrective Action System) or the internal Shell Manage Threats and Opportunities (MTO).

4.0 IMPLEMENTING THE APPROACH

We have gained valuable experience during the implementation of the Design for R&S approach; the following sections contain some examples of activities performed on Hydrogen Refuelling Stations (HRS).

4.1 Assessment of residual risk using Fault Tree Analysis (FTA)

When reviewing a Hydrogen refuelling system there was a need to perform quantitative risk assessment of the risks identified by HAZOP and Desktop Safety Review activities. In this case the LOPA methodology could not be fully applied due to the interdependency of the safety functions.[5]

FTA as described by O'Connor [6] is a "reliability/safety design analysis technique which starts from consideration of system failure effects, referred to as top events. The analysis proceeds by determining how these can be caused by individual or combined lower-level failures or events." We applied the technique to assess the most critical safety functions as defined by IEC 61025 [7] and described for calculation of electrical, electronic, and programmable electronic safety-related systems by IEC 61508 [8] and ISO/TR 12489 [9]. An example of a Fault Tree Diagram for a Safety Instrumented System is shown in figure 3 below.

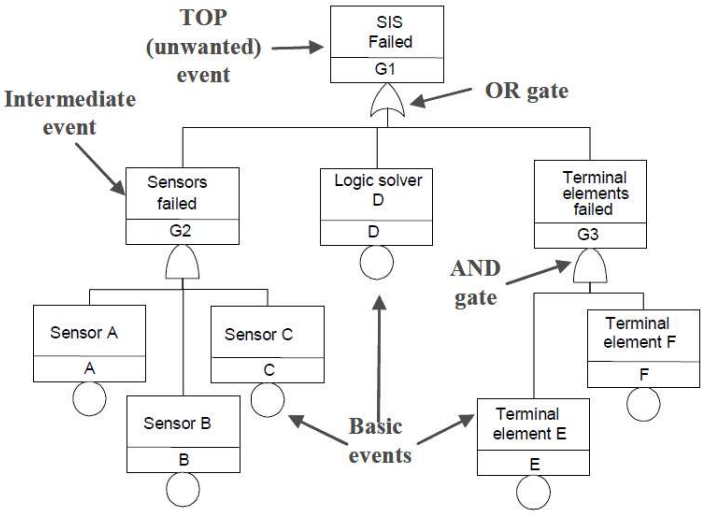

Figure 3. Fault Tree diagram for a Safety Instrumented System

Safety risks were assessed by calculating the probability of failure on demand PFD of the safety barriers and mapping their interdependencies in the fault tree diagram. Those risks included: elevated temperature at H2 compressor outlet; high H2 concentration in

compressor compartment; elevated temperature in LDV tank; high pressure at compressor inlet; and H2 leak due to fuelling hose failure among others. In those cases where the residual risk was deemed not in compliance with the tolerability criteria, or ALARP, further risk reduction measures were devised and assessed in the FTAs. This resulted in system upgrades in terms of hardware, software, and procedures (Operations and Maintenance).

Figure 4 below shows a snip of the simplified FTA analysis for one of the safety functions.

