Systems-Theoretic Likelihood and Severity Analysis for Safety and Security Co-Engineering

William G. Temple[1], Yue Wu[1], Binbin Chen[1], Zbigniew Kalbarczyk[2]

[1] Advanced Digital Sciences Center, Illinois at Singapore
[2] {william.t, wu.yue, binbin.chen}@adsc.com.sg
[3] University of Illinois at Urbana-Champaign, Illinois, USA
kalbar@crhc.illinois.edu

Abstract. A number of methodologies and techniques have been proposed to integrate safety and security in risk assessment, but there is an ideological divide between component-centric and systems-theoretic approaches. In this paper, we propose a new hybrid method for Systems-Theoretic Likelihood and Severity Analysis (STLSA), which combines desirable characteristics from both schools of thought. Specifically, STLSA focuses on functional control actions in the system, including humans-in-the-loop, but incorporates semi-quantitative risk assessment based on existing industry practice. We demonstrate this new approach using the case study of train braking control.

1 Introduction

Until recently, the security of information, communication and control systems has been considered separately from issues of safety during system design. However, there is growing recognition that safety and security properties and related design features may influence one another. This has led to a growing body of work relating to safety and security co-engineering. However, while there are a number of analysis methods available to help designers analyze the safety and security of a system, cyber security threats today are becoming more complex, and attackers can exploit physical phenomena in the system and environment (e.g,. Stuxnet), as well as humans-in-the-loop (e.g., phishing) to cause harm. In addition, for systems such as an automated (unattended) metro train, safety features like the emergency braking function could be exploited by cyber attackers to cause large-scale service disruptions. For example, in 2016 in Singapore, the circle line metro train system was affected with intermittent emergency braking of several different trains over the course of more than a week [22]. While the issue was eventually traced to a component failure on an individual train [5], it raises questions about whether such an event could be replicated maliciously.

Those types of complex interactions are challenging to account for using traditional methods for design-stage risk assessment such as fault trees, or failure mode and effects analysis—methods we refer to as component-centric [20]. The Systems-Theoretic Process Analysis for Security approach (STPA-Sec) [23],

with its emphasis on control loops, emergent system behavior and qualitative assessment of unsafe or insecure scenarios may offer one path to addressing these challenges. However, following the STPA-Sec process results in the identification of a large number of threat and/or failure modes [16], and that methodology does not provide further guidance on how to address those scenarios. The complexity of today's cyber-physical systems implies a great need for risk-based analysis to help system stakeholders understand the significance of safety/security issues and prioritize remediation. In this paper, we propose a new safety and security co-engineering method, Systems-Theoretic Likelihood and Severity Analysis (STLSA), which provides a top-down view of the functional control structure of a system and enriches threat/failure scenarios with a semi-quantitative risk rating system (severity times likelihood) inspired by a component-centric analysis method [15]. Specifically, we make the following contributions:

- We propose a new hybrid method, STLSA, to leverage advantages of STPA-Sec [23] and FMVEA [15] and address gaps.
- We present a case study applying this method on a realistic train braking system based on information provided from a railway operator.

The outline of this paper is as follows: in Section 2 we discuss related work in Safety and Security Co-Analysis; in Section 3 we present the Systems-Theoretic Likelihood and Severity Analysis method; in Section 4 we apply the STLSA method on a train braking system case study and discuss the results before concluding in Section 5.

2 Related Work in Safety and Security Co-Analysis

A number of methods have been proposed to improve the completeness of system risk assessment by covering the interactions between both unintentional/non-malicious failures, and intentional/malicious threats [4, 12, 9]. Different schools of thought have emerged regarding the appropriate manner of examining a system and evaluating potential hazards and corresponding risks. Many of the approaches in the literature are related to the field of security requirements analysis, which has been an active research area of its own (e.g. [11] and references therein) and often makes use of graphical models and risk assessment. Requirement analysis has been studied in the context of safety critical systems [8] as well. However, in our discussion of related work we focus on research that attempts to explicitly analyze safety and security risks together, often by combining or extending existing approaches from standards or academic literature. Below, we summarize a review and classification of safety/security methods from our earlier position paper [20] before detailing our STLSA approach in later sections.

Table 1 presents a taxonomy of prior work on safety and security co-analysis. In the first column of the table, Security Aware Hazard Analysis and Risk Assessment (SAHARA) [10] and Failure Mode, Vulnerabilities and Effect Analysis (FMVEA) [15] extend existing safety analysis techniques from ISO 26262 and IEC 60812, respectively, by incorporating threat information based on the

Table 1. Classification of related work [20]

	Extend	**Combine**	**Alternative**
Component-based	SAHARA[10], FMVEA [15]	FACT Graph[14], EFT[6]	
Systems-based		CHASSIS[13]	STPA-Sec[23], STPA-SafeSec[7]

STRIDE [19] model. In the middle column, the Failure-Attack-CountTermeasure (FACT) Graph [14], and Extended Fault Tree (EFT) [6] are based on a combination of fault tree and attack tree methods. Combined Harm Assessment of Safety and Security for Information Systems (CHASSIS) [13], which involves the combination of use/misuse cases and sequence diagrams, is classified as a systems-based approach because it places more emphasis on interactions between entities (which may include human actors) as opposed to the hardware/software structure of the system. In the last column, System-theoretic Process Analysis for Security (STPA-Sec) [23] and the subsequent STPA-SafeSec [7] approaches emphasize a top-down assessment of a system's functional control structure to identify unsafe/insecure control actions.

