

Applying System Safety Methodology and Related Tools for a Public Private Partnership Programme

Yue Sang, Fan¹, Boon Heng. Chua², Soon Hoe Ronald, Tan³, Minyi. Heah⁴ and Chee Ken, Ooi⁵

Abstract

Governmental agencies, including the Armed Forces, may require services that are available and ably provided by the private sector. Such collaborations between the public and private entities, commonly known as Public Private Partnerships (PPP), bring benefits to both parties and are well documented. This includes the ability to tap on the private sectors' facilities and resources without the need for the governmental agencies to make a similar high investment, while providing added revenue to the private sector.

This paper shares how the Defence Science and Technology Agency (DSTA), a statutory board under Singapore's Ministry of Defence (MINDEF), applied the System Safety process for a PPP programme. The programme entails the acquisition of the services of a vertical wind tunnel as a simulator to provide a safe, realistic and cost-effective free-fall training environment for the Singapore Armed Forces (SAF). The vertical wind tunnel facility is also open to the general public as a sporting and leisure facility. The paper discusses the challenges faced, the strategies implemented, and introduces two atypical tools that were utilised to good effect. One of the tools used is the Goal Structuring Notation (GSN) tool. The authors used the GSN tool as a graphical notation to communicate the structure of safety arguments. This approach facilitated the visualisation of how the safety integrity of the PPP Programme was ascertained.

Key words: Public Private Partnership, PPP, Goal Structuring Notation, System Safety Assurance, Defence Science & Technology Agency

Introduction

The SAF is manned largely by conscripts. All male Singapore citizens are required to serve two years of National Service. Not unlike most countries, Singapore places a high priority on the safety of her citizen soldiers, while ensuring realistic training to constantly enhance the capabilities of the SAF. Safety assurance not only keeps more of our soldiers operational but also contributes to the confidence that the populace places in the SAF to be able to perform its missions effectively and safely.

DSTA contributes to Singapore's defence through her core functions of Systems Architecting, Acquisition Management and Systems Management, to provide the SAF with

¹ M. Sc; Principal Engineer, Defence Science & Technology Agency (DSTA); Singapore. 1 Depot Road, Singapore 109679. Telephone – (65) 6373-4292, email – fyuesang@dsta.gov.sg

² B Eng; Engineer, Defence Science & Technology Agency (DSTA); Singapore. 1 Depot Road, Singapore 109679. Telephone – (65) 6373-2289, email – cboonhen@dsta.gov.sg

³ M Eng, Principal Engineer, Defence Science & Technology Agency (DSTA); Singapore. 1 Depot Road, Singapore 109679. Telephone – (65) 6373-4652, email – tronald@dsta.gov.sg

⁴ B Eng; Engineer, Defence Science & Technology Agency (DSTA); Singapore. 1 Depot Road, Singapore 109679. Telephone – (65) 6373-6564, email – hminy2@dsta.gov.sg

⁵ M Eng, Senior Engineer, Defence Science & Technology Agency (DSTA); Singapore. 1 Depot Road, Singapore 109679. Telephone – (65) 6373-3394, email – ocheeken@dsta.gov.sg

the technological edge and capabilities to deal with emerging new security challenges and non-traditional threats. Since the start of the new millennium, DSTA has further enhanced the defence material acquisition process by integrating the System Safety methodology into the MINDEF Life Cycle Management Framework.

This paper will share some insight on how DSTA leveraged the System Safety process to provide safety assurance for the acquisition of a realistic and cost-effective free-fall training environment for the SAF.

Vertical Wind Tunnel

The programme entails acquiring a local Vertical Wind Tunnel (VWT) training capability as part of the overall free-fall training requirement for the SAF. This is achieved through leasing of flying hours from a Commercially Owned and Commercially Operated (COCO) re-circulating VWT. A re-circulating VWT is a sophisticated technology combining a series of fans and ducts to produce a vertical laminar stream of air. When the fans are turned on to reach terminal velocity, the airflow provides the necessary lift for a person to simulate free fall. An actual flight chamber can range from four to five metres (twelve to sixteen feet) in diameter, and up to a height of ten metres (thirty feet). The basic layout of a re-circulating VWT is depicted in the figure below.