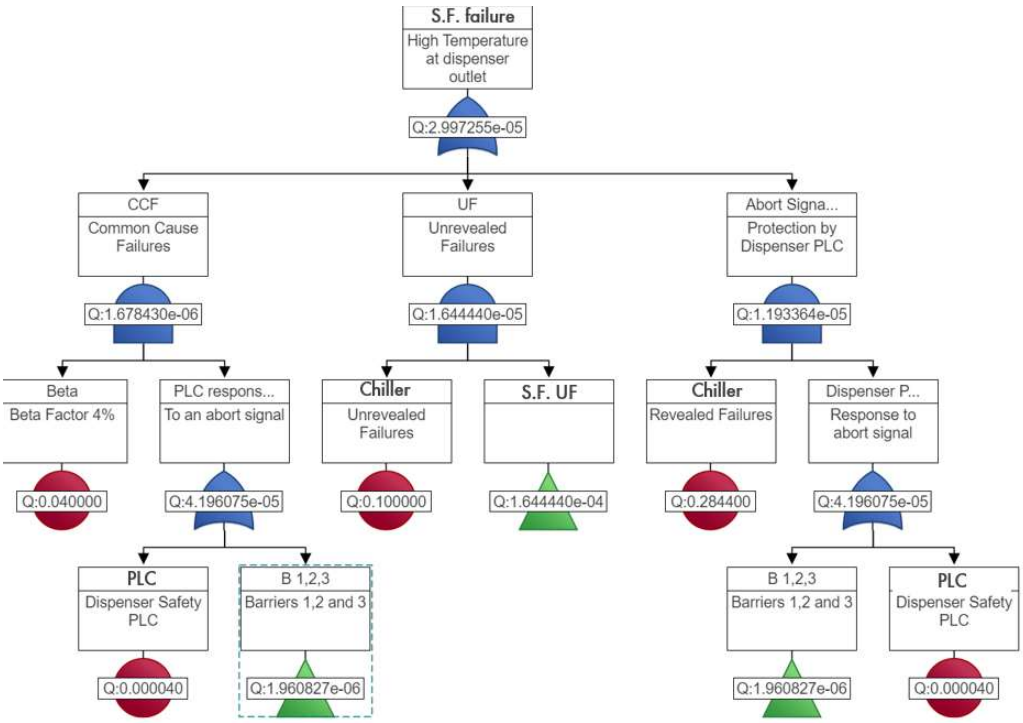

Figure 4. Simplified Fault Tree Diagram of a safety function designed to protect the system when there is high temperature at dispenser outlet.

In this particular case the residual risk, quantified as probability of failure on demand PFD, resulted in 3 x 10^{-5} occurrences per year which is lower than the threshold set by the criteria. Further risk reduction measures were considered not ALARP and therefore no additional barriers or design changes were recommended in this case. For the assessment of the common cause failures, the Beta (β) approach as described in IEC 61508-6 [8] was implemented. Calculations and scoring were performed as indicated by the standard

resulting in a Beta factor of 4% which was deemed acceptable considering the following ranges as described by the standard:

β =10% Conservative

β = 5% Good safeguard

β = 1% realistic

4.2 Failure Modes and Effects Analysis

Another well-known process that we have adopted for the identification, assessment and management of Reliability and Safety risks is the Failure Modes and Effects Analysis (FMEA). Shell Hydrogen applies the standard IEC 60812 for FMEA [10]. According to this standard "failure modes and effects analysis is a systematic method of evaluating an item or process to identify the ways in which it might potentially fail, and the effects of the mode of failure upon the performance of the item or process and on the surrounding environment and personnel."

The goal of an FMEA study is to support decision that reduce the risk of failures contributing to improved outcomes of the system of interest. These improved outcomes include, but are not limited to, improved safety and reliability, reduced environmental impact, reduced procurement and operating costs, and enhanced business reputation.

The FMEA is a bottom-up approach where the failure mode is at the core of the analysis and the barriers (controls) are designed to prevent or mitigate the impact of the system failure. This approach can be depicted by a bow tie diagram as shown in figure 5 below.

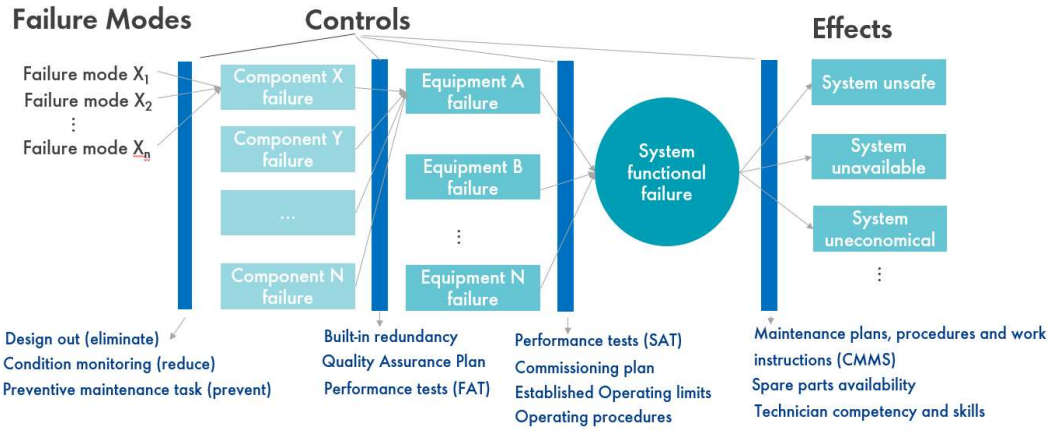

Figure 5. FMEA scope and potential controls (barriers)

Failure mode as defined by Moubray [11] is and event which is likely to cause a system functional failure, meaning that the system is no longer able to fulfil a function to a standard of performance which is acceptable to the user. In Shell we focused primarily on dominant failure modes that, as described by Bello [12], are more likely to be responsible for functional failure under consideration.