In our position paper [20], we advocated combining aspects of STPA-Sec (a systems-theoretic approach) and FMVEA (a component-centric approach). In complex systems, a systems-theoretic approach such as STPA-Sec seems to offer advantages in hazard/threat identification. However, the qualitative nature of the output of STPA-Sec and the large number of causal scenarios generated leads to challenges assessing risk. On the other hand, as a component-centric analysis method, FMVEA provides an assessment process with semi-quantitative ratings which is closer to existing industry practice.

3 Systems-Theoretic Likelihood and Severity Analysis

In this section we describe a new process for identifying and jointly analyzing the risks from safety (hazard/accident) and security (threat) perspectives. The Systems-Theoretic Likelihood and Severity Analysis method combines features from STPA-Sec and FMVEA, and integrates them into a unified analytical process. In this section, we first provide a more thorough introduction of the steps in each of the original methods before presenting the hybrid STLSA method.

3.1 Original STPA-Sec Process

STPA-Sec [23] is a security extension of the System-Theoretic Process Analysis (STPA) method from the safety engineering community, which is itself derived from the System-Theoretic Accident Modeling Process (STAMP). The motivation behind STPA-Sec is to consider the impact of cyber security on system safety from a "strategic" rather than a "tactical" perspective: taking a top-down analysis approach focusing on the functionality provided by a system, and

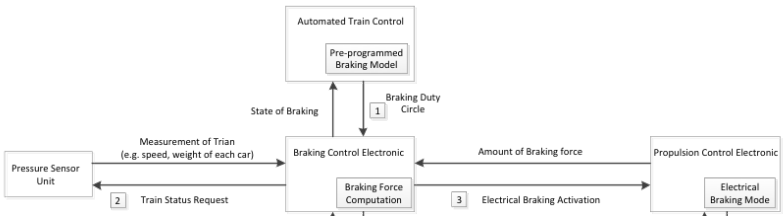

Fig. 1. Partial example of a functional control structure for a train braking system

its functional control structure, rather than focusing on threats and attacker properties such as intent and capability.

The process for carrying out STPA-Sec analysis is as follows:

1. Identifying **unacceptable losses** that should be avoided (called, Systems Engineering Foundation in [23]).
2. Modeling the system's **functional control structure** (see Figure 1)
3. Identifying **unsafe and/or insecure control actions** from the functional control structure using guide phrases (e.g., control provided too early/late)
4. Identifying **causal scenarios** which may be used to define security requirements and constraints.

It should be noted that the output of STPA-Sec analysis is qualitative in nature: a list of control actions in the system that may be unsafe or insecure, and how those control actions may lead to unacceptable losses in one or more causal scenarios. The STPA-Sec approach does not evaluate the relative likelihood or severity of impact for those causal scenarios, which is not fully aligned with current safety/security standards [16, 9]. In fact, the authors of [7] motivate their STPA-SafeSec approach in part by noting that the original method does not provide guidance on how to proceed after unsafe/insecure control actions and causal scenarios are identified.

3.2 Original FMVEA Process

FMVEA is an extension of the widely-used Failure Mode and Effect Analysis [15] method for safety risk assessment, as described in IEC 60812 [1]. FMVEA includes security-related information such as vulnerabilities, threat modes (based on STRIDE [19]), and threat effects. As described in [15], the FMVEA analysis process is as follows:

1. Divide a system into components
2. For each component, identify failure modes and/or threat modes
3. Identify the effect of each failure and/or threat mode (includes attack probability)
4. Determine severity of the final effect
5. Identify potential causes / vulnerabilities / threat agents

6. Estimate frequency or probability of occurrence for the failure/threat mode during the predetermined time period
7. Steps 3-6 repeat until there are no more failure modes/vulnerabilities or components left to analyze

We consider FMVEA to be a *component-centric* analysis method, as opposed to STPA-Sec which is *systems-centric*. The authors of [7] adopt a similar taxonomy, considering methods such as traditional FMEA and Fault Tree Analysis as failure-based hazard analysis (i.e., based on component failure), while STPA-Sec is regarded as systems-based hazard analysis. One challenge that component-based methods face is scalability: for large systems, particularly those with complex interactions or emergent behavior, is it sufficient to consider lower level failures and threats? Another challenge is the issue of multiple failures, which are far more plausible in a deliberate attack (security context) as compared with an accidental or random failure (safety context). Finally, in FMEA/FMVEA the *effect* component considers system effects, but the manner in which they are identified is not always made explicit.

An FMVEA case study paper [18] elaborates that components can be either hardware/software, or functions depending on the maturity level of the system design. Similarly, a more recent FMVEA case study [17] includes a three-layer dataflow model of the system as first step in the analysis process, to support the identification of failure modes and effects. If one takes the view that this preliminary system modeling exercise is independent from the documented FMVEA process as described in [15], it raises the question of whether STPA-Sec's functional control structure models could serve the same purpose, and whether the unsafe/insecure control actions would also help to inform FMVEA analysis.