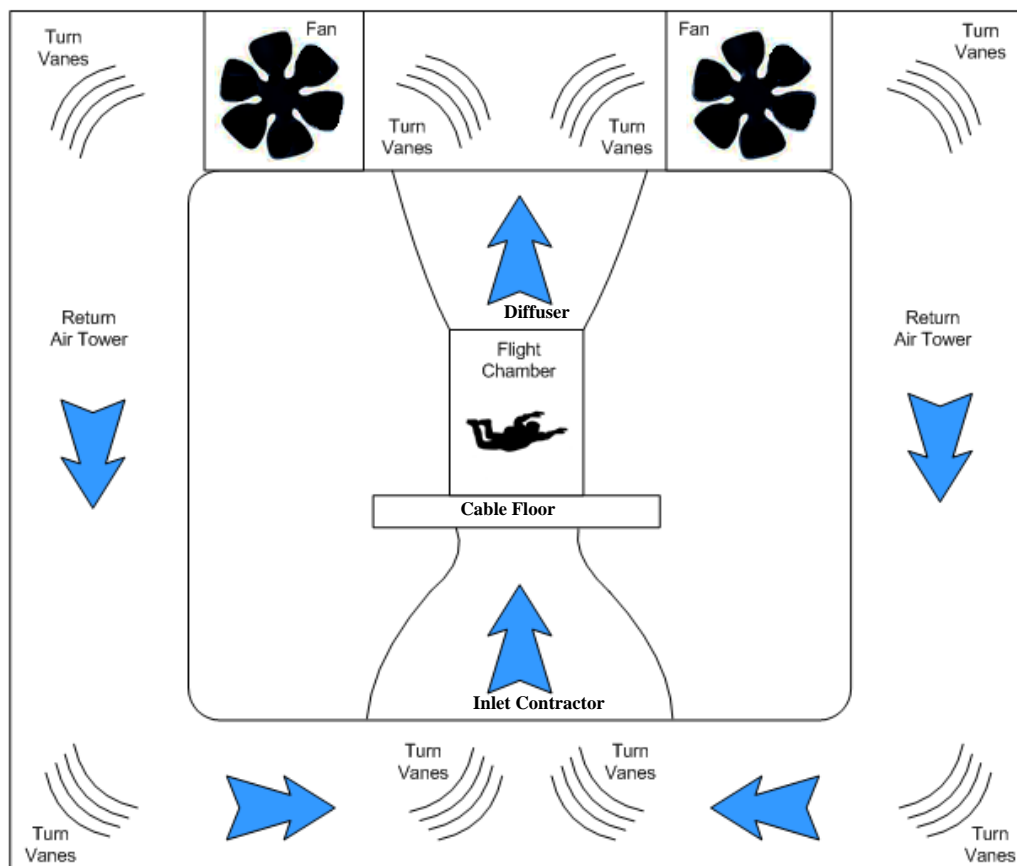


Figure 1 Layout of a Typical Vertical Wind Tunnel

The flight chamber is where the free-fall trainees (or flyers) perform their training. The fans are located at the top of the VWT and generate the airflow through the Return Air Tower (RAT) and the Inlet Contractor powers up the airflow for the person flying in the

flight chamber. The air is then re-circulated back through the diffuser, and back to the RATs. A series of turning vanes are also used to turn and smoothen the air to the flight chamber. A net, composed of interwoven cables, forms the floor of the flight chamber. The VWT system is operated via a control panel in an adjacent room from which the operator has a direct view of the flight chamber. Safety design features include inherent component safety features, automatic shut down circuits and emergency control capabilities. A minimum of two safety instructors are also on standby to ensure flyers' safety. The entire VWT is housed in a facility that includes offices, briefing rooms and viewing areas.