The FMEA methodology involves the risk assessment of each failure mode identified in the system based on its severity/impact, frequency of occurrence, and likelihood of its detection in a scale from 1 to 10. The criticality is then given by a risk priority number as follows:

Risk Priority Number = Severity x Likelihood x Detection (2)

As the standard [11] allows for a tailored approach, Shell Hydrogen has defined the rankings for Hydrogen refuelling stations. An example for detection ranking is shown in table 1 below.

Table 1. FMEA Detection ranking for Hydrogen refuelling station

FMEA Detection Ranking		
Detection	Criteria	Detection Ranking
Almost Certain	The design control will almost certainly detect the failure before the impact and consequence of the failure is realized. (E.g., controller exists and takes action)	1
Very High	Very high chance that the design control will detect the failure before the impact and consequence of the failure is realized. (E.g., there is an alarm)	2
High	High chance that the design control will detect the failure before the impact and consequence of the failure is realized. (E.g., there is an indication)	3
Moderately High	Moderately high chance that the design control will detect the failure before the impact and consequence of the failure is realized. (E.g., Operator daily check or sampling)	4
Moderate	Moderate high chance that the design control will detect the failure before the impact and consequence of the failure is realized. (E.g., explained in procedures but operator dependent)	5
Low	Low chance that the design control will detect the failure before the impact and consequence of the failure is realized. (E.g., monthly preventive maintenance routine)	6
Very Low	Very low chance that the design control will detect the failure before the impact and consequence of the failure is realized. (E.g., quarterly preventive maintenance routine)	7
Remote	Remote chance that the design control will detect the failure before the impact and consequence of the failure is realized. (E.g., annual preventive maintenance routine)	8
Very Remote	Remote chance that the design control will detect the failure before the impact and consequence of the failure is realized. (No preventive maintenance or inspection tasks)	9
Very Uncertain	There is no design control or control will not detect the failure before the impact and consequence of the failure is realized. (No detection)	10

Based on the tables RPN scores we have categorized the resulting RPN in the ranges low, moderate, and high as listed in the table 2 below.

Table 2. Risk categorization based on RPN score

RPN Lower Bound	RPN Upper Bound	RPN Risk Category
0	100	Low
101	200	Moderate
201	1000	High

The methodology has been applied to an existing HRS where initial RPN was assessed. In those cases where the scoring risk was deemed too high, additional controls and mitigations were formulated and the residual RPN was calculated assuming these new controls were implemented and performed as expected. The results of the assessment, initial vs residual RPN per subsystem, are summarized in the figure 6 below.

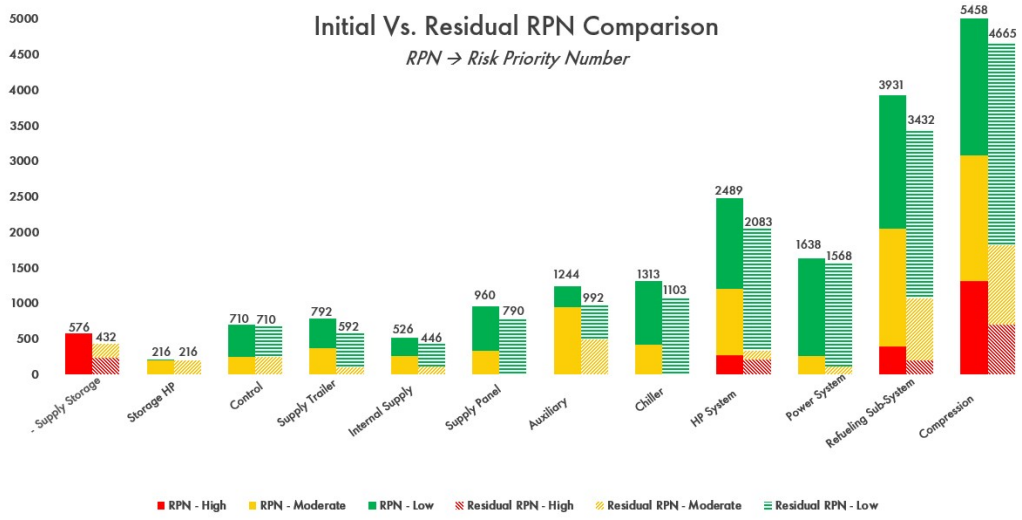

Figure 6. Initial vs Residual RPN for Hydrogen Refuelling Station

This assessment was performed on an existing HRS where no design changes were proposed but merely mitigating actions related to operations and maintenance activities. The impact of the risk reduction measures in the operate phase can be appreciated. This type of analysis