3.3 STLSA Combination

STLSA aims to leverage the high level (functional) control models from STPA-Sec, as well as the guide words and phrases, while introducing a familiar rating process inspired by FMVEA for evaluating the risk of causal scenarios. Risk in this sense is the product of a scenario's severity and the likelihood of occurrence. Severity and likelihood are rated on an ordinal scale (e.g., 1–4), providing a semi-quantitative risk score. In this paper, we use rating scales from existing railway standards and apply the method in a railway case study (see Section 4), however other industries (e.g., aviation) may have alternate rating systems that are already familiar to practitioners, and that could be applied within STLSA. Figure 2 depicts the steps in the STLSA analysis process, which we outline in detail below.

Systems-theoretic analysis

We start with an STPA-Sec analysis, with the steps summarized in [23]. However, there are a number of ways in which the functional control structure (step 2), and identification of unsafe/insecure control actions (step 3) are enhanced to better address complex interactions (see Section 4 for an example).

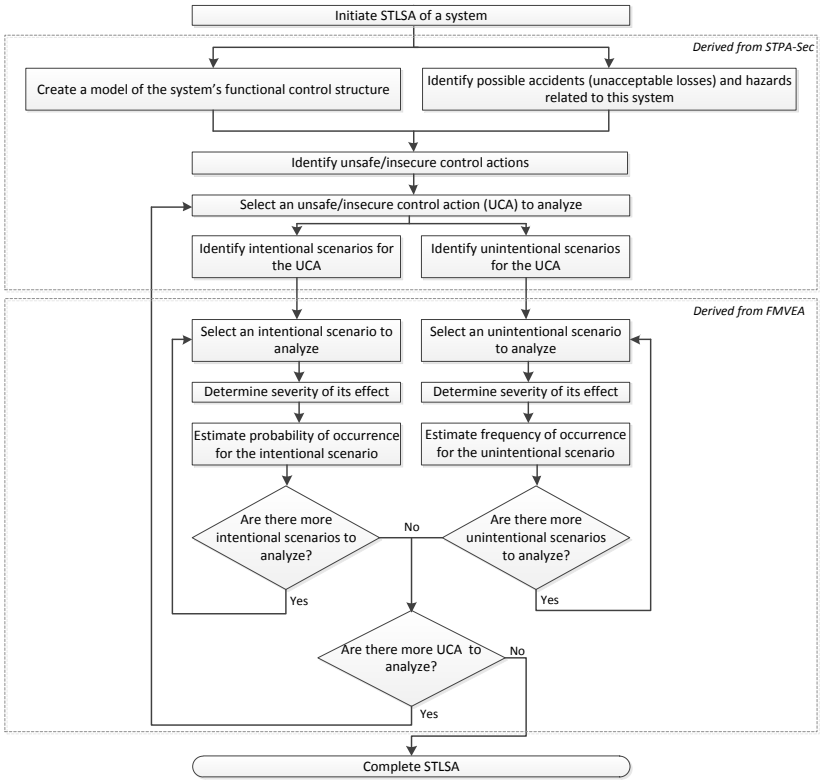

Fig. 2. STLSA: a Hybrid Method of FMVEA and STPA-Sec

– Explicitly indicating which aspects of the functional control structure are in the system and which are in the environment. Connections between the two are indicated with dashed edges.
– Showing multiple instances of actors & components in the system. This is intended to prompt analysts to think about complex failure modes between instances (e.g., multiple trains in a metro, or supposedly identical components behaving differently).
– Applying the extended guide word analysis from [16] (shown in Figure 3) when identifying causal scenarios for unsafe/insecure control actions. This introduces additional coverage for intentional scenarios (e.g., considering a spoofed controller).

An example of a causal scenario could be *jammed control input* for a train braking control unit, where the italicized text refers to a guide word applied to a generic control loop that is used to aid the assessment process (see Figure 3). Once the causal scenarios for each unsafe/insecure control action are identified,