The motivation behind training in a VWT facility stems from risk minimisation. Live jumps at altitude from an airplane present an array of hazardous conditions to a free-faller, especially to trainees. Obvious hazards such as parachute malfunction, inclement weather and falling from height at two hundred kilometres per hour fuels the anxiety of many novice free-fallers. It is no surprise that free-fall incidents largely occur due to inexperience. By training in a controlled environment, trainees have time to develop confidence and learn the techniques required for their first jump, thereby reducing the probability of a free-fall incident. Furthermore, the mishap severity of a free-falling accident is drastically reduced. This is obvious as the height from which a trainee can potentially fall from is tremendously decreased. From a training perspective, the VWT allows the instructor to spot and correct improper techniques. Emergency procedures can also be safely demonstrated in a controlled environment.

Utilising a VWT also results in significant cost and time savings for the SAF. An actual jump would cost more (due to ever escalating high cost of aircraft and fuel), and each jump would have a short window of utility. In the case of the VWT, the training free-faller can make use of extended time blocks in the VWT to perfect his techniques, without the need to rehire an aircraft, climb to altitude and jump out of an airplane. Training slots will also not be at the mercy of inclement weather and close adherence to training time slots makes for more efficient management of the instructors and trainees schedules. Having said that, nothing can replace the need for real operation as the experience from a live jump is invaluable to the trainee. The VWT serves to shorten the learning curve for the novice free-faller. Hence, many military users all over the world use VWT facilities to train their free-fallers.

Every programme has its fair share of unique challenges and learning experiences. In the following sections, the challenges faced by the DSTA Project Management Team (PMT) are presented to illustrate the kind of scenarios one can expect when applying System Safety in a PPP programme. Thereafter, the implementation of system safety activities and safety tools for the programme are described.

Programmatic Challenges

Unfamiliar System

Acquiring and assessment of such a first-of-its-kind system in Singapore was new both to the PMT and the SAF. The team was more familiar with acquiring weapons-related systems and platform-type defence capabilities. As such, defining a tailored set of safety requirements for this unique and uncommon system was a challenge. System Safety programmes require detailed information about the system, which was a challenge in this

project due to the proprietary nature of the system's design information. Without access to details, a collaborative effort between the PMT and the Contractor was initiated to achieve a mutually desired outcome on System Safety standards.

Application of Military Standards on Commercial Entities

The company providing the services is Sky Venture Singapore (SVS), a franchisee of Sky Venture International (SVI), which operates the world's largest VWT, iFly Singapore. SVI builds, operates and maintains thirty-two vertical wind tunnels around the world. With years of operational experience, a robust system and an excellent safety track record, having been endorsed by many skydivers and military around the world, SVS was confident that the VWT was safe and met all commercially required levels of safety. The proven platform coupled with existing systems of safety manuals, safety operational procedures and checklists were part of a programme to ensure safe daily operations. Nevertheless, there exist areas in which military standards and practices may complement commercial practices to enhance safety and achieve a better and safer outcome for all users. However, defining the scope of a military standard on a commercial platform was not straightforward.

Framework Gap

One of the main features of System Safety is the rigour of the residual mishap risk acceptance framework. The PMT is required to surface residual mishap risk to two groups within the SAF. First, the treatment of the hazards or the mitigation approach were scrutinised by a technical safety board, whose endorsement deems that the hazards have been adequately mitigated to "As low As Reasonably Practicable" from a technical perspective. Thereafter, the mishap risk would be surfaced to the SAF commanders for acceptance of the residual risk and allowing the weapon system to be brought into service. Although apparently straight forward, it will be shown that the subsequent effort presented a rather interesting twist to the process.

System Safety Activities

Defining Uncharted Territories

While there are inherent safety designs and considerations built into such a commercially operated VWT, it is important that a systematic safety assessment of such a system is done to provide information for the risk acceptance authority to make informed decisions. The PMT assessed that applying the full range of System Safety tasks stipulated in the MIL-STD-882D to this programme was unrealistic, and a tailored scope was crafted for the programme.

