An Innovative Application of System Safety Methodology

ABSTRACT

System safety uses a risk management strategy based on the identification and analysis of hazards, as well as the application of mitigation controls through a systems-based approach. For the military, system safety practice is guided by the MIL-STD-882D US Department of Defense Standard Practice: System Safety.

This article shares how a DSTA Project Management Team (PMT) leveraged the system safety process in the Ministry of Defence Life Cycle Management, to influence the safety assurance for a proprietary commercial facility which has been tapped for military training. In addition, the article presents various challenges faced by the PMT and the relevant strategies adopted in response. The Goal Structuring Notation was an effective tool used to present the safety argument.

Fan Yue Sang
Chua Boon Heng
Heah Minyi

AN INTRODUCTION TO THE VERTICAL WIND TUNNEL

The Vertical Wind Tunnel (VWT) combines a series of fans, ducts and vanes to produce a vertical laminar stream of air by recirculating wind energy. This recirculating laminar airflow provides stable lift to the personnel within the flight chamber, simulating a free fall. While "flying" in the flight chamber (see Figure 1), the flyer can execute various flight manoeuvring techniques.

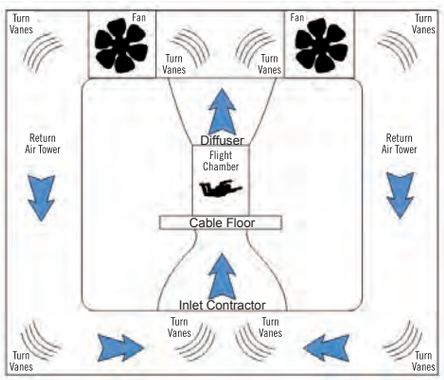

Figure 1. Layout of a typical VWT

Training in the controlled environment of VWT facility brings along numerous benefits, such as minimised risks of mishaps as compared to going for "live" jumps at high altitude. "Live" jumps are inherently hazardous with incidents including parachute malfunction and sudden inclement weather. With risks minimised, personnel can develop confidence and fine-tune their free falling technique in a controlled and safe environment. The mishap severity associated with "flying" in the VWT is reduced significantly as compared to an actual skydive.

Utilising a VWT also reduces substantial cost and time for the Singapore Armed Forces (SAF). An actual jump would incur the high cost of using an aircraft. Furthermore, there is only a short window of opportunity for each jump due to the need for the aircraft to take off, transit to the drop zone and then land. In the case of the VWT, the free faller could make use of extended time blocks in the VWT to perfect his techniques without the need to get on board an aircraft repeatedly for each free fall. This allows the SAF to manage training slots effectively and efficiently, shortening the learning curve for novices and maintaining currency of their skills.

The VWT was designed originally for public use. Members of the public using the VWT would only need to put on a jumpsuit and helmet. Military personnel, however, are required to carry additional equipment and accessories, which may affect their safety and the performance of the VWT. As the VWT is a proprietary licensed commercial facility, the DSTA Project Management Team (PMT) had limited influence on its design aspects. Furthermore, information about the design was limited due to intellectual property protection. Thus, innovative approaches (Fan et al., 2011) were used to secure the required safety assurances for our military free fallers while ensuring that members of the public could continue enjoying the facility as before.

CHALLENGES FACED

Unfamiliar System, Uncharted Territories

The application of military system safety processes for a commercial venture involved challenges.

The primary challenge faced by the PMT was related to the nature of the VWT. The VWT was the first of its kind to be built in Singapore, and the PMT had no prior experience in the acquisition management of such systems. In addition, the contractor operates a franchise licence from Sky Venture International (SVI) which builds, operates, and maintains 32 VWTs around the world. This franchise licence meant that the scope of the system safety analysis was not easy to define. The proprietary and closed nature of the system's design restricted the release of detailed information about the system.

The PMT brainstormed and developed various ways of overcoming the problem of limited available information. One of the possible solutions was to examine existing reports and compliances which could be used as a basis to justify the belief that the use of the VWT was inherently safe for the SAF. Employing this idea, the PMT rationalised that the proof of compliance to local legislative licensing requirement and the contractor's commissioning certificates could form a basis for safety assurance. This primary approach was documented (see section on Innovative Application of System Safety Activities).

System Safety and Existing Safety Systems

The contractor responsible for the operation and maintenance of the VWT is Sky Venture Singapore (SVS) which is a franchisee of SVI. With SVI's extensive experience in international operations and its excellent track record in safety, one could be reasonably confident that the VWT was safe and met all commercially required levels of safety. The proven facility design, well-written safety manuals, as well as the safety operational procedures and checklists were part of a programme to ensure that daily operations would be safe.