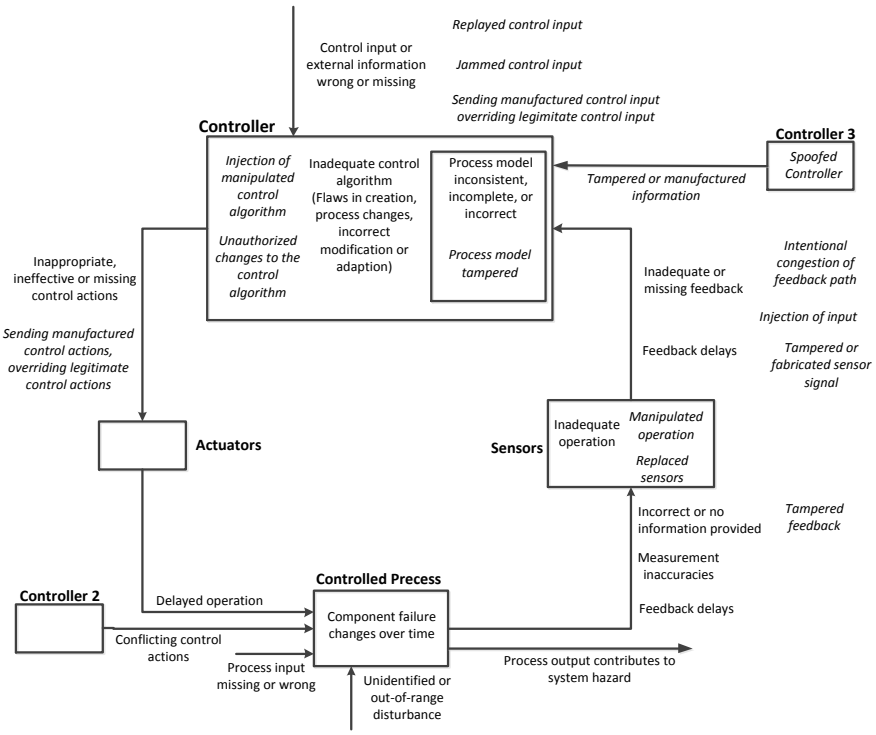

Fig. 3. Control loop with extended guide word (adapted from [16])

we borrow concepts from FMVEA [15] to assess the risk of each causal scenario in a more nuanced manner.

Severity analysis of causal scenarios

A causal scenario for an unsafe/insecure control action may be thought of as a failure mode in FMVEA. A failure mode has an effect, and that effect has a severity associated with it (see Figure 4). In STLSA, the effect of a causal scenario may be identified from the functional control structure. The severity of a causal scenario is assigned a rating; in this case we use railway safety standard EN 50126-1[3] which includes four levels:

1. **Insignificant:** Possible minor injury, and/or system damage.
2. **Marginal:** Minor injuries and/or minor damage to the environment, and/or severe system damage.
3. **Critical:** Severe injures and/or few fatalities and/or large damage to environment, and/ or loss of a major system.
4. **Catastrophic:** Many fatalities and/or extreme damage to the environment.

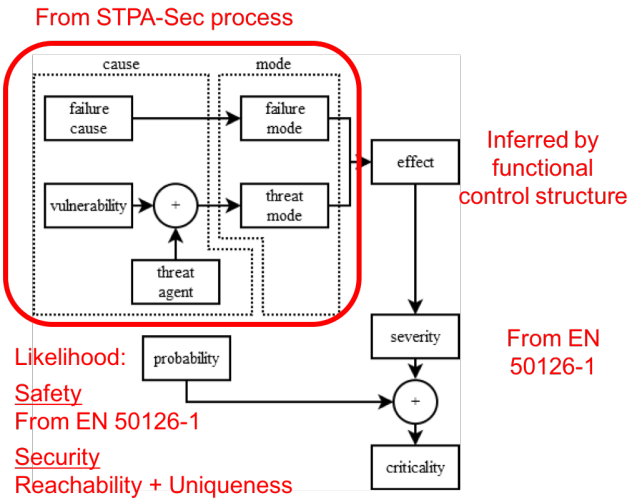

Fig. 4. Annotated FMVEA cause-effect chain (black) illustrating differences in the STLSA method: failure modes and effects are identified via STPA-Sec, while likelihood (probability) and severity have different rating systems.

The classification of severity levels is common between failure (safety) and threat (security) modes.

Rating the likelihood of causal scenarios

We assess the likelihood (called "probability" in [15]) differently for safety and security scenarios, as seen in Figure 2. In safety scenarios, the likelihood is expressed as a *frequency* score. This is quantified according to a 6-tier event occurrence frequency classification, as suggested in EN 50126-1[3], ranging from *highly improbable* (1) to *frequent* (6). The descriptions and for each frequency level are listed as follows:

1. **Highly improbable:** Extremely unlikely to occur. It can be assumed that the event may not occur.
2. **Improbable:** Unlikely to occur but possible.It can be assumed that the event may exceptionally occur.
3. **Rare:** Likely to occur sometime in the system life-cycle. Event can reasonably be expected to occur.
4. **Occasional:** Likely to occur sometime in the system life-cycle. Event can reasonably be expected to occur.
5. **Probable:** Will occur several times. Event can be expected to occur often.
6. **Frequent:** Likely to occur frequently. Event will be frequently experienced.

For security related scenarios, however, we adopt an alternative method to assess the likelihood, which is more closely connected to FMVEA. In [15] likelihood is defined as a combination of system susceptibility and threat properties. However, a challenge arises because the STPA-Sec method—the starting point of STLSA—explicitly rejects a threat-based approach (i.e., focusing on a potential adversary's motivation, resources, etc.), arguing instead for a system-centric focus that starts from identifying unacceptable losses.

Therefore, in our STLSA approach, we exclude the Motivation and Capability elements that characterize threats in FMVEA and focus only on the system's susceptibility to a threat, which is characterized by *reachability* ("R") and *uniqueness* ("U"). The likelihood score for security scenarios is given by $R + U$. These are rated according to the following scales:

- **Reachability** (0 = no network, 1 = temporary connected private network, 2 = normal private network, 3 = public network)
- **Uniqueness** (1 = restricted, 2 = commercially available, 3 = standard)

The Reachability and Uniqueness levels describe how easy it is for a potential adversary to connect to and acquire knowledge about the system. This numerical rating system, while simple, allows analysts to incorporate practical information such as the presence of air-gapped networks or the use of proprietary versus commercial-off-the-shelf devices. While *Uniqueness* is classified into 3 levels as suggested in [15], we add one additional classification in *Reachability*, which is called temporary connected private network. This is intended for components that are occasionally connected to network during patching or maintaining periods. Following this change from the original FMVEA, the likelihood rating scale for both intentional and unintentional sources take values up to 6.

