E-Magazine

Qualità nell'Aerospace

Numero uno

Settembre 2020

PROGETTO GRAFICO : **Chiara Graziano**

EDITORIALE

Cari lettori,

Come promesso nello scorso numero" che abbiamo chiamato numero zero" e' con grande piacere che presento il secondo numero dell' E- Magazine Qualità nell' Aerospace. Continua l'iniziativa di AICQ Aerospace di fornire regolarmente degli articoli, novità ed eventi che riguardano la Qualità e Sicurezza dell' Aerospazio sia in Italia che a livello internazionale. Il primo numero ha avuto un notevole successo dimostrando come fosse necessario avere una pubblicazione che parlasse dei temi della Qualità nel mondo Aerospaziale. *AICQ Aerospace vuole diventare, con questa pubblicazione periodica, un punto di riferimento per gli operatori della Qualità , Sicurezza e Affidabilità che lavorano nel settore.* Le competenze presenti nell' Associazione hanno permesso inoltre di avere un piano di formazione dettagliato sui temi della Qualità con docenti che provengono dalle Industrie e Università (ref ultima pagina di questo numero). L'Associazione e' anche ora parte del Distretto Aerospaziale Piemontese (DAP) con la finalità di condividere con le imprese grandi e piccole lo stato dell' arte e le iniziative sul tema strategico della Qualità. Per aggiornamenti , iniziative e novità del settore invito tutti gli interessati a visitare il sito di AICQ Aerospace . Dopo la prima uscita di Maggio sono accaduti diversi eventi, anche con la presenza del COVID, ne cito alcuni: il lancio di diverse Sonde Verso Marte da parte degli Stati Uniti, Emirati arabi e Cina , Il lancio del primo sistema di trasporto commerciale per la Stazione Spaziale Internazionale con Space X , la messa in orbita di ulteriori minisatelliti starlink prodotti sempre da SpaceX per l' accesso globale ad internet in banda larga. Purtroppo la pandemia ha avuto conseguenze al contributo Europeo per l' Esplorazione Marziana con il rinvio , come comunicato da ESA e Roscosmos (L' agenzia Spaziale Russa) del lancio della sonda Exomars al 2022. Tuttavia abbiamo visto in questo periodo come la sicurezza e l' affidabiltà dei sistemi spaziali abbia raggiunto livelli altissimi. A proposito di Sicurezza è di questo i giorni la comunicazione da parte della NASA che c'e' una leggera perdita di Atmosfera sulla Stazione Spaziale Internazionale. Non ci sono al momento problemi per sicurezza degli Astronauti e si sta continuando l'investigazione isolando i moduli singolarmente per identificarne la causa. Penso che nel prossimo numero potremo vedere il risultato di queste verifiche. Questo numero ha l' onore di ospitare un articolo che mi ha mandato uno dei massimi esperti mondiali della Gestione del Rischio nei Progetti Spaziali e dell' Affidabilità Umana "**Joseph Fragola"** attualmente Presidente and CEO di Asti Group, LLC azienda Statunitense dell' Aerospace .L' articolo e' in inglese ma molto interessante poiché fa una analisi critica sull' Approccio nella gestione del Rischio dal programma Apollo allo Space Shuttle ed infine alla Stazione Spaziale Internazionale (chiamata alpha).
Dal passato al presente e futuro, in questo numero abbiamo il prestigio di ospitare un interessante articolo che riporta la recente intervista a **Tommaso Sgobba** Executive Director e fondatore dello IAASS (International Association for the Advancement of Space Safety) sulla "International Space Governance". L' intervista affronta problemi quali i detriti spaziali e l'evoluzione della Sicurezza per i

Programmi Spaziali Commerciali. L'Italia come sappiamo si e' candidata con lo Spazioporto di Grottaglie ad accogliere i voli spaziali turistici della Virgin Galactic. A questo proposito troviamo in questo numero un 'articolo di **Alberto Del Bianco** ex responsabile di Qualità e Sicurezza di ALTEC e attualmente consigliere di AICQ Aerospace che tratta della Sicurezza dei Voli Sub Orbitali. Questo argomento riguarda direttamente il nostro paese e rappresenta la sfida per le prossime missioni con turisti nello spazio. E' possibile vedere il suo intervento su "you tube" al Convegno Nazionale sulla Qualità dell' Aerospace, indirizzo e dettagli nella sezione novità.

Nell' invitare tutti i lettori a contribuire con delle pubblicazioni Vi auguro una buona lettura.

Mario Ferrante
Presidente AICQ settore Aerospace

RISK MANAGEMENT IN US MANNED SPACECRAFT FROM APOLLO 11 TO ALPHA (ISS) AND BEYOND

J. R. Fragola[1]

[1] Science Applications International Corporation, New York, N.Y., USA, Tel: 212-239-8510 Fax: 212- 239-8512

ABSTRACT

As the launch of the first building block for the on-orbit construction of the international space station rapidly approaches, the US space agency is undergoing a transformation. The forces of budgetary pressure are affecting fundamental changes in the way NASA conducts business. Alternatives such as the privatization of space shuttle operations and drastic reductions in personnel once seen as lofty goals now represent the only viable options for agency survival. As has been pointed out recently(1), even in the safety risk management area, NASA can no longer afford the labor intensive qualitative risk management infrastructure that served it so well during the *Apollo* and early space shuttle era.

NASA risk managers will likely soon be faced with the initial start up risks and long term operational challenges of the new space station system while still being required to provide risk oversight of the critical shuttle program operated by a profit motivated private contractor team. Risk managers cannot be expected to fulfill these combined responsibilities in a business-as-usual fashion especially with the realities of personnel reductions. However, pioneering experiments with quantitative risk assessment over the decade since the *Challenger* accident and the recently completed comprehensive risk assessment of the entire space shuttle system and mission offer promise of an alternative approach to the management of spacecraft risk.

This paper reviews the approach taken by NASA toward risk management in the past. Insights are provided into the possible reasons which led NASA to (perhaps wisely) choose a qualitative approach during the *Apollo* and early shuttle eras. The pressure on NASA after the *Challenger* accident to provide quantitative risk estimates is also discussed, as well as the change in risk technology which permitted a detailed shuttle quantitative risk assessment. Examples are provided indicating how the quantitative results of the space shuttle risk assessment have been used to support programmatic decision making on the shuttle program as well as how it might be used along with a set of risk based programmatic indicators to provide risk control of privately managed shuttle operations in the future. Finally, the future promise and challenges of space station *Alpha* and other potential risky human space endeavors are discussed along with the pro-active role that risk management based upon quantitative assessment can play in their development.

1.0 EARLY APPLICATIONS AT NASA

The theoretical basis for quantitative risk assessment was firmly established in time for the birth of NASA and the onset of the *Apollo* program. And yet, NASA shied away from quantitative risk approaches during the course of the program despite evidence of interest early on. In fact, in the months following Kennedy's announcement of the lunar program, the founders of NASA decided that they had to have a quantitative numerical goal for the *Apollo* mission and after discussion, decided that a risk of 1 out of 100 was acceptable for mission completion and 1 out of 1000 was required for returning the crew safely. They also understood that setting a risk of failure goal was not enough, but rather that "identification of potential failures and their risks is essential to a successful design and thus to a successful mission."(2) Further, NASA managers knew that: "Risk is the basic common denominator for decision measurement."(2) This early reasoning led to the development of quantitative risk models which were initiated for all the *Apollo* program elements. The development proceeded along with the program so that by the mid-1960's models or modelling approaches existed at least for the *Apollo* Command and Service Module (CSM)(3), the Lunar Module (LM)(4), and the Saturn V launch vehicle(5).

Despite the availability of these tools and the recognized need to deal with risk in a quantitative fashion, NASA soured to quantitative approaches as the program progressed and fell back on a decision making approach based upon five qualitative factors:

1. Review of all significant equipment modifications incorporated since the last design review and all anticipated modifications not as yet approved.
2. The identification of and the determination of the qualification status of any system component whose failure, by itself, could cause loss of life, stage, or space vehicle (Single Failure Points)
3. A review of all vehicle and special system test results.
4. A review of all significant failures and subsequent corrective actions.

5. A review of unsolved problems, plans for corrective action, and estimated completion dates.

The identification of single failure points was predominantly accomplished by the performance of Failure Mode and Effects Analyses (FMEA). During the course of such analyses, each constituent part of a system was reviewed to determine its potential modes of failure and the subsequent effects which that mode of failure would have upon the component itself, the assembly of which it was a part, the subsystem, system, vehicle, mission, and crew. This bottom-up analysis was thereby intended to identify individual components whose failure might put the mission at risk. The analysis also indicated potential approaches that could be implemented within the existing design or, alternatively, possible design changes which might be made either to eliminate the failure mode, reduce its frequency to a acceptably low level, or mitigate its consequences. In this way, an FMEA exhibited some of the features expected of a risk analysis. Single failures which could not be eliminated or mitigated were collected across the design along with the rationale as to why they were retained and a list of all those identified SPFs were included in a Critical Items List (CIL). This list allowed the items to receive special attention in development, manufacture, installation, and test. Since the FMEAs and their associated CILs were critical determinants in the five factor decision process described above, the process as a whole is often referred to as the "FMEA/CIL" process. The FMEA/CIL process therefore was a static qualitative, bottom-up approach oriented toward assessing and reducing the risk of single independent component failures causing the loss of crew, vehicle, or mission.

2.0 FMEA/CIL PROCESS DRAWBACKS

While the FMEA/CIL approach certainly proved to be successful in producing reliable spacecraft and launch vehicles (based upon the success of *Apollo*), each of its characteristic features carried with them some drawback. An extended discussion of these drawbacks has been provided elsewhere[6], however, the following list provides a summary of the problems:

- No natural probability cutoff
- No risk focus
- Directed at single independent failures ignoring correlated failure or common cause failure impact
- Difficulties in incorporating human and software errors
- Difficulties in dealing with dynamic situations
- No systematic approach for identifying and dealing with uncertainties
- Significant financial cost in terms of test and personnel resources

Given the drawbacks of the FMEA/CIL process and the original intent of NASA to obtain quantitative assessments of risk, it is logical to ask why NASA would turn its back on quantitative assessment and so tightly embrace a qualitative approach with so many known problems. The answer to such a question is of course, at least to some degree, somewhat speculative, but the writer's experience and the available historical evidence provide support to one possible answer. The evidence is as follows: 1. Many of the defects of the FMEA/CIL process were not that serious given the environment extant during the *Apollo* era; 2. those that were serious were not adequately addressed by the quantitative approaches available at the time anyway; 3. the predictions available from existing quantitative models were completely unacceptable and inaccurate as forecasts of the risk "to be incurred" during an actual mission; and 4. abundant personnel and test facility resources were provided to establish the needed confidence that each critical item had been properly addressed.

Also, while rather primitive human error quantification approaches did exist at the time[7],[8] they were developed for process oriented and not control oriented tasks and would not be ready to address control oriented tasks for at least another decade and a half. Further, if human error quantification techniques were lacking, software techniques were essentially nonexistent. The first symposium on the subject was not even held until 1973[9]! Several years *after* the first manned lunar landing. As for the problems in dealing with common cause failures, dynamic situations and uncertainties, the available quantitative techniques of the day (i.e., fault trees, and reliability block diagrams) included no common cause failure approach, were also basically static when applied, and rarely, if ever, addressed uncertainties.