Nevertheless, the need for military equipment and free fall techniques in the VWT warranted additional safeguards to enhance safety. System safety was used to value add to the existing safety systems, through the methodical discovery of atypical hazards which are faced by military free fallers but not the general public. These hazards were documented in the Preliminary Hazard List (PHL) (Ericson, 2005) which is discussed in the following section.

INNOVATIVE APPLICATION OF SYSTEM SAFETY ACTIVITIES

Defining Uncharted Territories

One of the key challenges to the programme was to determine how to provide primary safety assurance to the military users without compromising proprietary information, given that the system was unique and proprietary to SVI. The PMT had to explore ways to overcome this challenge.

Before the VWT could be open for public entertainment, it had to comply with legislative requirements whereby the service provider had to provide evidence to show that the VWT was safe for public use. Leveraging this need for compliance to legislative requirements, the PMT obtained the same information from SVI to assess the VWT for military free falls. The legislative approvals and certifications are summarised as follows:

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

Under Singapore's Public Entertainments and Meetings Act, entertainment that is provided at any place accessible by the public requires a Public Entertainment Licence from the Singapore Police Force. To obtain this licence, the attraction has to be certified by a competent body, which is the Conformity Assessment Body, as having met relevant technical and safety standards. SVS thus had to obtain the Public Entertainment Licence prior to commencement of operations.

b) Legislative Requirement: Certificate of Statutory Completion and Fire Safety Certificate

SVS hired Registered Inspectors who specialise in the architectual aspects as well as the mechanical and electrical aspects of safety to certify the building and fire safety works. SVS also appointed personnel as Qualified Persons, who had to submit all documents related to the fire safety works to the Registered Inspector to perform the safety assessment. When the details of the assessment were submitted and found to be satisfactory by the Singapore Civil Defence Force and the Building Construction Authority, the Certificate of Statutory Completion and Fire Safety Certificate were issued.

c) Applicable Certification: Original Equipment Manufacturer Commissioning Certificate

During the final stages of constructing the VWT, SVI provided technical support 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.

d) Applicable Certification: SVS Instructors Certification

SVS instructors are trained personnel who ensure the safety of flyers in the wind tunnel. In the event of an emergency situation, the instructor's ability to prevent injuries to the flyer is crucial. SVS consistently keeps its instructors current by following a stringent set of requirements laid out by the International Bodyflight Association (IBA). IBA certifications issued to SVS instructors and tunnel operators are submitted to the SAF for periodic reviews.

With these proofs and certifications of compliance with legislative requirements, the PMT could use them as evidence for the system safety assessment within the Ministry of Defence (MINDEF). This approach is unique and different from the typical acquisition of weapons-related systems and platforms, where system safety techniques such as Fault-Tree Analysis and Functional Hazard Analysis are typically used as the means of providing safety assurance.

Collaborative Application of System Safety

The PMT, SVS and the SAF worked collaboratively to apply the System Safety methodology and techniques for the VWT to enhance the existing safety documentation. One area of collaboration was the development of a PHL, which was the first step in the System Safety process to identify potential hazards associated with the use of this system. To identify these hazards, the PMT needed a certain level of background information and engineering details which could not be revealed due to SVI's intellectual property rights.

The PMT brainstormed and adopted a three-pronged approach to develop this PHL.

First, dialogue sessions were conducted with SVS and SVI to extract potential hazards based on their experience in operating other VWTs. By analysing the safety features of the VWT, the PMT was able to retrospectively visualise the hazards that the safety features might be trying to protect against. Once the PMT had an idea of the possible hazards, it deliberated if such hazards could develop into other forms of hazards based on the unique utilisation of the VWT by the SAF.

Second, dialogue sessions were held with members of the SAF who are experienced skydivers or instructors to gather potential operational and training hazards. These dialogue sessions provided valuable information so that the PMT could sieve out credible hazards from the PHL.

Third, the PMT visited VWTs overseas to get a first-hand account of the safety features and issues relating to the use of such a system. While some hazards were universal, the PHL helped to identify hazards that were associated with the unique military applications of the VWT. Table 1 shows some of these hazards and the relevant mitigation measures.