Figure 4 illustrates the STLSA process in a different different manner from Figure 2, focusing on the differences from the original FMVEA method. As shown, the upstream aspects of the FMVEA cause-effect chain are replaced with the systems-theoretic modeling in STPA-Sec, while the downstream assessment steps are maintained with modifications to the rating systems. In the next section we go through a case study to illustrate the end-to-end assessment process.

4 Case Study: Train Braking System

A train's braking system is perhaps the most safety-critical of any subsystem, and as a result of this, modern trains have service and emergency braking processes. However, while there are multiple processes of activating and controlling various braking actions, many of the components involved in braking are shared. In addition to the obvious issue of train collision, the braking system should be designed to prevent other undesirable events. Two high-profile incidents from Singapore's mass rapid transit system illustrate the complex safety and security challenges inherent in this system.

Incident 1: Oil leakage on the track One of the most prominent railway safety incidents in Singapore was a train collision in 1993 [2]. A train that was stationary at the Clementi station was struck by another oncoming train that was unable to stop, injuring 156 passengers. Investigators traced the cause to an oil spill on the track from a maintenance locomotive. The spill had been detected earlier, but delay and miscommunication about clean-up led to a hazard and ultimately an accident. A number of operational changes were made after the accident, including checking all locomotives for oil leakage before and after leaving the depot [21].

Incident 2: Signalling interference from a nearby train More recently, in late 2016, the automated Circle Line train system in Singapore was afflicted with mysterious service disruptions. Trains would lose the signalling network connection seemingly at random and activate the emergency brake. After a detailed investigation, it was determined that a malfunctioning train was emitting a wireless signal that interfered with nearby trains' connectivity [22, 5].

Based on those incidents, a safety and security co-analysis method needs to be able to model complex system interactions, potentially including multiple instances of the same subsystem (e.g., train) within a larger environment and operational context. At the same time, safety engineers today need to consider both physical hazards and acts of tampering (e.g., oil on the track) as well as cyber threats (e.g., tampering with a train to jam nearby trains). In the case study below we aim to illustrate how the STLSA analysis method can help systems engineers confront these risk assessment challenges.

4.1 System description

Rolling stock are equipped with both electrical brakes and frictional brakes. Figure 5 shows a typical train with three cars, and overlays the key components of both braking systems. These components and their main functions are:

- ATC: Automatic Train Control. Pre-programmed to initiate service braking.
- BCE: Braking control electronics. Generally in charge of electrical braking and frictional braking at appropriate time.
- BCU: Braking control unit. Activates frictional brake via pneumatic control.
- PCE: Power control electronics. To activate electrical braking.
- EBK/EBR: Emergency brake contractor/Emergency brake relay. De-energized to activate emergency braking.
- Bogie: undercarriage with train wheels

Under normal circumstances of service braking, electrical brake is activated in the early phase, then BCUs activate the frictional brake at mid speed to compensate for the decrease in electric braking effort. This control constraint aims to ensure a smooth braking process and it's known as a blending request. When the train speed decreases to below 3km/hr, full frictional brake would be applied regardless of the receptivity of the traction power system.

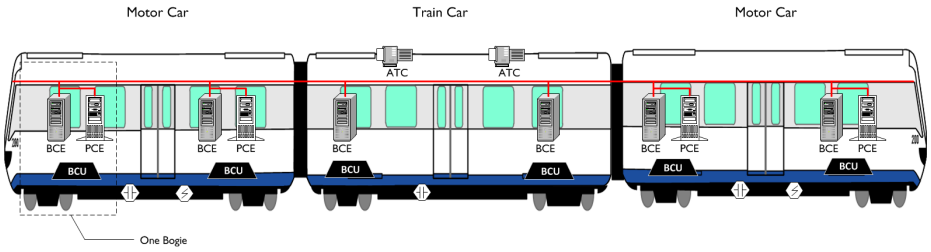

Fig. 5. Topology of the train brake system

Electrical braking is applied for energy saving purpose, since this process boosts power regeneration that kinetic energy of the train converts into electrical energy. In fact, the failure of conducting electrical braking does not have impact to train operation, since the braking force from electrical brake could be fully compensated by frictional braking. However, if frictional brake fails to be conducted properly, train operation will be affected. To specify, a single frictional brake failure of one bogie will not cause the train to stop immediately, and if it is a minor fault, no effects will be exposed to train normal operation, while major fault may affect the train's status, such as overrun.

Unlike normal braking, emergency brake is controlled by a different loop across the trainline, which is called the emergency brake loop. When the emergency brake loop is interrupted (e.g., by a passenger pressing the emergency call button) the train will activate the emergency brake to stop immediately. In an emergency brake scenario only the frictional brake is used, and full brake force is applied. When the emergency brake loop is interrupted, EBK and EBR are de-energized in sequence, which will be sent to BCE to activate frictional brake. The following process of activation of frictional brake from BEC works in the same way as the frictional brake in normal brake.