3.0 QUANTITATIVE ANALYSIS - A FALL FROM GRACE

As noted above, the quantitative approaches available in the 1960s appeared not to offer very much above the qualitative to recommend them. That alone might have been enough to doom quantitative analysis. However, in the writer's opinion, what assured the demise of quantitative analysis was that its predictions were *bad*. Bad in the sense that the predicted failure probabilities were so high that they appeared to be obviously inconsistent with the test and early unmanned flight experience. The exact predicted values for the entire mission were not able to be resurrected for this paper (they were actually one of the few things classified in the entire lunar program at the time). However, various sources place the Saturn V launch

vehicle mission success point estimate at about .88[2] and the writer's recollection was that the CSM and LM estimates were .90 and .95. These estimates would indicate an overall mission failure rate or risk of one in four missions (or a mission success probability of .75)[1]. Also, in the writer's recollection, these final point values resulted after review and update of initial estimates which were significantly worse! Why did these estimates appear so wrong to the project team (and hindsight appears to have borne out their viewpoint since there was only one mission failure, *Apollo* 13, in the entire program and the mean mission risk demonstrated was about 4 times lower)? More importantly, why were the predictions developed by the reliability analysts such poor forecasts? Again, although any answer has to be considered speculative, the following rationale seems supported by the evidence.

The decision makers at NASA (and by the way not the traditional NACA types and the Huntsville "Germans"; at least not at first according to one source[10]), seemed to fully recognize that there was no possibility of flying enough test missions to be confident in the system because of the number of times it worked. They seemed to know instinctively that the only way they could build up the "infrastructure of confidence"[11] required to give the go-ahead for a manned lunar flight was by structuring it from the engineering insights gained in development and the growth observed in the testing conducted. Thus they knew, because of the significant learning process expected and planned for, that significant growth in reliability would occur in the system throughout development. They reasoned that the history of past programs and early failures in *Apollo* only indicated what the reliability of the system had been in the past, not what its performance was *forecasted to be* over the spectrum of actual manned missions. In this way, they heuristically structured their design and testing processes not so much to be investigative, but rather to be confirmatory. They would *expect* the design to perform at flight levels so they would test at levels well above those expected during flight to provide them confidence that performance at flight levels would be assured. Thus, designs were robust, failures at flight levels were few, and the root cause analysis and corrective action programs ensured that those that did occur would tend to occur early enough in the test program so that their root cause could be eliminated. From this perspective, the decision makers had great confidence that even though estimates made from the scant early program history available and the history of past programs and equipment might indicate a mission risk of one in four launches, the actual risk was much lower.

On the other hand, the reliability analysts of the day were just beginning to address the issues of reliability growth and other alternatives for forecasting the risk in developing systems. While the theoretical basis was well established, practical applications for approaches such as the Bayesian combination of history, test and flight data were lacking. Since these approaches were considered experimental at the time, it is likely that the analysts based their predictions on a classical estimate derived directly from the test data and the history that was available, without growth considerations. For the reasons mentioned above, the test data available were extremely pessimistic. Further, the past flight experience was not at all good. (A recently declassified report[12] indicates just how bad it was. The report issued just one month prior to the Kennedy moonshot announcement indicated that US ballistic missiles had only a 70% success rate and that only 50% of US spacecraft had reached successful orbits). Given these considerations, it should not be at all surprising that quantitative estimates, even when properly performed, would significantly underestimate the actual in-service reliability. From such a pessimistic viewpoint, the forecasts produced were likely to be unrealistically unflattering to the program. Additionally, they were available so late in the program as to be of little use in design improvements, even in the relative sense, where they might have had at least some value. Therefore, the entire exercise might well have been viewed as counter-productive.

Whatever the actual reason might have been for quantitative assessment's fall from grace, it was certainly the case that these estimates were not widely circulated even within NASA and were sparingly, if ever, released to the public at large. With the quantitative exercise too late to be of aid as a design tool and counter-productive when eventually available, it is not surprising that the qualitative FMEA/CIL process (which had been seen as widely useful and, though somewhat ex post facto, much more timely) was therefore seen as the far superior approach. While the above scenario might not be entirely accurate it does provide one plausible explanation as to why the FMEA/CIL process received full endorsement in the subsequent Shuttle era and why quantitative approaches, at least comprehensive system level ones, were not employed again by NASA and its contractors until after the 51L mission (the ill-fated *Challenger* mission of 28 January 1986).

Early attempts at reducing probabilistic models to allow for quantification had been tried at Grumman[4] and North American[3] during *Apollo*, as was mentioned. These attempts had represented the Boolean equations derived from Reliability Block Diagrams (RBDs) in terms of event sets which approximated the

probability of success rather well in the case where each event had a reasonably high probability. Soon thereafter, techniques surfaced in the nuclear industry which took advantage of the network dualism of RBDs[2] and Fault Trees to represent the failure to perform the top event of a fault tree in terms of its minimal cutsets[3] (i.e., cutsets with no repeated events).

Despite the fact that the initial technical infrastructure for improved quantitative assessment was in place well before the first flight of the space shuttle on 12 April 1981, NASA took little note of these developments. This was not because NASA and Aerospace contractor personnel were ignorant of the ongoing efforts. There had been joint inter-industry exchanges in the intervening interval. For example, Mr. Eugene Kranz, the famed *Apollo* 13 flight director, had participated in one notable exchange(13), and additional NASA and industry representatives had participated in others(14). While these exchanges continued until the 51L mission, they had no perceptible influence on the NASA policy which continued to endorse the qualitative FMEA/CIL process.

4.0 THE AFTERMATH OF 5IL

The Rogers Commission(15), impaneled to investigate the *Challenger* accident, (especially the indefatigable Professor Richard Feynman(16)) recommended that NASA reconsider quantitative approaches and in fact by the time the Slay Commission(17) put forth its even more strongly worded suggestions for quantitative assessment initiatives, NASA already had two PRA "Proof-of-Concept" studies underway. These initially limited efforts focused on particular shuttle systems with the objective of indicating potential benefits to be gained from the quantitative approach over the traditional FMEA/CIL process. One study was performed on the Shuttle Auxiliary Power System(18) and its three Auxiliary Power Units (APUs), and the other on the Main Propulsion Pressurization Subsystem (MPPS)(19).

The former study in particular provided initial insight into the power of quantitative approaches. Although the executive summary seems to have missed the point, the study indicated the danger of measuring the risk by the number of items on the CIL. What it clearly showed was that while all items on the list had the *potential* of causing crew or mission loss, some were *far more likely* to be the cause. In fact a small minority of the CIL listed items contributed the overwhelming percentage of the risk. The quantitative analysis demonstrated that "not all CIL listed items are equal" even though they were theoretically to be treated so in terms of management and engineering attention. Further the study showed that several significant risk contributing failure modes were not even on the list and that some of these were ones with significant common cause failure potential.

At about the same time, an effort was undertaken under the auspices of the shuttle integration office at JSC in Houston. This study which went through a number of name changes became known as the "Shuttle Integrated Risk Assessment"(20). Despite the implication of its name, the study focused initially and primarily on a linked functionality assessment of the Shuttle Main Propulsion System Propellant Management System. Although the thrust varied considerably from a conventional quantitative risk analysis, the effort did introduce the concept of Probabilistic Risk Assessment (PRA), which had been significantly developed in the nuclear power industry as described elsewhere(21), to a broader segment of the NASA and contractor community.

Soon thereafter the first associate administrator of the recently created Office of Safety, Reliability, and Quality Assurance (Code Q) established a new Safety Division staff position in risk assessment. One of the first assignments of this newly selected individual was to review the risk study submitted by the *Galileo* program to INSRP and to recommend that an independent quantitative study be undertaken by NASA Code Q using a PRA approach. This study, when completed, represented the first quantitative assessment of the risk of the total shuttle system. Although it was limited to the ascent portion of the mission, was necessarily top level in nature, and focused primarily upon scenarios which presented a risk to the *Galileo* nuclear payload, it differed dramatically in kind and in its results from the previous effort undertaken by the payload program office. The study indicated that the loss of vehicle probability of the shuttle was uncertain, to be sure, considering the limited availability of information, however despite this fact, the 90% uncertainty range (based upon all the shuttle flight and test history available at the time, even considering substantial growth in reliability, but keeping the design and operational configuration constant) was between 1/350 and 1/18 missions with a median estimate of 1/78(22). This was far from the 1/1000 to 1/10,000 missions that some had been quoting even after 5IL. Many NASA personnel, perhaps with lingering memories of *Apollo*, widely criticized the study for what were believed to be its pessimistic predictions. However, Code Q stood by the findings, allowing for changes only if new evidence would be presented. Further, contrary to past tradition, Code Q released the study results to the press and they were widely

quoted[23]. Despite the initial furor and predictions of dire results on shuttle funding, the program continued and those who cared to look beyond the traditional view began to see uses for the study. It soon ceased to be the Code Q study and was endorsed by all NASA as the *Galileo* input to INSRP. Further, because of its systematic traceable nature and its familiar format to the courts (in dealing with Nuclear Power intervenor suits), it was used as evidence in a suit brought to delay the *Galileo* launch. The study's prediction of low public risk despite NASA's forthright admission of possible high shuttle failure probability convinced the court to deny the intervenor's petition and the launch proceeded on schedule.

Soon the controversial nature of the study had been so diminished that its approach was unanimously endorsed by both the program and Code Q for the INSRP submittal for the *Ulysses* nuclear powered payload[24]. The study proceeded without fanfare and the launch again was not delayed. Then the approach began to get wider exposure within NASA. It was applied to problems as diverse as wind tunnel design[25], the assessment of the viability of leak checking the field joint of the proposed Advanced Solid Rocket Motor[26], the support of the 1990 Space Station design via EVA maintenance[27], the structure and nature of redesign solutions[28], and the assessment of the risk of launch delay and other factors on the ability of the current station design to maintain a berthable attitude[29].

The deputy associate administrator for space flight was impressed enough with the power of the quantitative risk approach from his experience as the station redesign team leader that when he was asked to set priorities for shuttle redesign options and assess the safety benefit of each, he decided to apply the *Galileo* study results to the task. He recognized that although these results did not include the benefit of the design changes implemented since the study was performed and did not include the significant flight and test history which had subsequently been incurred, it was the best information available. This initial success caused a more comprehensive study of the space shuttle risk to be undertaken, in two phases. The first phase used the same basis as the *Galileo* Study but included the intervening design changes and history. The second phase was to undertake a comprehensive investigation of space shuttle risk throughout all mission phases from main engine start on lift-off to nose-wheel stop on touchdown. In addition, the study was also to go into greater depth in risk significant areas, investigating the element risk drivers down to individual components in some cases. The study was also to utilize, to the maximum extent possible, not only NASA experience but also contractor experience in an attempt to credit the unique features of the shuttle design and test program as well as the unique insights provided by its reusability.

Finally, an important feature of the work to be accomplished in this phase was to leave NASA with a "living" model of the mission risk. This living model and its current and potential future applicability to shuttle program risk management are discussed in the following sections.