The ability to identify hazards unique to military applications led to the incorporation of mitigation measures to reduce the mishap risk. For instance (see S/N 2 of Table 1), a procedure was enforced to ensure that trainees do not exit the VWT from a flying position. With information on these hazards, the SAF Commanders are able to make a better informed decision to manage their training requirements effectively and safely. The

S/N	Hazard Description	Causal Factors	Mitigation Measures
1	Military equipment falls off flyer	Failure of equipment securing mechanism	• Introduce a locking mechanism (capable of withstanding gravitational forces) to allow the flyer to strap and hook military equipment close to his body
2	Flyer carrying military loads attempts to exit VWT from a flying position, impacting the exit	Unstable flying position due to added equipment bulk	• Introduce a soft cushioning at the exit-cum-entrance of the flight chamber • Enforce the rule that military flyers with equipment shall exit only from a standing position
3	Kinetic energy of recirculating objects	Presence of loose objects (shoes, gloves, goggles, etc.)	• Use existing features such as the plenum, turn vanes and cable floors to impede flying objects from recirculating in the VWT • Conduct more frequent checks at points where loose objects are collected, to eliminate potential recirculation of such objects

Table 1. PHL

identification of the atypical hazards highlighted that system safety complements the existing safety management systems of SVS.

System safety was also seen as a useful tool for SVS as it provided some form of training and experience to identify workplace safety and health hazards. The identification of these hazards was relevant to SVS which needed to comply with the Workplace Safety and Health Act passed in 2006. This Act stresses the importance of managing workplace safety and health, with the requirement for stakeholders to take reasonably practicable measures to protect workers.

Goal Structuring Notation

Goal Structuring Notation[1] (GSN) is a graphical argumentation notation (Kelly, 1998; Kelly and Weaver, 2004) used to explicitly document the elements of any argument. It originated from the University of York in the early 1990s, but it was only formally recognised in November 2011 as a tool to improve the structure, rigour and clarity of safety arguments during the presentation of safety cases.

For this VWT programme, GSN was used initially to define the challenges at hand and to list the possible solutions to these challenges. Subsequently, it was also used as a representation tool to present a top level view of how the VWT was at an acceptable level of safety for use. These functions of the GSN facilitate easier understanding of the safety issues. Thus, the PMT used the tool for an effective presentation of safety cases to members of the safety boards.

When the elements of GSN (as shown in Table 2) are connected together, a goal structure is formed. Goal structures document the chain of reasoning in the argument with the relevant substantiating evidence. The principal purpose of a goal structure is to show how goals are broken down successively into sub-goals, until a stage where claims can be supported by direct reference to available evidence. A part of the actual GSN created for the project is shown in Figure 2.

GOAL	A goal, rendered as a rectangle, presents a claim forming part of the argument.
STRATEGY	A strategy, rendered as a parallelogram, describes the nature of the inference that exists between one or more goals and another goal.
CONTEXT	A context, rendered as a rectangle with rounded corners, presents a contextual artefact. This can be a reference to contextual information or a statement.
SOLUTION	A solution, rendered as a circle, presents a reference to evidence.

Table 2. Basic symbols of GSN

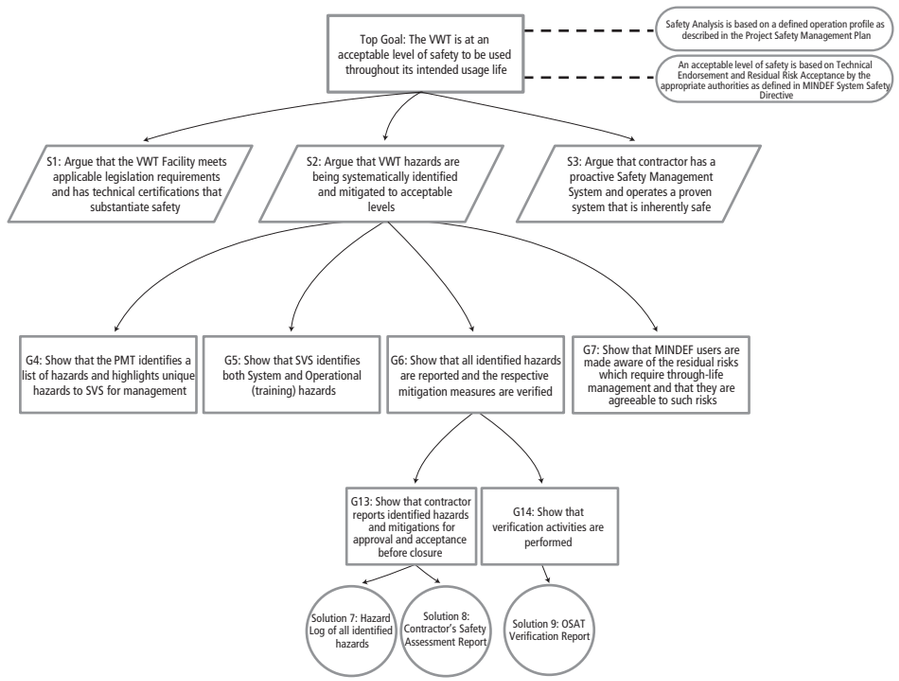

Figure 2. A portion of the GSN diagram for the VWT programme

The defined top goal for the GSN of the project was: "The VWT is at an acceptable level of safety for use throughout its intended usage life". The GSN has two contextual entries displayed on its right, which are important to capture the context for interpreting the top goal.