One of the key challenges to the programme was bridging the gap between the information that was needed for a System Safety programme and what was feasible for the Contractor to reveal without compromising their competitive advantage and intellectual property. The PMT had to explore new ways to overcome this challenge. As the VWT is a commercially operated attraction that is open to the general public, there are stringent Singapore legislative requirements in place to govern the safety of the VWT. The PMT rationalised that proof of compliance to these requirements will provide a primary level of safety assurance. The legislative approvals and certifications are summarised in the following paragraphs.

Legislative Requirement: Public Entertainment Licence and Conformity Assessment Body (CAB) Certification

- Under Singapore's Public Entertainments & Meetings Act, any entertainment that is provided in any place to which the public has access has to attain a Public Entertainment License (PEL). The Police Public Entertainment Licensing Unit (PELU) processes and issues this license. PELU requires the attraction to be certified by a competent body, termed the Conformity Assessment Body (CAB), as having met relevant technical and safety standards. SVS obtained the PEL prior to commencement of operations.

Legislative Requirement: Temporary Occupation Permit/Certificate of Statutory Completion & Fire Safety Certificate

- SVS hired a Qualified Person (QP) and a Registered Inspector (RI) for both Architectural and Mechanical & Electrical to certify building and fire safety works. All personnel were sanctioned and registered to be competent to check and verify the safety within the building. When the Singapore Civil Defence Force (SDCF) and the Building Construction Authority (BCA) were satisfied with the details submitted, the Certificate of Statutory Completion and Fire Safety Certificate were issued.

Applicable Certification: OEM Commissioning Certificate

- SVI was present during the final stages of construction of the VWT to provide technical support, and to test and commission the VWT. This ensured the correct installation and safety of the VWT. Upon completion, SVI issued a commissioning certificate to SVS, validating the functional and safety aspects of the VWT.

Applicable Certification: SVS Instructors Certification

- SVS instructors are highly trained personnel that ensure the safety of the flyers in the wind tunnel. The instructor's training and ability in the event of an emergency situation is crucial in preventing injuries to the flyer. SVS consistently keeps its instructors current by following a stringent set of requirements laid out by the International Bodyflight Association (IBA). Certifications by IBA and the currency of SVS instructors and tunnel operators are submitted to the authority and are reviewed periodically.

Collaborative Application of System Safety

The PMT and SVS worked collaboratively to apply System Safety methodology and techniques for the VWT to enhance their existing system safety documentation. Instead of being a “show stopper”, System Safety was introduced as a methodology to complement their existing safety documentation. Although flying in the VWT for public flyers and military flyers is largely similar, military users may employ unique flight techniques and equipment configurations in the VWT. The application of System Safety led to the discovery of atypical VWT hazards which were not present in the public domain.

System Safety was also seen as a useful tool to complement SVS’ existing capabilities in complying with local legislative requirement. In Singapore, the Workplace Safety and Health Act (WSHA) was passed in 2006, and it is being gradually introduced to all workplaces in phases. Most industries are already within the purview of this Act, and it will be fully applicable to all workplaces by September 2011. The Act emphasizes the importance of managing workplace safety and health by requiring stakeholders to take reasonably practicable measures to protect workers. Besides having a Safety Management System in place, the Act requires workplaces to perform risk-based analysis to identify hazards associated with the workplace and its intended activities.

As the need to impose system safety was a contractual requirement, the first important step was to include a more holistic system safety process which included SAF’s involvement. A collaborative effort between the DSTA Project Management Team (PMT) and SVS ensued and this resulted in SVS enhancing its Safety Management System to incorporate the PMT’s requirements of system safety. A system-centric hazard analysis was also performed to identify key areas of concern. Some of these hazards are showcased in the Preliminary Hazard List (PHL) section.