would have been more impactful in the design phase were further risk reduction could have been achieved by improvements to the proposed system design and architecture.

4.3 Modelling and Simulation

A model is a representation of a system with the objective to predict its emergences under a defined set of operating conditions. As stated above, high levels of safety and reliability are intended emergences of future Hydrogen assets and supporting systems, and therefore a consistent way to verify these emergences during the design phase is by modelling the system of interest. Shell Hydrogen leverages computer models in order to assess the expected Reliability, Availability and Maintainability (RAM) attributes of a system configuration and its potential variations in order to improve the design and verify the user requirements throughout the system lifecycle. Once the model is built, the simulation process takes place by specifying a set of inputs to predict the system response. The technique we use in this case is Monte Carlo simulation. The building blocks of RAM models are the system failure modes of the Hydrogen assets. Thus, the FMEA process becomes a fundamental prerequisite of the modelling activity. In this case, the failure modes as defined by FMEA, are parametrized by allocating probability distributions for failure and restoration based on manufacturing test data and/or historical performance in similar assets and operating conditions, when available.

There are several results that can be distilled from these models such as predicted availability of the system, throughputs, and equipment criticality, among others. As any other model the "garbage in -garbage out" rule applies and the more complex the model the higher the risk that they include mistakes [13]. It is expected that at the early phases of project development the fidelity of these models is expected to be low due to the high levels of uncertainty and limited amount of input data. As the project develops to detail design and execution phases these models can be further refined with more available data. As these models are intended to be useful tools for decision making it is paramount that clear objectives of the modelling activity are well defined and understood by all the stakeholders.

Figure 7 below shows the predicted availability results for one of the future HRS stations that is under development. The simulations are presented in histogram form where it can be seen the range of potential availabilities where P10, P50, and P90 values are indicated.

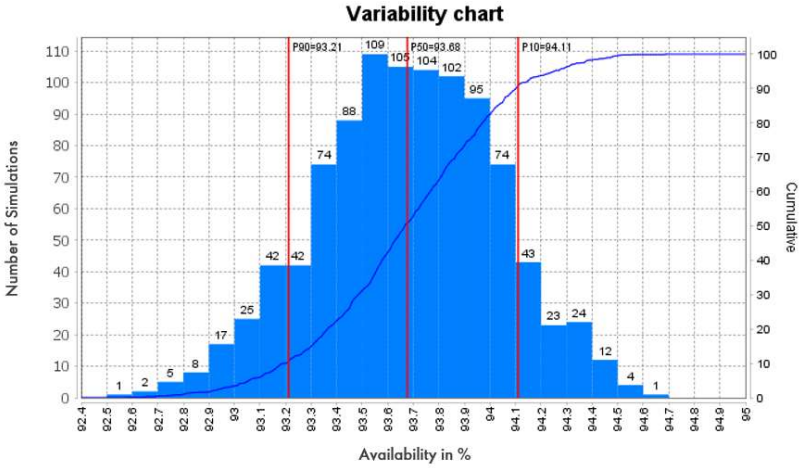

Figure 7. HRS RAM model availability results (10 years lifespan)

Another outcome of this model is criticality classification, i.e. top contributors to unavailability based on categories as shown in figure 8.

