Managing Technical Project Risks using STPA

Shufeng Chen*
WMG, University of Warwick, UK

1. Introduction & Motivation

A technical project refers to a project that involves the development, implementation, or management of technology-related solutions. There have already been technical projects going on everywhere. Technical project size varies depending on the scope and resources needed. Small-scale projects such as the development of a mobile application can progress with only less than 10 people. In contrast, a large-scale project would involve hundreds or even thousands of individuals across different roles and responsibilities. The challenges of completing a large-scale project arise due to the complexity of stakeholder interactions and emergent project risks. An example of emergent project risks could be an underperformance individual or team during the key phase of the project. Since each stakeholder of the project is working together to achieve a common project scope, they can be treated as a 'component' or 'function' of a 'system'. An underperformance 'component' cannot be simply identified as a 'component failure', instead it could be a symptom of systematic failure/flaw, which would need to be analyzed using a system-level analysis. A system-thinking-process method could therefore be applied to model and understand such complex interactions, and further identify potential project risks.

In this abstract, the author would like to propose a recent application of STPA to model the structure of a government-funded project related to the development of an electric vehicle. The project covers a diverse range of stakeholders, including regulators, and funding authorities from the Government, certification agencies related to vehicle type approval and ISO26262 certification, funded stakeholders involving the electric vehicle original equipment manufacturing (OEM) and its tier 1 (electric powertrain solution supplier) and tier 2 (battery management system solution supplier) suppliers, vendors of essential parts, and the public.

The initial motivations of this work are:

- To provide project stakeholders insights into the project structure and further the efficiency and accuracy of communications.
- To identify existing or potential flaws in the project structure.
- To create a blame-free working culture.

2. Results

To initiate the analysis, a couple of meetings involving funded stakeholders were scheduled to identify unacceptable losses and system-level hazards.

The initial losses agreed upon include:

- L1: Loss of capability of meeting project scope.
- L2: Loss of organizational reputation.
- L3: Loss of human life
- L4: Loss of damage to the property

The system-level hazards agreed upon include:

- H1: Resignation of project stakeholders. [leading to L1, L2]
- H2: Project stakeholders lose trackers on the project structure and progress. [Leading to L1]
- H3: Project operation does not meet the safety regulations. [Leading to L1, L2, L3, and L4]

The progress of the project is initially driven by human effort, any lack of workforce would mean a delay of the work and blocker of other stakeholders' work, leading to a loss of capability of meeting project scope (i.e., L1). It could also impact the way other stakeholders or external people think about the organization, leading to loss of organizational reputation (i.e., L2). If project stakeholders lose track of the project structure or progress, it will certainly degrade the efficiency and accuracy of their work, leading to L1. The development of an electric vehicle can be very safety-critical since it relates to the storage and deployment of high voltage (up to 1000V) batteries. Therefore, the occurrence of H3 could lead to all the losses.

Control Structure:

A couple of control structures were created at different abstraction levels. Due to the limited space, only two control structures (as illustrated in Fig.1 and Fig.2) were uploaded to this abstract (*please feel free to reach out if you need more information to proceed with the decision*).