5.0 RISK MANAGEMENT AND THE LIVING SHUTTLE RISK MODEL

While quantitative risk assessments were being reintroduced into NASA space programs, the technology of risk assessment continued to progress. Advances in computer hardware and newer, much faster, quantification algorithms reduced quantification times from days, to overnight, and then to hours. In addition, the crude workstations initially available became integrated packages with added data preprocessors and analysis post processors. Event trees could be automatically linked to all the appropriate fault trees and data in the data base could be automatically linked to the fault tree basic event set. The previously tedious task of drawing the fault trees and the even more tedious task of configuration control of changes to them was now implemented automatically. Analysts could use a short-hand, very fast, graphical method to generate the event trees and fault trees and these cryptic and basic screen models would automatically generate beautiful output trees. With the advent of postscript type laser printers, the task was even simpler and codes took advantage of the standard output format to implement automatic pagination and automatic input-output transfers from one tree to another. Routines were even available for automatically creating modular events from groups of independent lower level events to aid in rapid quantification. Currently, with the advent of the newest generation laptop PCs, an entire nuclear plant Level I PRA (i.e., one that tracks initiators until the onset of damage to the reactor core) can now be quantified in tens of minutes to an hour. The PRA in this way has become "living" in the sense that it allows the "vital signs" of the plant to be continually monitored and interrogates them in terms of their risk impact.

The risk assessment recently completed for the space shuttle has been performed in a similar fashion. The entire model is implemented on a PC or laptop. Quantification can take place as fast as 10 minutes, if gate probabilities are not desired, or 20 minutes if they are. An entire Monte Carlo based uncertainty propagation analysis based upon 5000 samples of each significant sequence can be completed in less than 15 minutes. In addition, ongoing programmatic data can

be input regularly to detect potential adverse trends, recent design changes can be evaluated for risk reduction potential, and proposed design changes can be evaluated on a cost benefit risk reduction basis.

6.0 RISK MANAGEMENT IN THE CURRENT SHUTTLE PRA

The shuttle PRA, as it exists in its currently available form, is extremely useful for ongoing risk related decision making. Two examples which are drawn from actual considerations, but which have been simplified for ease of illustration, are provided here. The first example involves the evaluation of possible design changes to the shuttle APU system and the second is related to aiding in making the decision to continue to fly after observing abnormal conditions during the post-flight inspection of the shuttle Redesigned Solid Rocket Motors (RSRM).

6.1 APU EXAMPLE

The shuttle PRA indicated that 10% of the overall operational risk is contributed by potential hydrazine leakage in the shuttle APUs. Such a significant contribution would make this problem a candidate for mitigation via redesign. For this example, consider two possible re-design approaches:

1. Hydrazine plumbing redesign to make it less susceptible to leakage (e.g., cast vs. welded piping).
2. Replacement of hydrazine fueled APUs with electric APUs.

For the first design alternative, investigations could be made into the effectiveness of cast piping in leak reduction in hydrazine systems. Data could be developed from existing design experience in other applications or from prototypical APU plumbing tests. From whatever the source, these data could be combined to modify the leakage failure rate estimate used in the APU leakage related basic event cut sets. The model could then be requantified using the new leakage probabilities. If it is assumed that by using cast plumbing we could reduce this leakage risk from 8.57E-2 to 2.00E-2, the PRA indicates that we would obtain a corresponding reduction in the overall shuttle LOV risk of 6.57%, a significant risk benefit. On the other hand, if we consider replacing the hydrazine fueled APUs with electric APUs, the change could eliminate all leakage induced failures and, if it did not introduce any significant new risk contributing failure modes, there would be a 10% improvement in risk.

Therefore, on the basis of risk reduction alone, electric APUs would be preferred. However, the costs of certifying and qualifying a completely new APU design could be considerable so the potential increased risk benefit must be considered in light of the cost to implement the design change. The benefit of risk reduction has been considered as loss protection against the loss of a shuttle and the cost of a shuttle loss is estimated at $5 billion. While the loss prevention benefit of electric APUs is higher than improving the plumbing ($500M vs. $300M), the cost to implement electric APUs is much higher ($950M vs. $250M). Therefore not only would the electric APU option be more than three times more expensive, it would also exceed the potential gain in loss protection by $450M. For this reason the electric APU option would not be cost effective in terms of potential loss protection benefit alone. Of course these costs should only be considered hypothetical and any cost estimate should also include an uncertainty estimate as well. Further, there may well be more than monetary benefits to consider as a result of risk reduction so the risk assessment should not be seen as *the* answer to a risk related decision, but it should be evident how useful a quantitative risk assessment is in *aiding* the decision maker.

6.2 RSRM NOZZLE JOINT NO. 3 RTV BLOWBY PROBLEM

On post flight analysis it was determined that on STS-71 the left hand RSRM nozzle joint Number 3 had experienced a blowby event (i.e., hot gas had blown-by the Room Temperature Vulcanizing (RTV) material, a thermal putty type material, and impinged on the primary O-ring seal). Joint No. 3 joins the nose inlet assembly to the throat support assembly. While evidence of blow-by had previously been experienced 11 times, this particular event was of concern because, for the first time, noticeable erosion had occurred on the primary O-ring seal in four (4) areas just downstream of the RTV backfill area. Downstream of the backfill are primary and secondary O-rings with a leak check port in-between. These two O-rings track any small movement in the nozzle joint and are introduced to form a redundant barrel seal against an external blowby event. A similar but less severe event occurred on the subsequent shuttle mission (the out of sequence STS-70 mission) on one RSRM. Because solid rocket booster double O-ring barrel seal failure had been the cause of 5IL, these new events concerned NASA to the degree that a decision had to be made whether it was safe to continue shuttle flights without a change in design or whether flights should be suspended pending modifications.

The double O-ring seals represent both a thermal and a pressure barrier to prevent the hot gases from the burning fuel from escaping. The problem is that any breach of the seal integrity, such as its inability to track

gap opening (the 5IL problem), or damage to the surface, improper installation, or any other mechanism which would create even a small gas pathway will quickly lead to a total seal breach. However, even if the primary O-ring is breached, the secondary O-ring is fully capable of performing the seal function unless it too, is compromised by a common cause failure event.

At the time of the PRA, it was discovered that out of 88 relevant hot firings (flights and static tests) there had been 10 RTV penetration events (an additional one occurred after PRA completion to make the total 11). This initiator frequency of 1 out of 7 flights was initially disturbing to the PRA team. However the significant flight history, static test history, and leak check history indicated that the probability of breaching the first O-ring is about 1 in 1000 flights. Additionally, if the second O-ring was considered as redundant, then the dual seal would only have an estimated risk of 1 in one million flights. For this reason, the concern at the time of the PRA was directed at the common cause failure potential for a dual O-ring seal breach because the seals were close together and on the same face. The common cause failure frequency was estimated conservatively to be one tenth that of the independent O-ring failure probability or about 1 in 7000 flights (still low but considerably higher than one in a million). With an overall LOV probability estimated at 1 in 131 flights, this risk represented a non-negligible, but certainly not a driving contributor, and therefore did not elicit undue concern.

What occurred in the STS-71 flight raised a new concern. The erosion observed in the primary O-ring, even though minor, indicated the possibility that a concentrated hot gas stream had impinged on a local area of the O-ring causing the erosion observed. If such a gas jet did occur, and if it were sustained, the initial backfill penetration could by itself cause a breach of initially the first O-ring and then the second. While a correlated effect of this type is by no means certain, even a correlation of only 10% between the gas jet initiator and the dual O-ring seal failure would cause this event to become one of the dominant contributors to overall LOV risk. This one event would raise the mission risk by 16% to a 1 in 110 mission level. If the failures were completely correlated the overall mission risk would be increased by 65% to a 1 in 45 mission level; a very significant increase indeed. The PRA insights into this problem provide a way to quickly focus the activity on the possible mechanisms which might cause this potential common cause initiator, and on the sustainability of the problem when it did occur. Such analytical investigations might indicate that near term continuance of shuttle flights was a risk worth taking. However, even if that decision were made the PRA shows the potential significance of the problem in the longer term and thereby helps to establish priorities for its elimination via design or via procedural changes in assembly later on. As it turned out shuttle mission managers decided to be conservative and delay the launch of the next mission (STS-69) at least until the O-ring issue was more thoroughly examined.

7.0 USE OF THE SHUTTLE PRA IN RISK CONTROL IN A CONSTRAINED BUDGET ENVIRONMENT

The above two examples provide an indication of how the current operationally related shuttle PRA could be used to treat individual issues raised as risk drivers, or to deal with the occurrence of hitherto unobserved phenomena. An additional, perhaps more significant, use of the shuttle PRA is in managing the operational risk as budgets are significantly reduced. This concept of Zero Based Risk Management begins by applying the simple principle of reducing the operational steps needed to process anything to the steps actually required to implement a process function. For the shuttle, the essential steps are those absolutely required to be able to launch the next flight. Surviving steps are considered for possible restructuring for further step reduction. Once reduced to a minimal set, the remaining steps include no test or check out steps at all, no post-flight investigations, no maintenance actions, nothing but what is necessary to load the payload and enable launch. This becomes the Zero Base. The set of zero based launch process steps are then reviewed and ranked according to their importance to each of the shuttle mission risk contributors. In this way, the differential risk incurred as a result of the elimination of the associated assurance related process steps can be assessed. When this assessment is completed, the assurance steps are evaluated in terms of their historically documented effectiveness in identifying or eliminating precursors to mission risk scenarios, the associated risk mitigated, and the associated implementation cost required. Assurance steps are then added to the front-line processing steps needed for launch one at a time or in groups on a cost/risk reduction priority basis until an estimated risk goal consistent with the currently accepted flight risk is obtained. All additional assurance steps are identified as candidates for frequency reduction or elimination subject to program management review. A series of risk-based processing indicators can then be established and tracked based upon measurable process parameters to identify, and to direct management attention to, any process risk increases. Finally, a "living" process risk management program is established. This program allows accumulating flight experience to be used systematically and increasingly to supplement the assurance provided by the residual ground processing assurance steps and thereby allows for their decrease in

frequency and eventual elimination in light of the growing base of flight experience.

Such a system of processing risk management, utilizing the shuttle PRA as a backdrop, might offer direct assistance toward the solution of the shuttle operations cost vs. safety risk dilemma. Managing shuttle processing in this way maintains in place only those assurance tasks with the highest mitigation cost-effectiveness and might permit shuttle operational experience to be substituted for process step assurance in an orderly fashion, thereby maintaining shuttle flight frequency without risk increases even in the severely constrained budgetary environments of the future. It also might provide a way for NASA to be provided with assurance that the current shuttle safety level is not compromised if shuttle operations are transferred (as seems to be increasingly likely)[30] to a private contractor operating under a profit motive.

8.0 *ALPHA* RISK MANAGEMENT AND BEYOND

Quantitative risk assessment has already been applied to the assessment of EVA maintenance requirements[27], and the ability of the space station to maintain a berthable attitude[29]. In this way quantitative risk assessment has already influenced the design. While it is true that quantitative approaches have been useful up to now their potential usefulness in the future offers even greater promise. Consider that *Alpha* is the first truly international space enterprise. That is, it represents the first permanent union of US and Russian spacecraft technology. Also consider that while the "western" international partners involved in the space station program have all been immersed in the NASA qualitative risk management culture the Russian approach derives more closely from the classical approach to risk management. That is, they have gained their design confidence through successful flight experience with relatively static designs rather than structuring it from engineering insights and growth gained throughout development.