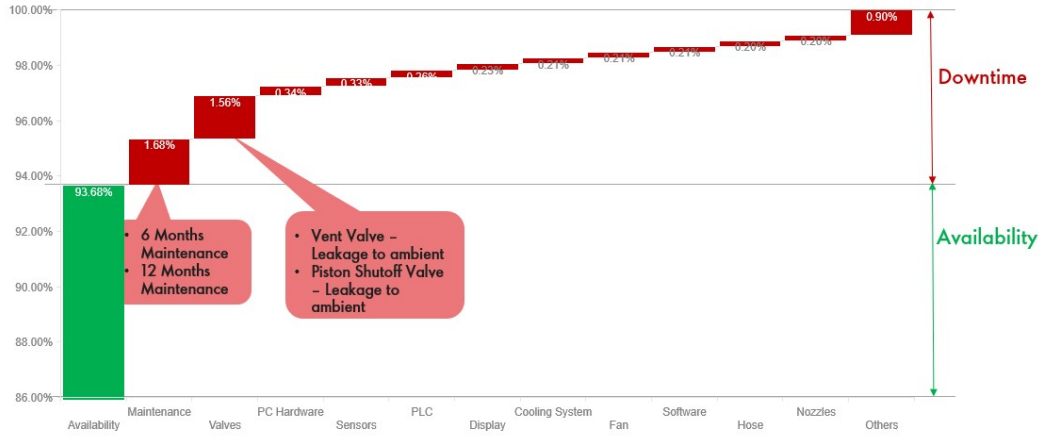

Figure 8. Unavailability breakdown based on planned maintenance and unexpected component failures

These results indicate what the expected downtime is. It also pinpoints potential areas for improvement. As part of the Design for R&S process we use these models extensively to evaluate alternatives, perform trades studies, and assess impact of proposed solutions.

5.0 CHALLENGES AND OPPORTUNITIES

We have described in this document the Shell Hydrogen mobility Design for Reliability and Safety approach and provided examples of early implementation. We are using reliability assessment methods such as Fault Tree Analysis FTA, Failure Modes, and Effects Analysis FMEA, and RAM modelling and simulation, besides the well-established technical safety methods such as HAZOP and HAZID, among others. These methods and tools are aiming at identifying and assessing the safety and reliability risks of the future assets while providing the decision makers enough information to develop and test alternatives to reduce those risks to ALARP in early phases of development. All of this in alignment with Shell HSSE and SP framework and business objectives.

We have faced several challenges during the early phases of implementation, to begin with the limited amount of historical failure and repair data of the systems under assessment brings uncertainty to the process. The way we have mitigated this shortcoming is by using a semiquantitative approach that combines operational experience with hard data. An example of this is the RPN rankings in FMEA, see table 1. We are also building a reliability library with the failure and repair data captured from our Hydrogen operating assets that is accumulating as we get more operational experience.

Another set of challenges comes from the level of credibility of these studies among our partners and stakeholders. Some suppliers have limited capability in these tools and their traditional approach to design does not involve sophisticated risk assessment. We have mitigated this by involving them in the analyses and demonstrating the benefits at preliminary stages of the development process. There is certainly a way ahead for further improvement but so far, the results are promising.

REFERENCES

1. Health Safety Security Environment & Social Performance Management System. Shell International B.V.
2. The definition of ALARP (As Low As Reasonably Practicable) is widely accepted as the point at which the cost (in time, money, and effort) of further reduction is grossly disproportionate to the Risk reduction achieved.
3. Global Hydrogen HEMP standard and recommended practice. Shell International B.V.
4. International Council on Systems Engineering. Systems Engineering Definition (incose.org).
5. Design and Engineering Practice DEP 01.00.002.13-Gen. February 2021. Shell International B.V.
6. O'Connor, D.T. and Kleyner, A. Practical Reliability Engineering, 5th ed. 2012, Wiley, Padstow.
7. IEC 61025 International Standard: Fault Tree Analysis. International Electrotechnical Commission, Second edition 2006-12
8. IEC 61508 International Standard: Functional safety of electrical/electronic/programmable safety-related systems. Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3. International Electrotechnical Commission, Second edition 2010-04
9. ISO/TR 12489 Technical Report. Petroleum, petrochemical and gas industries – Reliability modelling and calculation of safety systems. First Edition 2013-11-01
10. IEC 60812 International Standard: Failure modes and effects analysis (FMEA and FMECA). International Electrotechnical Commission, Edition 3.0 2018-08
11. Moubray, J., Reliability Centred Maintenance, 2nd edition, 1997, Elsevier, Oxford.
12. Bello, J.H., Impact of the pump systems availability in the plant maintenance: model development. MSc Dissertation, 2006, The University of Manchester, UK.
13. Savoie, Troy B., Daniel D. Frey. Detecting Mistakes in Engineering Models: the effects of experimental design. Research in Engineering Design 23, no. 2 April 2012: 155-175, Springer-Verlag