Preliminary Hazard List (PHL)

The first step in the system safety process was the identification of the Preliminary Hazard List (PHL). Collaboratively, a three-pronged approach was undertaken by the PMT and SVS. Firstly, dialogue sessions were held with SVS/SVI to extract potential hazards based on their experience in operating other VWTs. By analyzing the safety features of the VWT, the PMT was able to work backwards and visualise the kind of hazards the safety features might be trying to protect against. Once the PMT could cue into the perceived hazard, they expanded their imagination and deliberated if such hazards could morph into other forms of hazards based on the unique utilisation of the VWT by the SAF. Secondly, dialogue sessions were held with members of the SAF who are experienced skydivers and/or instructors to solicit potential operational and training hazards. Finally, the PMT (with the assistance of SVS) visited VWTs overseas to get a first hand feel of the safety features and concerns from the usage of such a system. While some hazards would be applicable universally, the PHL effort identified hazards associated with the military applications of the VWT that would not manifest themselves in commercial usage of the VWT. Some examples of the PHL so developed are presented in Table 1.

Table 1 Sample of PHRL effort



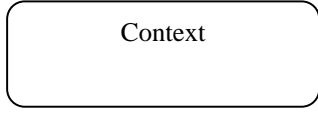
SN	Hazard Description	Possible Causal Factors
1	Unsecured Military Equipment	Failure of equipment securing mechanism
2	Flyer with military loads attempts to exit VWT from a flying position, impacting exit	Unstable flying position due to added equipment bulk
3	Kinetic energy of re-circulating objects	Presence of loose objects (shoes, gloves, goggles, etc.)

The ability to identify hazards that are unique to military applications led to the incorporation of mitigation measures to reduce risk. For instance (ref to SN2), an enforced procedure was introduced to ensure that the trainee did not exit the VWT from a flying position.

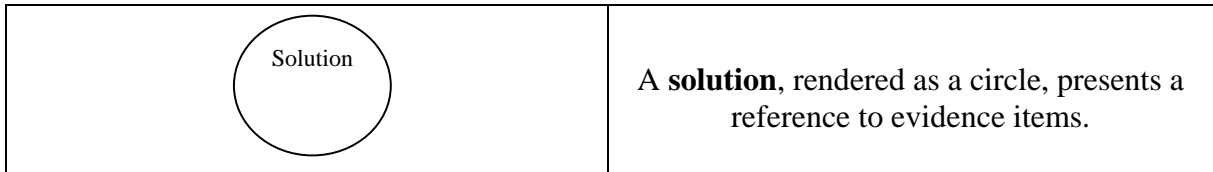
Goal Structuring Notation (GSN)

Goal Structuring Notation⁶ (GSN), developed by Dr John McDermid, was utilised to frame the argument for the safety integrity of the programme. Primarily, GSN is a useful tool to communicate how a particular claim is shown to be true in a graphical manner. Arguments shown using the GSN can help provide assurance of critical properties of systems, services or organisations. For this programme, GSN was initially used to define the challenges at hand, and to list the possible solutions to these challenges. Subsequently, it was used as a representation tool to present a top level view of how the VWT is acceptably safe for usage. The symbols of the notation are shown in Table 2.

Table 2 Basic Symbols of GSN (The GSN Drafting Committee, 2010)

	A goal , rendered as a rectangle, presents a claim forming part of the argument.
	A strategy , rendered as a parallelogram, describes the nature of the inference that exists between one or more goals and another goal.
	A context , rendered as shown left, presents a contextual artefact. This can be a reference to contextual information, or a statement.

⁶ GSN is a graphical argumentation notation which can be used to explicitly document the elements of any argument and - perhaps more significantly - the relationships that exist between them. (The GSN Drafting Committee, 2010, p. 3)



When the elements of GSN are connected together, a ‘goal structure’ is formed. Goal structures document the chain of reasoning in the argument, and how the argument is substantiated by evidence(s). The principal purpose of a goal structure is to show how goals are successively broken down into sub-goals, until a stage where claims can be supported by direct reference to available evidence. In the following paragraphs, part of the actual GSN created for the project is showcased for sharing.

The defined “Top Goal” for the GSN was “The Vertical Wind Tunnel (VWT) is acceptably safe to be used throughout its intended usage life”. The rounded rectangular shapes in Figure 2 below are contextual entries. It is important to capture the context in which the claim is to be interpreted. In C2, the interpretation of “Acceptably safe” in the Top Goal is referenced to the MINDEF System Safety Directive, assisting readers to understand the term.