The Bayesian or learning-based nature of quantitative risk models allows both approaches toward establishing the infrastructure of confidence necessary for flight to be evaluated on a level playing field basis. The Russian experience can be evaluated against the tolerance uncertainties associated with applying a well understood design in an unfamiliar design environment, while the uncertainty assciated with the use-specific western designs can be evaluated in terms of scant, but risk focused, test experience. In this way quantitative risk assessment allows uncertainty to be used as the common currency for design evaluations and tradeoffs. Using uncertainty in this way allows a well known design (with significant in-space experience but limited analysis and test pedigree), to be understood in comparison with a new design, (with limited flight experience but significant analysis and test pedigree). Providing a common basis for understanding the risk incurred by various elements of the space station design can also assist management in assigning test or redesign resources in the areas where they would provide the most cost effective risk benefit.

Further, if a fully integrated space station risk assessment is incorporated into a living model of the space station throughout its deployment phase until full human- tended capability is reached, then the model can be used in real time for risk management. The risk impact of alternatives that they may face throughout the deployment cycle due to failures or deployment delays as well as the risk reduction benefit of options available to them can thereby be assessed on a continuing basis. In addition, once full human-tended capability is achieved the risk assessment living model can be deployed on the station itself to monitor the incremental risk impact of routine and ongoing activities such as preventative or corrective maintenance. This would allow planners to avoid periods of unsuspectedly high risk. The risk model so deployed would also provide the station with a damage assessment and emergency response planning tool. Such a tool would allow the station crew to rapidly assess the extent and risk impact incurred by natural, human, or equipment failure induced upset conditions and to determine the best course of action to assure recovery of maximum capability. The tool could also be used interactively in far more serious conditions to determine when evacuation to a "safe-haven" or abandonment of the entire station might be required. Such a use has distinct advantages over the relatively static mission rules used in the past especially as they might be applied to long term facilities such as *Alpha* since the history of experience with operation can be factored into the model on an ongoing basis as well as the specifics of the particular upset condition. A combination of actual history in a risk structured format along with the particulars of the immediate problem can provide the station crew members and their limited ground supporting personnel with an immediate, flexible, and effective risk based decision making tool.

Finally, quantitative risk assessment provides a way for new advanced concepts to be evaluated. Even at the conceptual stages quantitative approaches have indicated the viability of various strategies toward the achievement of mission objectives. They also can provide insight as to where the mission risk drivers are and what the limitations are to the achievement of key mission objectives. In this way, quantitative risk assessment can be a valuable tool for the establishment

of viable programmatic alternatives and for indicating the key mission uncertainties which might be addressed by test or via interim development. The approach can also aid in minimizing the possibility that apparently promising approaches are not pursued in a fashion which leaves mission planners without alternatives in case their promise is not forthcoming.

If properly developed, integrated, and implemented quantitative risk assessment may provide a significant aid to effective design decision making in a manner consistent with the rapid development of advanced designs within a constrained budgetary environment. Risk management offers the promise that the admirable safety levels achieved throughout the history of human spaceflight might be maintained despite the inherently risky nature of past and future endeavors. It provides us with a mechanism to better assure ourselves that whatever level of human spaceflight risk we find acceptable our designs will be effectively balanced to properly address the contributors to the risk. Finally, and perhaps most importantly, it may provide a way to continue to aggressively pursue ambitious goals even within limited budgets, provided we are willing to accept the risks that can now be more clearly identified.

10.0 ACKNOWLEDGEMENTS

The writer would like to thank Mr. David Whittle of NASA JSC and Mr. Bryan O'Connor of NASA Headquarters for supporting some of the work upon which this paper has been based. He would also like to recognize the pioneering efforts of Mr. Benjamin Buchbinder formerly of NASA Headquarters now with Futron Corporation. Without the vision and perseverance of Mr. Buchbinder, it is unlikely that the paradigm shift that has been occurring at NASA over the past year would have occurred. The writer would like to thank Mr. Gaspare Maggio of SAIC for his contributions to the performance of the Shuttle PRA mentioned herein, and finally special thanks to Mr. Darrell Walton and Ms. Erin Collins of SAIC for their assistance in the preparation of this manuscript.

11.0 REFERENCES

[1] Kraft, C., "Report of Shuttle Management Review Team", NASA JSC, February 1995.

[2] Cato, R.E. Jr. and Wheadon, W.C., "The Impact of Failure Data on Management of a Launch Operations Reliability Program", *Annals of Assurance Sciences*, 8th Reliability and Maintainability Conference Proceedings, 7-9 July 1969, Gordon & Breach, New York, 1969. LCN64-22868

[3] McKnight, C.W. et al, "Automatic Reliability Mathematical Model", North American Aviation, Inc., Downey, CA, NA66-838, 1966.

[4] Weisburg, S.A. and Schmidt, J.H., "Computer Technique for Estimating System Reliability", Proceedings 1966 Annual Symposium on Reliability, pp. 87-97.

[5] _____, "Saturn V Reliability Analysis Model Summary", SA-502, MSFC Drawing No. 10M30570, August 1967, NASA/MSFC, Huntsville, AL.

[6] Fragola, J.R., "Space Shuttle Program Risk Management", Reliability Availability Maintainability Symposium (RAMS) 96, Las Vegas, NV, January 1996.

[7] Swain, A.D., Altman, J.W., and ROOK, L.W., *Human Error Quantification: A Symposium*, SCR-610, Sandia National Laboratories, Albuquerque, NM, April 1963.

[8] Meister, D., "Methods of Predicting Human Reliability in Man-Machine Systems, *Human Factors*, 1964, pp 621-646.

[9] _____, Proceedings of the 1973 IEEE Symposium on Computer Software Reliability, IEEE, New York, 30 April-2May, 1993, Cat No. 73CH0741-9CSR.

[10] Murray, C. and Cox, C.B., *Apollo: The Race to the Moon*, Simon and Schuster, NY, 1989.

[11] Fragola, J.R., "Reliability and Risk Analysis Data Base Development, An Historical Perspective", submitted to Reliability Engineering and System Safety, special issue on Reliability Data Bases, Elsevier - North Holland, Amsterdam, The Netherlands.

[12] Moody, J.W., "Reliability of Ballistic Missiles and Space Vehicles", Working Paper, Reliability Office, George C. Marshall Space Center, Huntsville, AL, April 15, 1961.

[13] T.Schmall (ed), *Conference Record for 1979 IEEE Standards Workshop on Human Factors and Nuclear Safety*, Institute of Electrical and Electronics Engineers, 1980.

[14] _____, Proceedings of the AIAA/EPRI Aerospace-Electrical Power Conference, Williamsburg VA, 1981.

[15] Rogers, W. et al., "Report of the Presidential Commission on the Space Shuttle *Challenger* Accident", Washington DC, 1986.

[16] Feynman, R., "Personal Observations of Reliability of the Shuttle", Appendix IIF in Rogers, et al, Ref. [15].

[17] Slay et al, "Post-*Challenger* Evaluation of Space Shuttle Risk Assessment and Management", National Research Council Report, National Academy of Sciences, National Academy Press, Washington, DC, January 1988.

[18] _____, "Space Shuttle Risk Assessment Proof-of-Concept Study, Auxiliary Power Unit and Hydraulic Power Unit Analysis Report", McDonnell Douglas Corp., 18 December 1987.

[19] Plastiris, J. et al, "Space Shuttle Main Propulsion Pressurization System Probabilistic Risk Assessment", Final Report, Lockheed Corp., Palo Alto, CA, 1988.

[20] Robitaille, R. et al, "Shuttle Integrated Risk Assessment (SIRA) Program Main Propulsion System Propellant Management System", Rockwell International Corp. April 1991.

[21] Fragola, J.R., "Space Shuttle Probabilistic Risk Assessment", to be presented at the International Conference Probabilistic Safety Assessment and Management (PSAM III), Crete, Greece, June 1996.

[22] Buchbinder, B., "Independent Assessment of Shuttle Accident Scenario Probabilities for the *Galileo* Mission", Vol. 1, April 1989, NASA/HQ Code QS, Washington, DC, 20546.

[23] Broad, W.J., "High Risk of New Shuttle Disaster Leads NASA to Consider Options", *N.Y. Times*, Sunday April 9, 1989.

[24] *Ulysses* PRA

[25] Frank, M.V. and Epstein, S.A., "Turbine Blade Trade Study: A Risk and Decision Analysis", Safety Factor Associates, NASA/Ames Research Center, February 1993.

[26] Appignani, P.L., Fragola, J.R., and Frank, M.V., "Decision Analysis for ASRM Field Joint Leak Check", Risk Management Seminar, Goddard Space Flight Center, 23-25 September 1992.

[27] Fisher, W.F. and Price, C.R. et al, "External Maintenance Task Team", Final Report, Vol. 1, NASA/JSC, Houston, TX, 1990.

[28] Johnson, G.E. et al, "Space Station *Freedom* External Maintenance Solutions Team", Final Report, NASA/JSC, Houston, TX, 1991.

[29] Fragola, J.R. and McFadden, R.W., "Technical Report, SAIC/NY 93-09-27 An Analysis of Selected Risk Factors and Uncertainties for Space Station Assembly Up to Human Tended Condition for Space Station Transition Options A1 and A2", SAIC, New York, 30 September 1993.

[30] Iannotta, B., "Firms Double-Team Shuttle Management Issue", *Space News*, August 7-13, 1995, pg. 3.

---

[1].The goals established for the *Apollo* program given below (from "The *Apollo* Spacecraft-A Chronology", NASA/HQ, 1969.) were higher and consistent with the actual mission success performance of the program. The crew safety goal was identical to the 1 out of 1000 discussed previously, and not inconsistent with the perfect Apollo crew safety performance record:

	Mission	**Crew**
	Success	**Safety**
Apollo Spacecraft (CSM):	0.9638	.99958
Apollo-Saturn System:	0.9	.999
Lunar Module (LM):	0.984	.9995

[2].A network dual is generally formed by replacing the nodes with the edges and the edges with the nodes. In a logical network it also requires negation, i.e., converting success into failure and union to intersection and vice versa.

[3].A cut set is a set of events that causes the occurrence of the top event. Since in a fault tree the top event is a loss of function it "cuts off" the functionality of the system.

T. SGOBBA AIAA Podcast July 30, 2020
Participants: Tommaso Sgobba (IAASS), Scott Kordella (MITRE), Thomas Dorame (Space Foundation), Steve Sidorek (AIAA), Christian Zur (US Chamber of Commerce)

Scott Kordella:
Welcome to episode seven of the space policy pod, brought to you by AIAA, the Space Foundation, the US Chamber of Commerce and the MITRE Corporation. My name is Scott Kordella, Director of Space Systems at MITRE and its my privilege to serve as the host of this space policy pod episode.