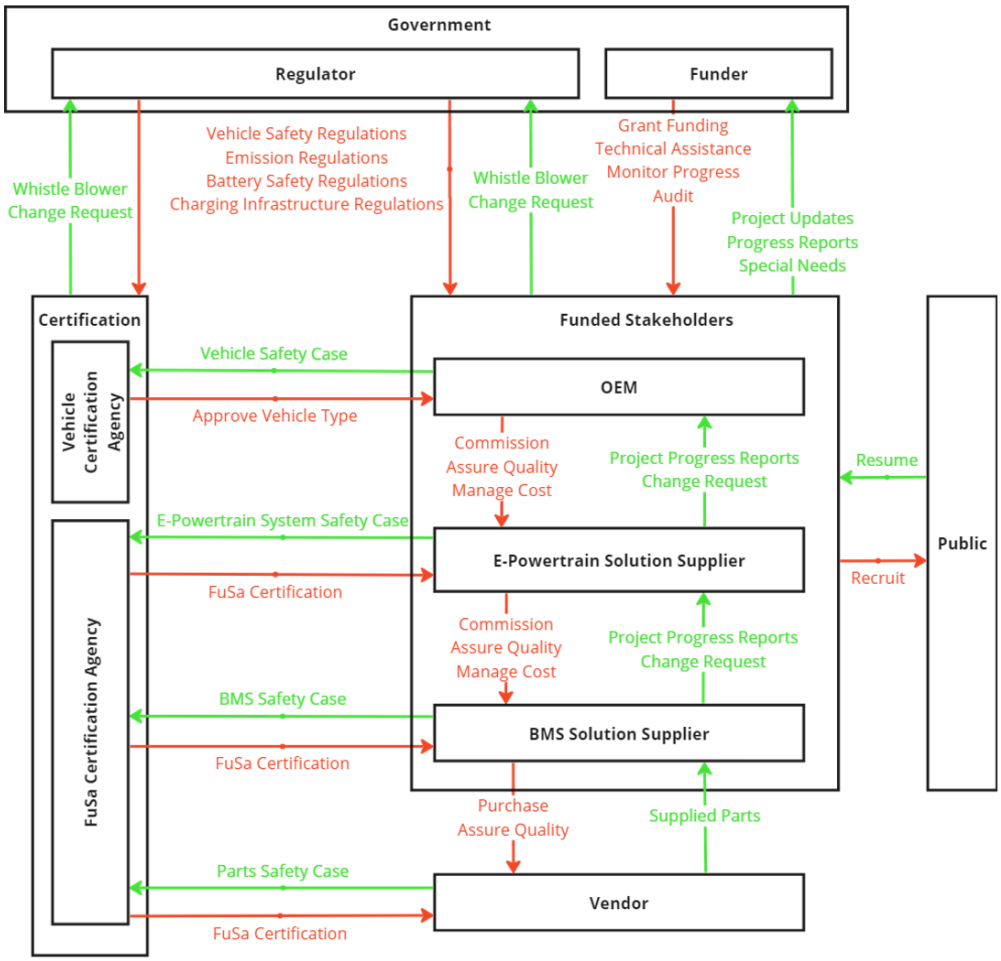

Fig. 1 A high-level control structure covering all stakeholders

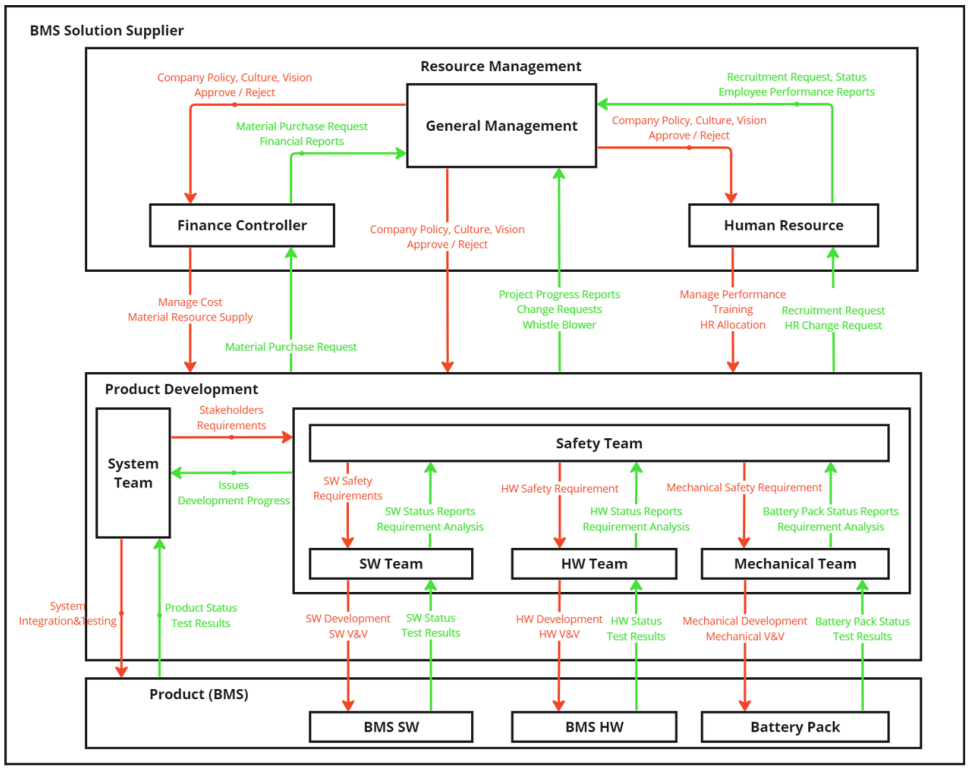

Fig. 2 Control structure of BMS Solution Supplier

UCAs and Loss Scenarios:

Due to the complexity of the system and the need to balance between the investments of time on the project tasks and STPA, the analysis has been ongoing slowly. Therefore, not all the control actions shown in the control structure have been analyzed thoroughly. However, there are a few 'interesting' UCAs and their derived Loss Scenarios which the author would like to highlight below. Both UCAs are based on the control structure in Fig. 2.

1. UCA-1: Safety Team issues incorrect/outdated SW Safety requirements to the SW Team when the SW team is in a critical phase of releasing the next version of the software. [Leading to H2]
2. UCA-2: General Management does not provide (or barely provide) organizational vision to the Development Team when there have been new team members joining, and HR is away. [Leading to H1]

For UCA-1, issuing incorrect requirements could be easily fixed once identified. However, the consequence can be severe if it happens during a critical deliverable phase. From the requirement management point of view, the requirements can be updated from time to time depending on the progress of the development and the interactions with other stakeholders. It is essential to record and be able to identify the change of requirements. Following standard procedure, the requirements are recorded in Excel and uploaded to the document version control system called SVN. In this UCA, the requirement engineer believed that he had already updated the requirement file because he did so in his local folder but was unable to commit the latest file to the server due to IT issues (and he was unaware of it). When communicating with the SW team, he simply copied the SVN link into an email mentioning that the latest requirement list was ready. If the engineering procedure/training does not require the inclusion of version number in such communication, or vice versa the recipient double checks the version number, this UCA could very likely happen again with different people.

For UCA-2, a general manager could have already been overwhelmed with various tasks and dedicated to HR for organization inductions. However, the general manager was not aware that HR was away as they did not have catch-ups recently. A new joiner without a welcoming induction of the organization could soon lose confidence and motivation, and therefore decide to leave (i.e., H1). To avoid this UCA, it is suggested that each team leader should also be able to conduct organization-level induction (on top of team-level induction). Also, if any team member is away, they should set up relevant messages in their calendar or auto-reply.

3. Conclusions

The STPA analysis of project risk management was initiated at the start of 2024. It is still ongoing and so far, we have identified 80 UCAs and around 200 loss scenarios from these UCAs. The graphical nature and simplicity of STPA have made the analysis outputs relatively easy to communicate and interpret the potential risks. Although there is a trade-off between the time spent on the project work and the analysis, from our experience, they complement each other. Having applied STPA, the team members develop a system-thinking process in mind, which helps them more clearly understand their daily tasks and the reasons behind them. Throughout their daily work, any potential risks could also be identified by each team member, which can then be further analyzed using STPA.