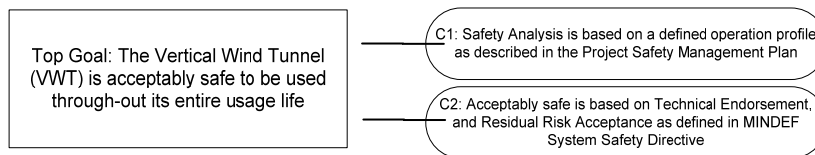


Figure 2 Top Goal of VWT Programme

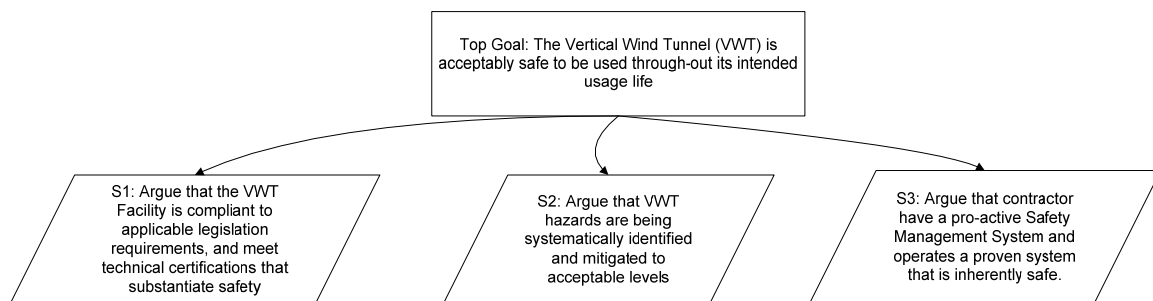


Figure 3 Top Goal with Strategies

In Figure 3, the Top goal is expanded into three separate strategy blocks. Each strategy block is a reasoning step that connects the top goal to the sub-goals. In this case, more than one argument approach is adopted to support the top goal. S1 argues that the VWT is compliant to applicable legislation requirements and technical certifications. S2 argues that all VWT hazards are identified and mitigated to acceptable levels. S3 argues that the contractor have a pro-active safety management system and operates a proven system that is inherently safe. The sub-goals that branch from S2 will be elaborated in the next section.

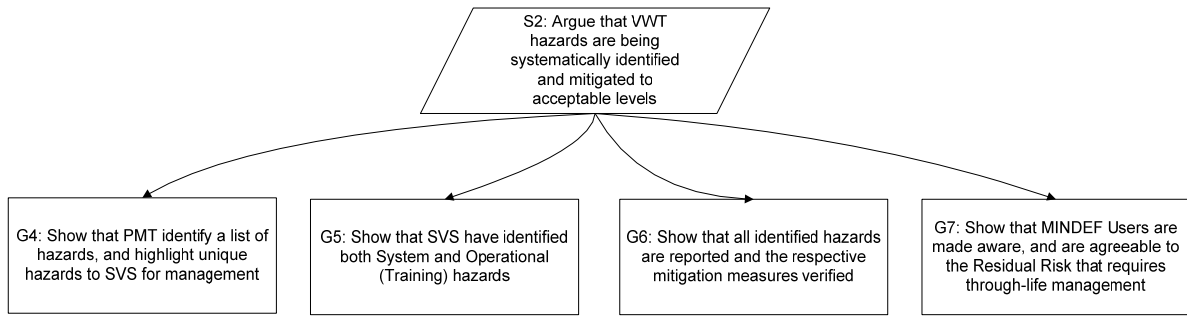


Figure 4 Strategy S2 and its Sub-goals

Strategy S2 is a description of the argument that is asserted to relate the sub-goals G4, G5, G6 and G7 to the Top Goal. As we move further away from the Top Goal, the problem is divided into smaller and more manageable activities. It will finally reach a point where it ends in a “Solution” block. This can be seen in Figure 5, a continuation of sub-goal G6.