Today we are fortunate to have as our guest, Mr. Tommaso Sgobba, Executive Director of the International Association for the Advancement of Space Safety, located in The Netherlands.

Joining us in this discussion is Thomas Dorame with the Space Foundation, Steve Sidorek with the American Institute of Aeronautics and Astronautics and Christian Zur of the US Chamber of Commerce. Before I hand it over to my fellow podcast colleagues for the balance of the show, I would like to yield to Tommaso to get the conversation started and walk us through some of the major activities and challenges that have emerged over the past few months. Tommaso…

Tommaso Sgobba (~5 minutes; high-level talking points):
Hi, good morning. I want to thank you very much for this opportunity. Today I am here to talk about international space governance. Space programs can be national or international, but when we talk about space governance only international space governance makes truly sense. The reason is that the hazards created by space missions are of international nature, in the sense that they are created by space actors internationally, and can be effectively controlled only through international cooperation.
When a country launches a rocket, usually spaceports are close to the sea, in a matter of few seconds the rocket will be flying through the international airspace (that begins just 12 miles off the coastline) and then overflying foreign territories before achieving orbit. The risk along the rocket trajectory is mainly on foreign populations. The traffic on orbit is international too: operational and decommissioned spacecraft of almost any nationality, and spent rockets upper stages from a smaller but ever growing number of countries. From time to time due to residual energy stored in components as fuel tanks and batteries some of those abandoned satellites and spent upper stages will explode creating a multitude of smaller but yet very hazardous debris. Same story at reentry from space. At the end of a mission in Low Earth Orbits it costs fuel to make a controlled reentry that would place a satellite in a precise (safe) spot on the Earth surface, but of course operators prefer to spend that fuel on orbit to generate revenues. Therefore most spacecraft and spent rockets upper stages are left to slowly renter the atmosphere following a so-called "natural" descend due the tiny friction generated by the residual atmosphere. When the spacecraft is low enough to get in contact with the denser layers of the upper atmosphere it would randomly bounce and skip until it sinks fragmenting and sometimes exploding. Most

fragments would just evaporate because of the intense heat of reentry (with pollution effects still to be understood) but many would survive and hit the Earth surface on a several hundredth miles long ground track. Many debris end up in the oceans, some would hit the ground. Small debris may be of no consequence if hitting a building but are potentially catastrophic if colliding with an airliner at cruising speed (300 grams is enough). Uncontrolled reentries happen every week. In the near future with the deployment of large satellites constellations, uncontrolled reentries may become a daily occurrence.
Many human activities are fraught with risks that need to be managed, but few match the neglect reserved for space mission risks. There is an apparent lack of political will to effectively engage the international cooperation beyond the exchange of scientific data and the offer of unilateral services. The issuing of policy standards is a government responsibility that cannot be delegated to technical standardization organizations, like ISO, as was done for space debris mitigation. The resulting deficient enforcement is before everybody's eyes. For managing the risks of space operations we need an organization similar to ICAO (International Civil Aviation Organization) that since the end of WWII has been successfully coordinating air traffic and aviation safety internationally. An organization that is international but not supranational. We need also a ban on anti-satellite systems tests, and to set up rules for military suborbital rockets tests like those performed by North Korea. Last but not least, we need to agree that it is no longer against the interest of a few, but in the interest of the many to establish where sovereign airspace ends, and outer space begins. Back to you Scott

Scott Kordella:
Thank you Tommaso. Now, to get started with our panel, let's begin with Thomas Dorame of the Space Foundation, Thomas.

Thomas Dorame:

1. **Tell us about the International Association for Space Safety. When was it formed, what does it do? Can you give a few examples of the impact that the Association has had over the years?**
   A. *Yes, thanks for the question. The IAASS was established in 2004 in the aftermath of the Shuttle Columbia accident by a group of safety engineers and managers working on the International Space Station program, from US, Europe, Russia, Japan, and Canada. We recognized some common problems with the Shuttle program and additional complications from the international set up of the ISS program, and we decided that it was time to give a voice, a forum, to the international space safety community. In the name of the association is our goal: advancing space safety! We often hear about how difficult and risky space missions are. Yes, sure. But we should also add that almost nothing is done in terms of basic research and education to change the status quo. Often safety is just considered the "natural" by product of a "good" (reliable) design. At IAASS instead we are convinced that is a matter of organization, integrated technical competences, robust processes, and wide-spread safety education. We started defining the scope of space safety, which goes from human spaceflight to launch, reentry, environment protection, space traffic management, and planetary defense. We have technical committees operating in each of those fields and regularly informing the United Nations COPUOS, of which we are observer member since 2006, about the results of our work, findings, and recommendations. Our Launch and Reentry Safety Committee has performed some pioneering benchmarking of risk analysis tools used worldwide. This committee is a unique forum where experts from allied spacefaring countries (i.e. except Russia and China!) meet periodically to compare notes. Our Commercial Human Spaceflight Committee has published the first standard on safety certification of commercial space vehicles. The Committee is currently working with The Aerospace Corporation to develop the concept of Space Safety Institute as intermediate organization to support companies and regulators. Our Space Policy and Regulations Committee has developed unique legal framework proposals for space debris removal, and for legally delimitating the border between airspace and outer space. At IAASS, we have a robust educational program. We have published a series of world-class university textbooks on design, operations, and*

human performance. The last book, "Space Safety and Human Performance" published by Elsevier in 2018 won 3 awards including the prestigious PROSE award of the American Association of Publishers (AAP) as best book of the year in the field of engineering and technology. We publish the quarterly Journal of Space Safety Engineering (JSSE), part of ScienceDirect the largest repository of scientific and medical publications worldwide. We have also a professional training program now being transitioned to on-line courses. In cooperation with our US based sister organization ISSF (International Space Safety Foundation), we provide grants for undergraduate students projects in US and Europe in the field of space safety.

2. **How is space safety evolving? Are there safety issues that we should be concerned about?**
   A. We are at a turning point. The role of the space agencies is going to be redefined to take into account the reality of a mature industry willing to take the lead in all kinds of space missions, except perhaps robotic space exploration in which science institutions maintain an irreplaceable leading role. This is a challenging passage for space safety because the self-regulating approach of the space agencies cannot be transferred to industry. At the same time, regulatory organizations like FAA/AST will never be able to keep the pace with industry in terms of skills and competences to independently assess the design of advanced space systems. In this evolving scenario I am concerned about the attitude to procrastinate the regulatory set up of commercial human spaceflight and by the rather secretive attitude of some companies about the safety of their systems, their policies, and their organization. Some high visibility failures often disappear from media, without any apparent effort for transparent communication. Safety is not proprietary, and lessons learned need to be shared. Finally, I am concerned that cutting costs without substantially improving the poor safety record of space missions could be a recipe for business failure.

Steve Sidorek:

3. **You've spoken about International Civil Aviation Organization (ICAO) and the idea of a forming a new Space equivalent of ICAO. To provide some context, can you tell us what the ICAO has done, and what a Space ICAO would notionally do?**
   A. *The ICAO, a specialized agency of the United Nations, made international air travel the reality we know today. The ICAO is essentially a safety (standardization) agency, which operates based on a membership convention initially signed in 1944 (Chicago Convention) to harmonize air navigation and aviation safety rules and services worldwide. The primary impetus for ICAO was the need to develop commercial aviation with the projected increase of aircraft manufacturing and air traffic after WWII. A space ICAO, or better, a branch of ICAO for space would do exactly the same for space traffic and in addition make provisions for an integrated use of the air space.*
4. **Regarding a Space ICAO – are other approaches for international collaboration in space, such as United Nations Committee on the Peaceful Uses of Outer Space ('COPUOS'), not sufficient? What is missing that a Space ICAO could provide? Why is now the right time to consider alternative approaches?**
   A. *The UN COPUOS, with 95 members one of the largest committee of the United Nations General Assembly, is not an action body but a forum to debate the status of international cooperation in the field of space activities, promote mainly scientific cooperation, and from time to time make recommendations to the General Assembly for deliberations. The COPUOS is supported by the limited staff of the Office of Outer Space Affairs (OOSA) that provides secretariat services to the two annual sessions of the committee. The COPUOS is just not meant to be the kind of organization needed to organize and manage space traffic internationally. An alternative could be the establishment of a standardization consortium. Back at the time of 2nd IAASS Conference in Chicago (IL) in 2007, Bryan O'Connor NASA Associated Administrator Safety & MA suggested that international space governance could be easier achieved*

through cooperation on space safety standards instead of a full-fledged organization on the ICAO model. The IAASS followed up by drafting an MoU that NASA presented first to FAA/AST and then jointly to the DoS. The standardization cooperation was meant to be open to all spacefaring countries. The MoU provided mechanism and organization for harmonizing national space safety policies for those issues that could be effectively mitigated only through international cooperation. The parties subscribing the MOU would voluntarily adopt the resulting policy rules as main/preferred reference for their own national regulations. Furthermore, they would jointly review the adequacy of lower levels industrial standards, issued by specialized standardization bodies such as ISO, ASTM, SAE, etc. in view of recommending their use (recommended best-practices). In 2008, IAASS received a response letter from the DoS stating that «the United States Government does not believe that a set of international space safety standards of the type in the IAASS MoU proposal is necessary at this time». Nowadays the time seems mature. The issues raised by the deployment of large satellites constellation in particular is becoming the tipping point to launch the international cooperation.

Christian Zur:

5. **As an international player in space, how do you view progress towards greater use of space among various nations? Who are the strong leaders? What makes them strong? Which countries should we be paying close attention to in their space development?**
   A. Greater use of space is a natural step of human progress. The "high ground" of modern times for communication, observation, and, of course, for military advantage. More assets on orbit more need to defend them. There is truly no choice. Europe, in due time, will emerge as the commercial competitor. China as the strategic competitor, with Russia always playing some role. The space development will be in step with the technological and economic development and wealth of the nations.
6. **Given space is becoming less exclusive, what are your thoughts about the US role and how do you see this evolving?**
   A. Space needs to be organized internationally, but it cannot be done without US for the simple reason that US has the technological resources, the innovation drive, the diplomatic strength, and the greatest commercial and military interest to lead such gigantic endeavor. US was the power driving the establishment of ICAO in 1944, I am confident that US will be again the leading power for Space ICAO!

Scott Kordella:
Thanks Tommaso, a great conversation all around, and unfortunately with that, this episode of the space policy pod has come to an end. I would like to thank our guest Tommaso Sgobba for his time here today and invite listeners to stay tuned for upcoming podcast episodes exploring events, technologies and policy affecting the space sector. On behalf of AIAA, the Chamber of Commerce, the Space Foundation and the MITRE Corporation thank you for tuning in today.

di Alberto DEL BIANCO

INTRODUZIONE

In questi ultimi anni si parla sempre di più di Voli Suborbitali, come nuova frontiera del mondo aerospaziale. Attualmente il volo suborbitale è in fase di sviluppo, da parte di diverse industrie private. Purtroppo, però, questa nuova attività ha generato situazioni che hanno provocato incidenti a persone o all'ambiente circostante.