4.2 Analysis

According to the system description, we construct the control model for the train brake management system as shown in Fig. 6. We first identify the main entities involved in the train brake scenario, including automated controllers, cyber and physical components, as well as human factors (e.g. passengers and station staff). In the hierarchical control structure shown in Fig. 6, the interactions among entities are modeled as control loops, composed of the actions or commands that a controller sends to controlled process, and the responses or feedback that the controller receives from controlled process. In every control loop, any flaws or inadequacies could possibly lead to unsafe control actions and hazardous states in the system.

In Table 2, we list several of the possible accidents related to the train brake management system. Here we focus on safety related losses and exclude other losses like financial or operational losses. Four common accidents (A1 to A4)

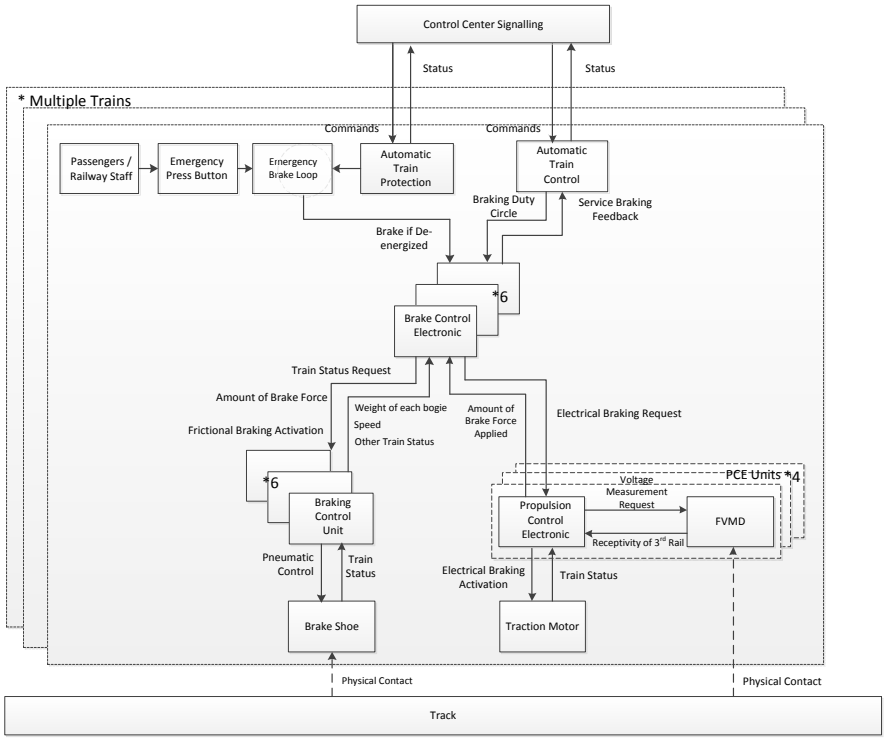

Fig. 6. Hierarchical Control Loops of a Train Brake Management System

related to the braking scenario are suggested. For example, if sequential brake processes fail to connect in an appropriate way, train's smooth operation can no more be ensured, and this may cause passengers fall down or even get injured (A1). Another accidental scenario is property damage (A2). For instance,during the regeneration phase of electrical braking, there are risks of damage to traction power system when 3rd rail voltage is too high or too low. Similarly, the couplings between cars will be compromised by excessive force if individual bogie does not brake at correct rate. Collision with objects or other trains (A3) is another major type of accident. Additionally, braking failure can cause disruption of availability as well, like the train unexpectedly stops in the middle of a tunnel, or misses the platform (A4).

According to the aforesaid braking accidents, the hazardous scenarios are identified and attached to the related accidents, as shown in Table 2. For example, in train braking phase, individual cars need to sense weight and brake with different force accordingly, since the corresponding equipment like BCE and BCU are dedicated to control the braking process for each bogie. Due to the complex interactions of their control loops, the couplings of cars could suffer

Table 2. Accidents and System Hazards in Braking Control Process

Identified Accident
A1. Train decelerates or stops in a sudden way, making passengers fall down and even get injured
A2. Related system or equipment are damaged.
A3. Collision with objects or other trains.
A4. Train stops at wrong places.
Identified Hazards and Corresponding Accidents (in parentheses)
H1. Coupling between adjacent cars is being compromised.(A2)
H2. Train is not at the right speed at certain location.(A3, A4)
H2-1. Train is overrun.
H2-2. Train is underrun.
H3. Substantial phases fail to connect smoothly.(A1)
H4. Traction power system e.g., 3rd rail, is over voltage.(A2)
H5. Procedure continues for a prolonged time (A3, A4)
H6. Train does not stop properly (A3)
H7. Braking phases are conducted with unintended timing, in an unintended amount, or at an unintended location (A3, A4)

Table 3. Example Conditions under which control actions may lead to Hazard

Type	Control Action	UCA No.	Unsafe Control Actions	Possible Hazards
Required Action Not Performed	Request electrical braking	UCA-1	Electrical braking request is not preformed by PCE in the train braking scenario	Non-hazardous
	Activate frictional braking	UCA-2	Frictional braking is not activated during the train braking phase	H1, H2-1, H5, H6
Hazardous Action Performed	Activate frictional braking	UCA-3	Inadequate braking force is performed and transmitted to downstream braking units in frictional braking phase	H1, H2-1, H5, H7
Incorrect timing or order	Activate pneumatic control	UCA-4	Pneumatic control isn't properly be applied at the mid of speed to compensate for the decrease in electrical break effort	H3, H7
Incorrect Duration	Activate electrical braking	UCA-5	Electrical braking is preformed too long, and fails to stop before traction power system has been fully regenerated.	H4

from excessive extrusion force or separating force, once there is any inadequate control in this process. This condition could be a significant hazardous scenario (H-1)leading to the damage of relevant equipment (A2), especially for the train with multiple cars.