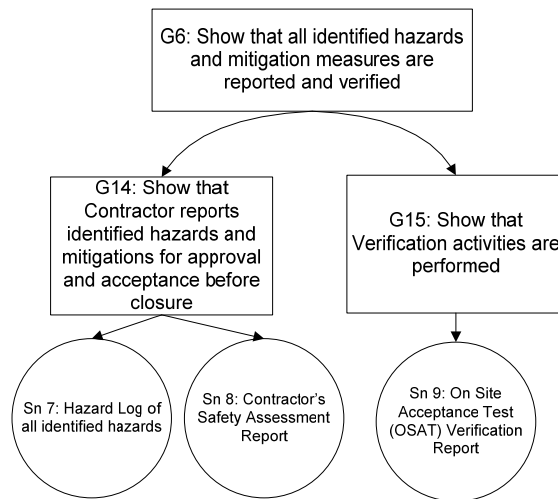


Figure 5 G6 with Sub-goals and Solutions

At the end of the GSN, the solution block (as represented by Sn7, Sn8 and Sn9 in Figure 5) presents the direct reference to the evidence. For instance, Sn9, the On Site Acceptance Test (OSAT) Verification Report is the evidence that G15 (Show that Verification activities are performed) is achieved. When reading a GSN graphical notation, the reader is guided through the chain of assurance argument in a structured manner. This is useful for complicated projects, and can be use to provide a “bird’s eye view” for someone reviewing the safety argument of the programme. For this programme a total of seventeen solution blocks provide assurance that the Top Goal was achieved.

Bridging the Gap

One of the key steps in executing the system safety effort was the requirement to seek risk acceptance by the SAF. One interesting question which was posed to the PMT was

whether the SAF should accept the residual risk for ALL hazards associated with the operation of the VVT (inclusive of “universal hazards” which the general public would also be exposed to) or should they only accept the risks associated with the hazards which are unique to the flying techniques being executed by the SAF. After some deliberation, it was rationalised that only the hazards which are unique to the users of SAF need to be accepted by SAF. This landmark decision sets the baseline for future projects of this nature.

Conclusion

Applying System Safety has demonstrated positive benefits for all the parties involved in this Public Private Partnership programme. MINDEF/SAF acceptance authorities were successfully apprised of the unique hazards associated with the use of the VVT. It equipped them with relevant information to make a deliberate decision and allow the use of the VVT for the SAF users. The SAF users reaped benefits from the availability of a safe, realistic and cost effective training environment. The DSTA PMT was able to successfully deliver a state-of-the-art capability to its customers in good time. The contractor, SVS, enhanced their competency in applying a risk-based process in the form of System Safety. Besides meeting the contractual requirements for this programme, they could adapt similar techniques to meet local legislative requirement of the Workplace Safety and Health Act.

Having introduced System Safety into its Life Cycle Management Framework since 2000, MINDEF/SAF has made significant advancement in the application of the System Safety process. DSTA, together with MINDEF/SAF will continue to enhance and fine-tune the methodology to meet challenges from the ever-changing security and defence landscape. The involvement in this PPP programme provided a unique experience to tailor the existing framework for future applications in similar programmes.

References

- Ericson, C. I. (2005). *Hazard Analysis Techniques for System Safety*. New Jersey: John Wiley & Sons Inc.
- Kelly, T. (1998). “*Arguing Safety: A Systematic Approach*,” *PhD dissertation*. Dept of Computing, Univ. of York.
- Kelly, T., & Weaver, R. (2004). The Goal Structuring Notation: A Safety Argument Notation. *Proc. Workshop Assurance Cases: Best Practices, Possible Obstacles, and Future Opportunities* .
- Teo, Y. K., & Fan, Y. S. (2007). Development of a Credible Preliminary Hazard List -The First Crucial Step in a Successful System Safety Effort-. *International System Safety Conference 2007*.
- The Drafting Committee, University of York. (2010). *GSN Draft Standard*. Retrieved January 10, 2011, from The Goal Structuring Notation: <http://www.goalstructuringnotation.info/>