1.0 GLI INCIDENTI

26/7/2007 Mojave Spaceport, California

Esplosione durante una prova di sistemi a razzo, da parte della società Scaled Composites, utilizzando protossido di azoto (N2O) – morti 3 Test Engineer

31/10/2014 Mojave Desert, California

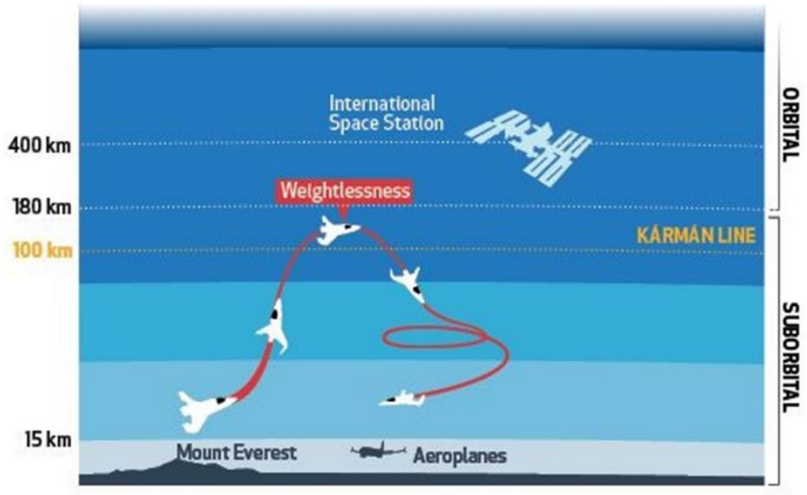
Lo SpaceShipTwo, il veicolo sperimentale per il volo sub-orbitale, operato da Scaled Composites per conto di Virgin Galactic, subisce la rottura della struttura in volo, durante un volo di prova, e si schianta nel Deserto del Mojave, vicino a Cantil, in California. Il co-pilota Michael Alsbury rimane ucciso e il pilota Peter Siebold gravemente ferito.

13/05/2017 West Texas

Blue Origin subisce una battuta d'arresto nello sviluppo del suo motore BE-4, per la perdita di un componente hardware del motore durante un test.

2.0 CONCETTO DI VOLO SUB-ORBITALE

Il Volo suborbitale viene definito come un volo che interessa la porzione di spazio compresa tra i 15 e i 100 km. Una nuova sfida per assicurare collegamenti, punto a punto, sulla superficie terrestre, che potrebbero consentire collegamenti Torino – Tokio in un'ora e 1/2. Inizialmente il turismo spaziale userà velivoli con la sola capacità di portare i passeggeri fino a circa 100km di altitudine, con una traiettoria praticamente verticale, per poi atterrare nello stesso sito di decollo.



3.0 SAFETY DEGLI SPAZIOPLANI

La Safety è un fattore determinante nella progettazione del veicolo da certificare, in riferimento a specifici requisiti di aeronavigabilità, impianti, emergenze, etc. Il progetto deve dare evidenza che il veicolo è sicuro rispetto ad una serie di linee guida e livelli di Safety, che dovrebbero essere riconosciuti a livello nazionale ed internazionale; pertanto il veicolo deve ricevere un 'approvazione di Safety, prima di poter essere utilizzato.

L'operatore, di uno spazioplano, deve ricevere un'autorizzazione, rispetto ad una serie di requisiti riconosciuti a livello internazionale, come:

- le licenze dell'equipaggio,
- Il Safety Management System

secondo gli standard aerospaziali, per poter operare in modo sicuro.

3.1 Approvazione del veicolo.

Il progettista / operatore di veicoli suborbitali deve ottenere l'approvazione che certifica che il veicolo è stato progettato in accordo a requisiti di Safety, quali:

- **Criteri di Safety**: Raggiungere l'obiettivo di sicurezza di 1x10-4 per missione, in caso di perdita catastrofica (secondo le IAASS Suborbital Guidelines).
- **Safety Requirements**: Soddisfare i requisiti di sicurezza tecnica concordati, come gli standard proposti (IAASS Space Safety Standards Manual e IAASS-SSI-1700).

3.2 Approvazione dell'Operatore di voli suborbitali

L'operatore del veicolo suborbitale deve ottenere un'approvazione che soddisfi i seguenti requisiti:

- Personale con l'esperienza specifica per il tipo di operazioni richieste

- Veicolo "sicuro", adatto al tipo di operazioni richieste
- Sistemi accettabili per il funzionamento dell'aeromobile (Manuale delle operazioni) e l'addestramento dell'equipaggio
- Un sistema di qualità, per garantire che vengano seguite tutte le normative applicabili;
- La nomina di personale di riferimento, che è responsabile di specifiche funzioni critiche di Safety come la formazione, la manutenzione e le operazioni.
- Un'assicurazione di responsabilità finanziaria e /o responsabilità civile, sufficiente a coprire adeguatamente l'esposizione per lesioni o morte a seconde o terze parti, in accordo sia con la legge applicabile nazionale sia con la legge internazionale;
- Fondi sufficienti per finanziare l'operazione;
- Un'infrastruttura di terra sufficiente a sostenere le sue operazioni negli spazioporti identificati;
- Approvazione rilasciata ad una persona giuridica che risiede nel paese o nella regione di applicazione;
- Un sistema di gestione della Safety (SMS), secondo i requisiti dell'Autorità o dell'ICAO, approvato dall'autorità competente.

4.0 SAFETY DEGLI SPAZIOPORTI

Gli Spazioporti possono essere nuovi o collocati presso un aeroporto già esistente. In questo caso, potrebbero sorgere nuovi problemi e rischi che dovrebbero essere affrontati, in dettaglio, attraverso un sistema di gestione della Safety e Analisi dei rischi operativi (aerei commerciali, traffico aereo, passeggeri).

A questo proposito, uno Spazioporto dovrebbe avere un suo Safety Management System per gestire tutti gli aspetti di Safety e, in particolare, la movimentazione/uso di propellente per razzi, sia per il pericolo di esplosione che anche di tossicità.

4.1 Safety Management System

Un Safety Management System di Spazioporto deve garantire che tutti i dipartimenti, dello spazioporto, siano:

- costantemente al corrente dei potenziali pericoli (hazards) presenti, inerenti la Safety;
- in grado di dare la priorita' a tali potenziali pericoli in funzione del relativo rischio, sulla base del rischio per la Safety;
- agire, se il potenziale pericolo inerente la Safety genera un rischio troppo elevato, mitigando il rischio stesso e assicurandosi che la mitigazione attuata stia dando i risultati voluti.

I requisiti di un SMS dovrebbero integrare le Standard Operating Procedure (SOP) già disponibili, in particolare per gli aeroporti che intendono estendere la loro attività ai voli suborbitali. I quattro componenti fondamentali di un SMS sono:

- Safety Policy and Objectives
- Safety Risk Management
- Safety Assurance
- Safety Promotion

Politica della Safety e Obiettivi

La politica di Safety deve includere una dichiarazione degli obiettivi di Safety, da parte della direzione dello spazioporto. Deve includere l'impegno a dare alla Safety la massima priorità e l'impegno al miglioramento continuo. Deve essere parte di una politica più ampia, integrando capacità, aspetti economici, ambientali e sociali. SAFETY FIRST

Safety Risk Management

La gestione dei rischi di Safety deve essere considerata un'attività principale, nella progettazione del sistema, finalizzata all'identificazione dei pericoli, all'analisi e alla valutazione dei rischi, generati da tali pericoli, e alla definizione di controlli necessari a ridurre i rischi al livello più basso. Dal momento che i voli sub-orbitali commerciali sono una novità, l'identificazione del pericolo, la valutazione e la mitigazione del rischio sono di fondamentale importanza per raggiungere un livello accettabile di Safety, dall'inizio dell'attività operativa dello spazioporto.

Safety Assurance

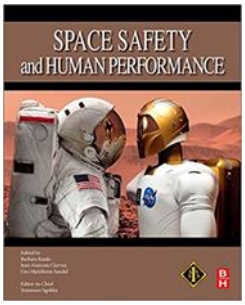
La garanzia della Safety deve essere un'attività continua, condotta senza sosta, per garantire che le operazioni, relative ai voli con veicoli suborbitali, siano adeguatamente protette dai pericoli. L'attività della Safety dovrebbe essere monitorata e misurata mediante opportuni indicatori di Prestazione di Safety (Safety Performance Indicator).

Safety Promotion

Uno spazioporto e il suo personale devono avere le competenze sufficienti per svolgere le funzioni assegnate e le attività di pertinenza. Il programma di formazione sulla Safety, che garantisce la competenza del personale a

svolgere i compiti definiti nel SMS, deve essere appropriato alle attività di ciascun ruolo. A questo scopo devono essere previsti corsi, seminari e conferenze di Safety, mirate al continuo miglioramento delle conoscenze.

5.0 SAFETY DEI PASSEGGERI (ADDESTRAMENTO)



Ai fini della Safety, i passeggeri devono effettuare il seguente iter:

- Idoneità fisica
- Addestramento

5.1 Idoneità fisica

- Certificato di buona salute del medico generico.
- Certificato medico, da parte di un medico specialista in medicina aerospaziale, del Centro medico dell'operatore, almeno 6 mesi prima del volo.

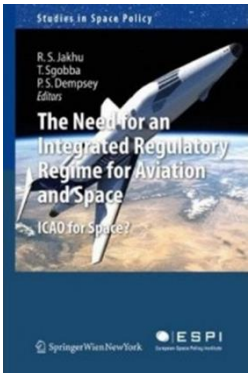
- Controllo medico finale, pochi giorni prima del volo, da parte del Centro Medico dell'operatore, per accertarsi che le condizioni e l'idoneità del passeggero non siano cambiate rispetto alle visite mediche iniziali.

5.2 Addestramento

- Corso specifico su tutti gli aspetti del volo, inclusi l'ambiente spaziale, il veicolo e il profilo del volo.
- Aspetti di Human Performance & Limitations
- Addestramento al simulatore.
- Familiarizzazione con la cabina, incluso l'uso di tutte le attrezzature e impianti che saranno utilizzati.
- Formazione per l'uscita di emergenza dal veicolo
- Allenamento per le accelerazioni (accelerazioni elevate, microgravità, tuta anti-G)

6.0 REGOLAMENTAZIONE

Attualmente la regolamentazione, per i voli sub-orbitali, è limitata alla sicurezza del pubblico. Il quadro normativo più sviluppato in vigore è quello degli Stati Uniti. L'FAA, attraverso l'Office of Commercial Space Transportation (AST), è responsabile del rilascio di licenze di lancio e rientro e per siti di lancio (spazioporti). L'Agenzia Europea per la Sicurezza Aerea (EASA) ha presentato alla Commissione Europea una proposta che delinea diverse opzioni per la gestione dei voli suborbitali.



Mentre l'Unione Europea non ha assunto una posizione ufficiale sui voli suborbitali, la proposta dell'EASA presenta comunque un approccio completamente diverso dagli Stati Uniti, sulla questione della regolamentazione. Da questo ne deriva che la regolamentazione dei voli suborbitali dovrebbe essere sviluppata da un **ente esterno**.

Un Ente, riconosciuto a livello internazionale, che disciplini le attività suborbitali, con un ruolo simile a quello esercitato da ICAO (International Civil Aviation Organization), ma con un alto livello tecnico, indipendente, che permetta anche di verificare la conformità ai requisiti di sicurezza del veicolo, e l'adeguatezza delle organizzazioni, dei costruttori ed operatori, nella gestione del rischio.