We further investigate the contexts under which control actions could be unsafe and lead to hazardous status. As per STPA-Sec, unsafe control actions

could be categorized into four types: 1) control action not given, 2) control action given not correctly, 3) wrong timing or order of control action, 4) control action stopped too soon or applied too long. In this step, to identify unsafe control actions, all the control loops in Fig. 6 are reviewed. Due to the limitation of space, we only show one example under each type (see Table 3).

In Table 3, we highlight the unsafe control action type, the unsafe control actions which could lead to a hazard, and the possible system hazards. For example, an unsafe control action is that too little brake force is performed and transmitted to downstream brake units (UCA-3), which would lead to hazardous system status like wrong speed, compromised couplings, etc. Another example is electrical brake is applied too long and fails to properly stop in time, when the 3rd rail is fully regenerated (UCA-5), and it may cause the damage of related equipment.

Afterwards, with the help of the annotated control graph from [23, 16], we consider intentional and unintentional causal scenarios for each unsafe control action. Table 4 shows a few possible causal scenarios for UCA-3. We distinguish unintentional scenarios and intentional scenarios with the label of "U" and "I" respectively. Unintentional causal scenarios may include safety oriented factors such as possible flaws in the algorithms and models, malfunctions of related components, inadequate or evening missing feedback. While in security perspective, intentional scenarios focus on malicious attacks such as injection of manipulated data, tampered or congested feedback etc.

These scenarios should not be seen as exhaustive checklist which covers all possibilities, but a starting point for further thoughts and investigations. It is also important to note that quite a number of unsafe control actions may share similar causal scenarios, but they happen on different controller and controlled process. That means there are some common causes for unsafe and insecure scenario which calls for extra attention and efforts.

Last, we assess the likelihood of identified causal scenarios with the method suggested in Section 3. Specifically, we rate "Reachability" and "Uniqueness" according to the braking management case. The example of evaluation is shown in Table 4 (for UCA-3).

Reachability. Internal cyber components in a train brake management system are not public accessible and best described as a private network. In most of cyber attacks targeting this system, attackers need to manage the control process via a private network connection (reachability = 2).

Uniqueness. Most of train brake systems are restricted and not common for commercial or non-commercial applications (uniqueness = 1). While the process, operation and a few devices such as sensors can be assumed as commercially available (uniqueness = 2).

4.3 Discussion

As seen in the analysis above, elements from STPA-Sec and FMVEA can be combined to provide a system-level view of unsafe or insecure control actions with greater support for structured risk assessment in the form of likelihood and

Table 4. Potential Causal Scenarios and Assessment of UCA-3

ID	Potential Causal Scenarios	Type (U/I)	S	R	U	p/f score
A	Sensors or related equipment(e.g. BCE, BCU) malfunction.	U	1	-	-	5
B	Inadequate control algorithm occur to BCE calculation model, which causes the amount of breaking force is not calculated correctly.	U	2	-	-	2
C	**Unidentified disturbance such as the changes of environment(e.g. the track is oily), makes the braking force in normal circumstance not adequate any longer.**	U	3	-	-	2
D	The feedback path to BCE may be congested intentionally, then the train cannot explicitly determine the required brake force for each bogie	I	2	2	1	3
E	Manufactured braking force amount is sent by BCE to the downstream braking equipment, and that forged message overwrites the legitimate braking force.	I	3	2	1	3
F	**Maliciously tamper or fabricate readings of relevant devices (e.g. oil gauge,sensors) after creating an unsafe situation of environment.**	I	3	2	2	4

Note: Type(U/I)–Type(Unintentional scenario/Intentional scenario); S–Severity; R–Reachability; U–Uniqueness; p/f score–probability/frequency score.

severity scores grounded in standards such as EN 50126-1 for railway applications. By reconciling those perspectives on safety/security co-analysis, we arrive at a method that can be used to identify unsafe situations posed by the environment's impact on system control actions (i.e., oil on the track in Table 4) and prioritize high-risk security/safety issues (high S and p/f score) for remediation.

This work represents an initial attempt to reconcile concepts from STPA-Sec with more traditional component-based analysis methods. As such, there are a few limitations we would like to acknowledge. First, it may be possible to incorporate other methods into an STPA-Sec inspired analysis process. We chose FMVEA in this work due to its close alignment with a classical safety/reliability engineering approach used in industry (FMEA). Second, the control structure diagram in Figure 3, while more expressive than the functional control diagrams used in [23], is also more complex with the addition of multiple instances and environmental interaction. Also, as pointed out in [16], the STPA-Sec process results in a large number of control loops and causal scenarios to analyze. It is our view that these factors point to a need for tool support to assist with creating/maintaining/tracking assessment documentation. This is a topic we will explore in future work.