The top goal is further expanded into three separate strategy blocks namely S1, S2 and S3. Each strategy block is a reasoning step which interfaces between the top goal and the sub-goals. The descriptions in S1, S2, and S3 support the top goal. This GSN continues to be developed until sufficient evidence is found to substantiate the top goal. The evidence collected is represented by solution blocks (see solutions 7, 8, and 9 in Figure 2). For instance, solution 9 "On-Site Acceptance Test (OSAT) Verification Report" is the evidence that G14 "Show that Verification activities are performed" has been achieved.

When reading the GSN tree, the reader is guided through the assurance argument in a structured manner. This provides a bird's eye view of the safety argument, which can enable someone without any prior system knowledge to review the argument.

CONCLUSION

System safety is typically applied for the acquisition of weapons-related systems and platform-type defence capabilities, taking reference from the Military Standard: MIL-STD-882D (2000). Hence, applying the system safety requirements from MIL-STD-882D to a commercial programme posed several challenges which called for innovative approaches.

Applying system safety to this unique programme benefitted all parties. First, MINDEF and the SAF acceptance

authorities were equipped with information on the unique hazards of using VWT in a military context – thus they were able to decide on its application in SAF's trainings. Second, system safety helped to ensure a safe, realistic, reliable and cost-effective training environment for the SAF. Third, the PMT was exposed to new tools and methodologies through its collaboration with a commercial service provider, gaining knowledge that can be applied to similar programmes in the future. Finally, SVS enhanced its competency in applying a risk-based process and it could adapt similar techniques to meet local legislative requirements of the Workplace Safety and Health Act.

ENDNOTES

[1] The GSN became a community standard on 16 November 2011 and is freely available on the Internet. The website is at www.goalstructuringnotation.info/

REFERENCES

Ericson, C.A. 2005. Hazard Analysis Techniques for System Safety. New Jersey: John Wiley & Sons Inc.

Fan, Y.S., Chua, B.H., Tan, R., Heah, M.Y. and Ooi, C.K. 2011. Applying System Safety Methodology and Related Tools for a Public Private Partnership (PPP) Programme. Paper presented at the International System Safety Conference 2011, Las Vegas, USA.

Kelly, T. 1998. Arguing Safety: A Systematic Approach. PhD dissertation, University of York.

Kelly, T. and Weaver, R. 2004. The Goal Structuring Notation: A Safety Argument Notation. Paper presented at the Workshop on Assurance Cases: Best Practices, Possible Obstacles, and Future Opportunities, Florence, Italy, 1 July.

MIL-STD-882D. 2000. Department of Defence Standard Practice: System Safety.

BIOGRAPHY

Fan Yue Sang is a Principal Engineer (Systems Engineering). He is responsible for the development and implementation of the System Safety Assurance process for DSTA. Before joining DSTA, Yue Sang was an Air Engineering Officer in the Republic of Singapore Air Force and rose to the rank of a Lieutenant-Colonel. In his 24 years of service, he served in various capacities, including the Commanding Officer of a Maintenance Squadron. From 2007 to 2009, Yue Sang was the President of the System Safety Society (Singapore Chapter). He graduated with a Bachelor of Science (Aeronautical Engineering) degree from the University of Manchester, UK in 1988 and a Master of Science (Aeronautical Engineering) degree from the Naval Postgraduate School, USA in 1995.

Chua Boon Heng is an Engineer (Systems Engineering). He provided system safety assurance support on platform projects, as well as related developmental work on systems safety. As a recipient of the DSTA Postgraduate Scholarship, Boon Heng is currently pursuing a Master of Science (Systems Engineering) degree from the Naval Postgraduate School, USA. He graduated from Nanyang Technological University (NTU) with a Bachelor of Engineering (Mechanical Engineering) degree in 2007.

Heah Minyi is an Engineer (Systems Engineering). He provides system safety assurance support to various platform projects in DSTA. Besides contributing to the development of organisational system safety processes, Minyi is actively involved in the planning and execution of in-house system safety courses. He graduated with a Bachelor of Engineering (Electrical and Electronic Engineering) degree from NTU in 2008.