6.1 Space Safety Institute

Necessità di creare una struttura esterna e indipendente, che svolga un ruolo simile alla NASA o all'ESA, ma applicabile a tutti gli stati partecipanti, al fine di:

- Stabilire norme per la sicurezza delle persone a bordo
- Verificare, in modo indipendente, il rispetto delle regole
- Monitorare, tramite audit, il programma di verifica
- Educare e formare per gli aspetti di Safety

Un'organizzazione creata (e finanziata), dalle industrie, come uno Space Safety Institute, è più adatta ed economica rispetto a un'organizzazione governativa. Al fine di valutare la solidità delle soluzioni progettuali, scelte per mitigare i rischi, è necessario un team indipendente, per le certificazioni di Safety, con competenza comparabile (o superiore) rispetto al team di progettazione. Questo garantirebbe una valutazione al di sopra delle parti, riconosciuta a livello internazionale.

7.0 CONCLUSIONI

Per i voli suborbitali si dovrebbe applicare la stessa raccomandazione, emessa dalla Commissione presidenziale degli Stati Uniti, che ha indagato il disastro petrolifero "Deepwater Horizon" dell'aprile 2010, nel Golfo del Messico:

"L'industria del volo spaziale commerciale deve muoversi verso lo sviluppo del concetto di Safety come una responsabilità collettiva. L'industria dovrebbe stabilire un «Safety Institute"... questo sarebbe un'entità creata dalle industrie, mirata a sviluppare, adottare e applicare standard di eccellenza, per garantire il miglioramento continuo della Safety.

BIBLIOGRAFIA

- Safety Design and Operation of Suborbital Vehicles – IAASS, October 2015
- Space Safety Standard - Commercial Human-Rated System – IAASS-SSI-1700, July 2018
- Recommended Practices for Human Space Flight Occupant Safety – FAA, August 2014
- License to operate a launch site - US Title 14 → Chapter III → Subchapter C: Part 420
- Launch and Reentry of a reusable launch vehicle (RLV) - US Title 14 → Chapter III → Subchapter C: Part 431

AUTORE: Alberto Del Bianco ,Ex-Responsabile Qualità & Safety – ALTEC, Consigliere AICQ Settore Aerospace

E-La Qualità nel mondo

a cura di Giovanni Canepa

PERCHÉ ADERIRE AL PROGRAMMA DI CERTIFICAZIONE NADCAP?

Il Nadcap è lo standard di riferimento per il mercato aerospaziale , da un lato è uno strumento per il controllo di processi e fornitori, dall'altro è uno strumento di garanzia della qualità consegnata al cliente. Il programma garantisce un approccio settoriale alla valutazione delle conformità dei Processi Speciali.(quei processi i cui risultati non possono essere verificati tramite misurazioni e monitoraggi poichè eventuali difettosità risulterebbero evidenti solamente dopo l'utilizzo del prodotto)

L'acronimo NADCAP, che sta per National Aerospace & Defense Contractors Accreditation Program, è un programma di cooperazione internazionale delle imprese che operano nel settore aerospaziale e difesa, definite come Primes.

Il programma era stato creato in origine dal ministero della difesa americano per garantire il rispetto dei requisiti tecnico/qualitativi del prodotto aerospaziale; la comprovata validità ne ha consentito la rapida evoluzione e adozione da parte delle primarie industrie del settore aerospaziale e della difesa. Oggi praticamente tutti i Primes Aerospaziali con i principali fornitori in tutto il mondo sottopongono i propri Processi Speciali all'accreditamento Nadcap.

Il Nadcap si configura come una condizione essenziale per dare certezza alle parti del rapporto contrattuale in un settore dove coesistono elevate produzioni e fortissime esigenze qualitative dei prodotti. Il pieno rispetto dei requisiti delle normative consente di avere una produzione di serie costante e ripetibile nel tempo.

Quindi se un'azienda in ambito aerospaziale aspira a divenire fornitrice di una delle aziende Primes, deve avere necessariamente l'accreditamento NADCAP per fare parte dell'albo dei fornitori qualificati .

L'accreditamento Nadcap vi consente di dimostrare che la vostra azienda conosce e applica le regole del settore e che la vostra qualità è frutto di un sistema rigoroso e ben organizzato; attraverso degli audit, condotti da tecnici esperti del settore, vengono assegnati giudizi sulla qualità e robustezza dei vostri processi operativi e, di conseguenza, sulla vostra capacità di costruire prodotti affidabili da utilizzare in ambito aerospaziale.

Lo scopo è stato quello di istituire una procedura standard unica di accreditamento per tutti quei processi definiti speciali da applicare alle aziende della supply chain delle Primes stesse, evitando il proliferare di audit di seconda parte ridondanti e di fuori di un'ottica di Qualità collegata ad una logica di ottimizzazione dei processi e quindi, di riduzione dei costi.

Un Audit NADCAP è molto diverso rispetto ad un Audit svolto in regime di Iso 9100, perché è una visita ispettiva più profonda che va a valutare , oltre alla conformità del sistema Qualità vigente,degli aspetti squisitamente tecnici del processo di quel determinato fornitore ponendo attenzione a tutte quelle carenze che potrebbero palesarsi e quindi rendere quell'aspirante fornitore non conforme rispetto agli standard qualitativi del programma in questione.

Creato nel 1990 dalla SAE Inc., il programma Nadcap è amministrato dal Performance Review Institute (PRI), un ente no-profit. Il PRI si identifica come fornitore globale di soluzioni orientate al cliente progettate per migliorare il processo e la qualità del prodotto aerospaziale, riducendo i costi totali e promuovendo la collaborazione tra le parti interessate in un settore in cui sicurezza e qualità sono obiettivi condivisi. Il PRI lavora a stretto contatto con le aziende operanti nel settore aerospaziale per cogliere al meglio le specifiche esigenze e i bisogni emergenti, offrendo risposte e soluzioni personalizzate.

Il programma, gestito dal PRI con il supporto di innumerevoli Primes Aerospaziali concorrenti tra loro, è in grado di:

- Fissare standard rigorosi comuni per il settore in grado di soddisfare i requisiti di tutti i clienti coinvolti;
- Condurre audit sui Processi Speciali in maniera approfondita e di elevato contenuto tecnico;
- Migliorare la qualità dei fornitori in tutto il settore grazie all'introduzione di requisiti rigorosi;
- Ridurre i costi promuovendo un livello di standardizzazione più elevato;
- Utilizzare valutatori esperti a livello tecnico (Nadcap Auditors) per ogni differente processo.

Alcuni dei cosidetti "processi speciali" che sono sottoposti all'Audit NADCAP:

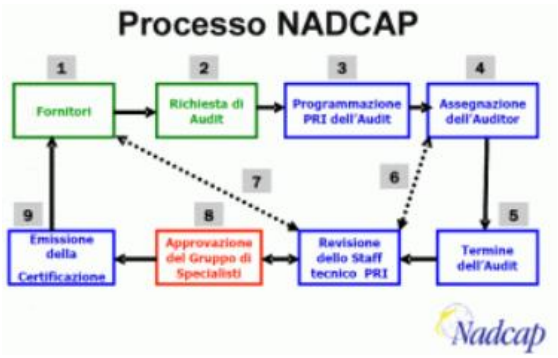
- ✓ Sistema di qualità aerospaziale (Aerospace Quality System, AQS);
- ✓ Processi chimici (Chemical Processing, CP);
- ✓ Rivestimenti (Coatings, CT);
- ✓ Materiali compositi (Composite Materials, COMP);
- ✓ Lavorazione di macchina convenzionali (Conventional Machining as a Special Process, CMSP);
- ✓ Giunti a elastomero (Elastomer Seals, SEAL);
- ✓ Elettronica (Electronics, ETG);
- ✓ Distribuzione dei fluidi (Fluid Distribution Systems, FLU);
- ✓ Trattamento termico (Heat Treating, HT);
- ✓ Laboratori per i test dei materiali (Materials Testing Laboratories, MTL);
- ✓ Misurazione e controllo (Measurement and Inspection, M&I);
- ✓ Test non distruttivi (Nondestructive Testing, NDT);
- ✓ Lavorazione a macchina non convenzionale e trattamenti superficiali (Nonconventional Machining and Surface Enhancement, NMSE);
- ✓ Sigillanti (Sealants, SLT);

- ✓ Saldatura (Welding, WLD)

Per maggiori dettagli visitre il sito PRI https://it.p-r-i.org/

Aderire al programma Nadcap non è solo un requisito essenziale per operare nel settore aerospaziale, ma è anche un'opportunità per migliorare i processi produttivi. Inoltre, l'accreditamento Nadcap è anche un'occasione da non perdere per ottenere una maggiore visibilità della azienda.

Per chiudere possiamo affermare che il programma NADCAP di sicuro rappresenta un'evoluzione fondamentale nell'ambito della produzione aerospaziale perché la valutazione dei fornitori avviene in un'ottica totalmente imparziale ed indipendente, che è andata nei fatti ad aggiungere valore e a ridurre i costi senza nascondere che il Nadcap sia una certificazione non facile da ottenere senza uno sforzo comune a livello aziendale



AUMENTANO I PROBLEMI A STARLINER RISCONTRATI DALLA NASA

Dopo più di sei mesi dall'ultimo volo della capsula Starliner di Boeing, la NASA ha concluso un'altra ispezione, trovando altri errori e situazioni critiche.

La capsula Starliner CST-100 di Boeing fa parte del Commercial Crew Program della NASA insieme alla Crew Dragon di SpaceX. A Dicembre la Starliner eseguì uno dei principali test del programma. Durante quella missione la capsula, senza equipaggio a bordo, avrebbe dovuto raggiungere la ISS ed eseguire un attracco automatico alla stazione , purtroppo dopo pochi minuti dalla partenza la stessa Starliner ebbe un problema al software di bordo.

Questo comportò la ritardata accensione dei propulsori che non permisero di arrivare all'orbita necessaria per l'attracco con la ISS, la capsula di Boeing riuscì comunque a rientrare a terra con successo dopo qualche giorno passato in orbita. A marzo un team congiunto della NASA e di Boeing completò una prima revisione completa di tutto il progetto Starliner ed in quell'occasione vennero trovate tre principali criticità.

Le prime due riguardavano il software di bordo. Il terzo problema principale riguardava invece le comunicazioni con la capsula che durante il test di volo vennero a mancare più volte.

Questi tre principali problemi riscontrati dalle prime revisioni si sarebbero risolti con 60 azioni correttive che il team di Boeing avrebbe dovuto eseguire. Queste riguardavano sia la revisione completa di molti software ma anche il controllo di molte procedure aziendali, sia pratiche sia logistiche.

La NASA ha però condotto ulteriori revisioni durante questi mesi aumentando le correzioni da eseguire da 60 a 80. Queste sono principalmente divise in 5 aree.