5 Conclusion

In this paper, we propose a new method for identifying and evaluating safety and security risks. Our Systems-Theoretic Likelihood and Severity Analysis (STLSA) method combines aspects from the systems-theoretic STPA-Sec method, which identifies unsafe/insecure control actions in a system, and component-centric FMVEA method, which is an extension of failure mode and effects analysis from IEC 60812. We illustrate the STLSA process using a railway case study.

Acknowledgements. This work was supported in part by the National Research Foundation (NRF), Prime Minister's Office, Singapore, under its National Cybersecurity R&D Programme (Award No. NRF2014NCR-NCR001-31) and administered by the National Cybersecurity R&D Directorate. It was also supported in part by the research grant for the Human-Centered Cyber-physical Systems Programme at the Advanced Digital Sciences Center from Singapore's Agency for Science, Technology and Research (A*STAR).

References

1. IEC 60812: Analysis techniques for system reliability ? procedure for failure mode and effects analysis (FMEA).
2. First mrt accident. http://eresources.nlb.gov.sg/infopedia/articles/SIP_814_2004-12-31.html, 2004.
3. BS EN 50126-1. *Railway applications-The Specification and Demonstration Reliability, Availability, Maintainability and Safety (RAMS). Part 1: Basic Requirements and Generic Process*, 2015.
4. S. Chockalingam, D. Hadziosmanovic, W. Pieters, A. Teixeira, and P. van Gelder. Integrated safety and security risk assessment methods: A survey of key characteristics and applications. In *CRITIS*, 2016.
5. Defence Science and Technology Agency blog. How we caught the circle line rogue train with data. https://blog.data.gov.sg/how-we-caught-the-circle-line-rogue-train-with-data-79405c86ab6a#.4fu3jqint, 2016.
6. I. N. Fovino, M. Masera, and A. De Cian. Integrating cyber attacks within fault trees. *Reliability Engineering & System Safety*, 94(9):1394–1402, 2009.
7. I. Friedberg, K. McLaughlin, P. Smith, D. Laverty, and S. Sezer. STPA-SafeSec: Safety and security analysis for cyber-physical systems. *Journal of Information Security and Applications*, 2016.
8. O. Henniger, L. Apvrille, A. Fuchs, Y. Roudier, A. Ruddle, and B. Weyl. Security requirements for automotive on-board networks. In *Intelligent Transport Systems Telecommunications,(ITST), 2009 9th International Conference on*, pages 641–646. IEEE, 2009.
9. S. Kriaa, L. Pietre-Cambacedes, M. Bouissou, and Y. Halgand. A survey of approaches combining safety and security for industrial control systems. *Reliability Engineering & System Safety*, 139:156 – 178, 2015.
10. G. Macher, A. Höller, H. Sporer, E. Armengaud, and C. Kreiner. A combined safety-hazards and security-threat analysis method for automotive systems. In *SAFECOMP*, pages 237–250. Springer, 2015.

11. F. Massacci and F. Paci. How to select a security requirements method? a comparative study with students and practitioners. *Secure IT Systems*, pages 89–104, 2012.
12. L. Piètre-Cambacédès and M. Bouissou. Cross-fertilization between safety and security engineering. *Reliability Engineering & System Safety*, 110:110–126, 2013.
13. C. Raspotnig, P. Karpati, and V. Katta. A combined process for elicitation and analysis of safety and security requirements. In *Lecture Notes in Business Information Processing*. Springer, 2012.
14. G. Sabaliauskaite and A. P. Mathur. Aligning cyber-physical system safety and security. In *Complex Systems Design & Management Asia*. Springer, 2015.
15. C. Schmittner, T. Gruber, P. Puschner, and E. Schoitsch. Security application of failure mode and effect analysis (FMEA). In *SAFECOMP*, pages 310–325. Springer, 2014.
16. C. Schmittner, Z. Ma, and P. Puschner. Limitation and improvement of STPA-Sec for safety and security co-analysis. In *SAFECOMP*, pages 195–209. Springer, 2016.
17. C. Schmittner, Z. Ma, E. Schoitsch, and T. Gruber. A case study of fmvea and chassis as safety and security co-analysis method for automotive cyber-physical systems. In *ACM Workshop on Cyber-Physical System Security*, pages 69–80. ACM, 2015.
18. C. Schmittner, Z. Ma, and P. Smith. Fmvea for safety and security analysis of intelligent and cooperative vehicles. In *ISSE Workshop*, pages 282–288. Springer, 2014.
19. A. Shostack, S. Lambert, T. Ostwald, and S. Hernan. Uncover security design flaws using the STRIDE approach. MSDN Magazine, 2006.
20. W. G. Temple, W. Y., B. Chen, and Z. Kalbarczyk. Reconciling systems-theoretic and component-centric methods for safety and security co-analysis. In *Proc. of the 5th International Workshop on Assurance Cases for Software-Intensive Systems (ASSURE'17)*, 2017.
21. The Straits Times. Oil spillage led to mrt train collision: Panel. http://eresources.nlb.gov.sg/newspapers/Digitised/Article/straitstimes19931020-1.2.2, 1993.
22. The Straits Times. Train's faulty signals behind circle line woes. http://www.straitstimes.com/singapore/transport/trains-faulty-signals-behind-circle-line-woes, 2016.
23. W. Young and N. Leveson. Systems thinking for safety and security. In *ACSAC*, pages 1–8. ACM, 2013.