- ✓ 21 correzioni sono da fare ai test e simulazioni fatti da Boeing, sottolineando la necessità di maggiori test sulla corretta integrazione software-hardware della Starliner
- ✓ 10 correzioni si riferiscono ai software che garantiscono la copertura completa dei test.
- ✓ 35 modifiche sono richieste alla documentazione delle revisioni, richiedendo l'aumento dei partecipanti ai controlli e alle revisioni dei dati dei test con espressa richiesta di aumentare "coinvolgimento di esperti in materia di sicurezza".
- ✓ 7 modifiche sono richieste alla cultura aziendale di Boeing in materia di sicurezza.
- ✓ 7 correzioni vengono infine richieste al software che gestisce la separazione fra il modulo di servizio e la capsula Starliner.

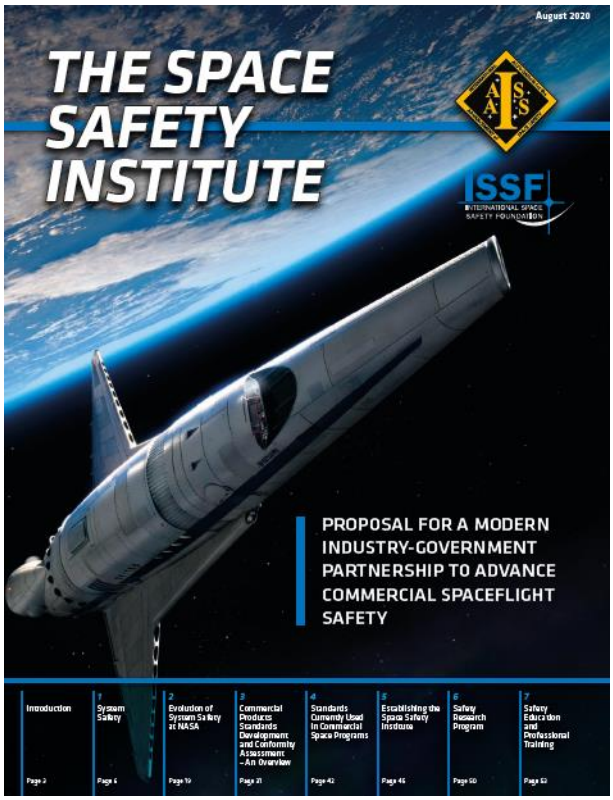
Queste revisioni sono state comunicate in un'apposita conferenza stampa condotta interamente da personale NASA il 7 luglio.

Già ad Aprile Boeing dichiarò di essere pronta ad eseguire nuovamente prima della fine dell'anno il test fallito a dicembre. Questo test l'azienda l'avrebbe eseguito interamente a proprie spese, affermando di aver già stanziato 410 milioni di dollari. Quest'affermazione fu abbastanza interessante in quanto fra febbraio e marzo si discuteva addirittura di non eseguire più questo test e passare direttamente al primo volo con equipaggio.

Le previsioni di Boeing e della NASA lo collocano ancora per la fine del 2020 con la speranza di veder volare la Starliner con equipaggio verso meta 2021.

La Sicurezza dei voli Spaziali Commerciali Abitati

Vedremo nell' immediato futuro con Virgin Galactic, Space X, Blue Origin e altri un aspetto nuovo a cui non siamo abituati : I Voli Spaziali abitati commerciali. I voli spaziali commerciali **rappresenteranno una sfida per gli aspetti della sicurezza poichè non saranno piu controllati da Agenzie Spaziali quali NASA, ESA** (se ne parla in questo numero con Alberto Del Bianco nell' articolo dei voli Sub Orbitali). **Diventa quindi necessario avere un ente esterno che permetta a tutti gli attori internazionali di avere un riferimento indipendente per la Sicurezza dei passeggeri. La proposta dello Space Safety Institute si propone proprio di coprire questo ruolo.** Qui di seguito la copertina del Documento e l' indice della proposta. Per chi fosse interessato contattare AICQ Aerospace.



INDEX

Artemis Accord

Il 10 Luglio si e' tenuto un interessante WEBINAR organizzato dallo IAASS , McGill e l' institute of AIR and Space Law dal titolo **Artemis Accord : challanges and opportunities** . L' Evento ha trattato il punto centrale della Space Economy nei prossimi anni **"L'Esplorazione Lunare e le implicazioni sullo sfruttamento delle risorse extraterrestri"**
Per chi fosse interessato ad avere dettagli sull'evento contattare AICQ Aerospace.

Novità sulla normativa Spaziale dall' ECSS
(European Cooperation for Space standardization)

Questa sezione dell' "E magazine" riporterà periodicamente lo stato e l' avanzamento della normativa Spaziale in Europa.

E' stato pubblicato dall' ECSS per la "pubblic review" lo standard che definisce i processi e i requisiti di Quality Assurance per le polveri in materiale metallico per l' **Additive Manufacturing nelle applicazioni spaziali**. Lo standard fa riferimento alle polveri per A.M. che usano laser o fascio di elettroni come sorgenti di fusione. Queste includono

- Selective Laser Melting (SLM)
- Direct Metal Laser Sintering (DMLS)
- Laser Sintering in Solid Phase (LSSP)
- Laser Beam Melting (LBM)
- Electron Beam Melting (EBM)

Chi volesse far pervenire dei commenti allo Standard contattare AICQ Aerospace


ECSS-Q-ST-70-80C DIR1
26 August 2020

EUROPEAN COOPERATION
ECSS
FOR SPACE STANDARDIZATION

Space product assurance

Processing and quality assurance requirements for metallic powder bed fusion technologies for space applications

This document is distributed ECSS community for Public Review.
(Duration: 8 weeks)

Start of Public Review: 27 August 2020
END of Public Review: 23 October 2020

DISCLAIMER (for drafts)
This document is an ECSS Draft Standard. It is subject to change without any notice and may not be referred to as an ECSS Standard until published as such.

Noordwijk, The Netherlands

Sarà emesso a breve lo standard di **Non destructive Inspection** in fase di finalizzazione.

ECSS-Q-ST-70-15C DIR1+impl.DRRs
26 August 2020

EUROPEAN COOPERATION
ECSS
FOR SPACE STANDARDIZATION

Space product assurance

Non-destructive inspection

This document is the draft from the Public Review with the impl. DRRs distributed for DRR Feedback.

Start of DRR Feedback: 27 August 2020
End of DRR Feedback 9 September 2020 (during TA#71)

DISCLAIMER (for drafts)
This document is an ECSS Draft Standard. It is subject to change without any notice and may not be referred to as an ECSS Standard until published as such.

ECSS Secretariat
ESA-ESTEC
Requirements &and Standards Division
Noordwijk, The Netherlands

CONGRESSI E CONFERENZE

AICQ Aerospace ha il piacere di comunicare , per chi non avesse avuto la possibilità di partecipare al primo convegno nazionale sulla Qualità dell' AEROSPACE di Novembre 2019, che e' disponibile su you tube una parte degli interventi al seguente indirizzo:
https://youtu.be/jpcD3P8vDE8

SAVE THE DATE :10 NOVEMBRE 2020

Il 2020 e' stato un anno particolare e critico ma AICQ sempre attenta ai temi del momento vuole comunque organizzare il convegno Annuale che si terrà a Novembre in Webinar . Considerando il periodo che abbiamo vissuto e stiamo vivendo tutt'ora con il COVID e il cinquantenario di una tra le più grandi emergenze spaziali , "L' Apollo 13" AICQ riprende il forum periodico iniziato su questo tema nel 2017 con il **convegno annuale AICQ Piemontese sulla Gestione delle Emergenze .** Questo convegno gratuito in Webinar **ha l' obiettivo di condividere l' esperienza nella gestione della Pandemia dai settori ad alta tecnologia come l' Aerospazio all' Automotive alla Sanità all' Università e il turismo.** Ci saranno testimonianze di eccellenza in diversi settori. Qui di seguito il manifesto dell' evento, seguirà il Programma con i vari relatori . Per iscrizioni scrivere a**: segreteria@aicqpiemonte.it**

Convegno Prevenzione Gestione delle Emergenze del 2017 intervista:

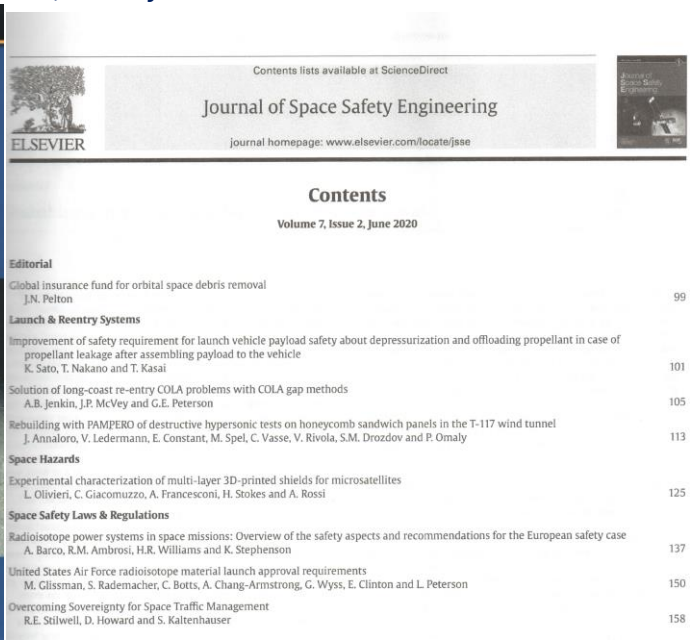
https://www.youtube.com/watch?v=uJPbfs-pjLk


11th IAASS Conference
International Association for the Advancement of Space Safety
MANAGING RISK IN SPACE
19-20-21 OCTOBER 2021
OSAKA - JAPAN
JAXA
Japan Aerospace Exploration Agency
http://iaassconference2021.space-safety.org


Convegno -LA QUALITA' NELL' "AEROSPACE"
le sfide e i risultati
SAVE THE DATE
Torino novembre 2021

PUBBLICAZIONI /LIBRI

Qui di seguito la copertina e l' indice **del Journal of Space and Safety Engineering numero 2 del 2020.** Questa pubblicazione raccoglie articoli di esperti internazionali sulla Sicurezza dei Voli Spaziali. La rivista e' distribuita agli associati allo IAASS (international Association for the Advancement of Space Safety)
contatti Mario Ferrante AICQ Aerospace, IAASS founder Member



Contents lists available at ScienceDirect

Journal of Space Safety Engineering

journal homepage: www.elsevier.com/locate/jsse

ELSEVIER

Contents

Volume 7, Issue 2, June 2020

Formazione


AICQ PIEMONTESE e AICQ SETTORE AEROSPACE
propongono
PERCORSI SETTORE AEROSPACE
I CORSI
PRODUCT ASSURANCE (QUALITY FOR SPACE)
ROOT CAUSE ANALISI (COMPRESO L'ERRORE UMANO)
PARTS MATERIAL AND PROCESS (PMP) FOR SPACE APPLICATION
SOFTWARE PRODUCT ASSURANCE (SW QUALITY FOR SPACE)
SATEFY FOR SPACE APPLICATION
HUMAN FACTORS FOR AERONAUTICS
aicq
Associazione Italiana Cultura Qualità
Piemontese
aicq
Associazione Italiana Cultura Qualità
Settore Aerospace
Per info: 011.5183220 - silvia.gamba@aicqpiemonte.it