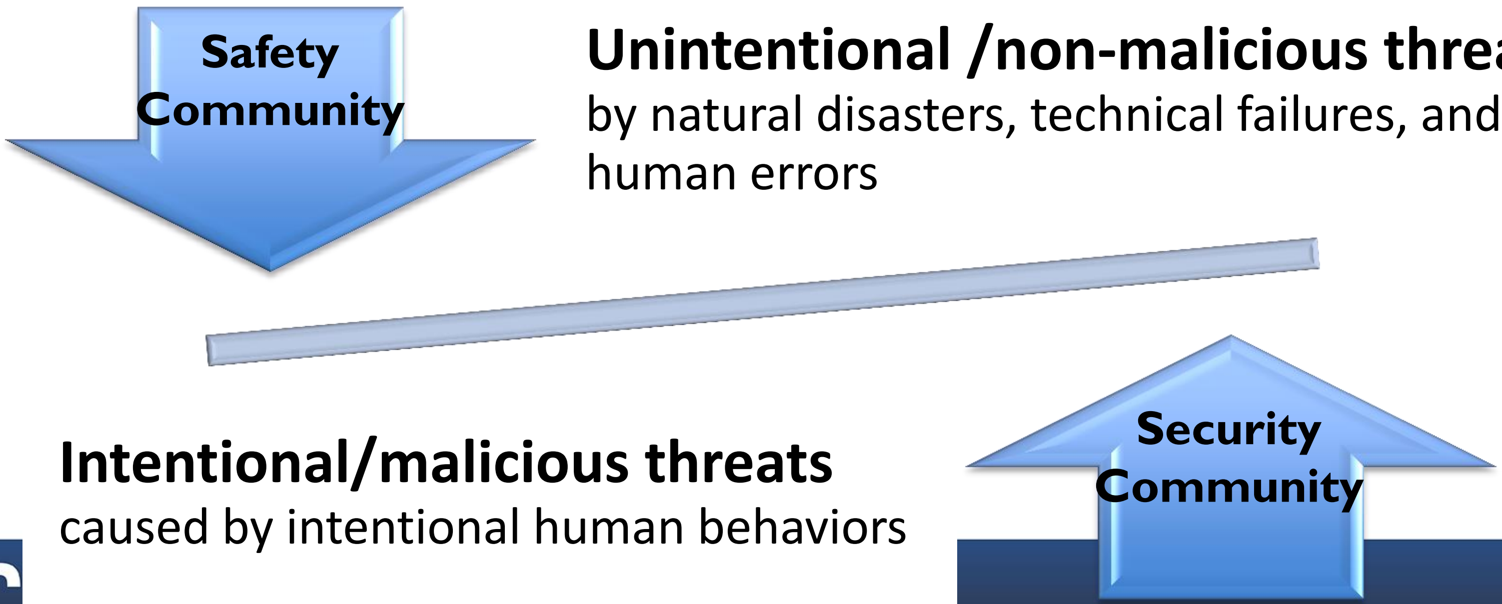
International Conference on Reliability, Safety and Security of Railway Systems: Modelling, Analysis, Verification and Certification
RSSR 2017

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

William G. Temple — Advanced Digital Science Center
Yue Wu — Advanced Digital Science Center
Binbin Chen — Advanced Digital Science Center
Zbigniew Kalbarczyk — University of Illinois at Urbana-Champaign

Safety and Security

- Safety and Security
  - Represented by separated communities in both industry and academia
  - Issues have been considered separately during the system design



Safety and Security Co-Engineering

- Information technologies and communication devices are increasingly being integrated into modern control systems
  - Easily discovered once connected to the Internet
  - Vulnerable to cyber attack, causing physical impacts
- Security vulnerabilities exploited to compromise the safety critical systems, leading to financial losses and in some cases, human injures or death
- Usually, it is a matter of time before security flaws are discovered and exploited even in well engineered critical systems

Example: Automated Metro Train

An incident with Singapore MRT

- 2016 Singapore
- Circle Line Metro
- Intermittent emergency brake
- Several different trains
- Over the course of more than **1 week** (From 26th Aug to 02nd Sep)

Example: Automated Metro Train

- An intermittent failure of the signalling hardware on a single train
  - The cause for the loss of signalling communications of other trains on Circle Metro Line
  - The safety feature, emergency brake, being automatically activated

Example: Automated Metro Train

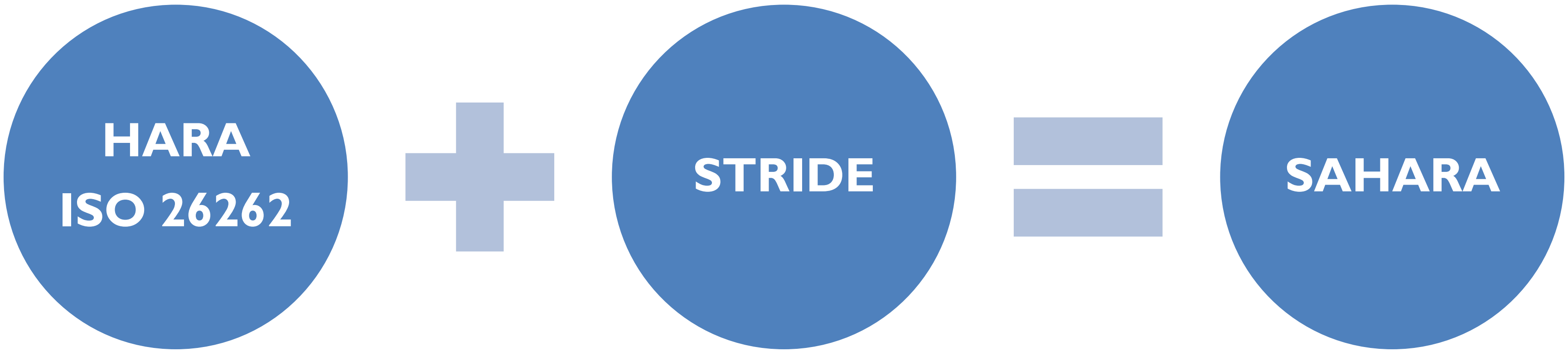
Could such an event be replicated maliciously?

Exploit Safety Features (e.g., Emergency Braking) to cause large-scale service disruptions

Safety and Security Co-Engineering

- Therefore, it is becoming increasingly important to address the combination of safety and security in modern control systems.
- A transformation among safety and security communities to work together especially in risk assessment
- A growing body of work relating to safety and security co-analysis methods

Safety and Security Co-Engineering Method (SAHARA)



ISO 26262- Hazard Analysis and Risk Assessment (HARA)

- Used in a conventional manner to classify the safety hazards according to the Automotive Safety Integrity Level (ASIL)

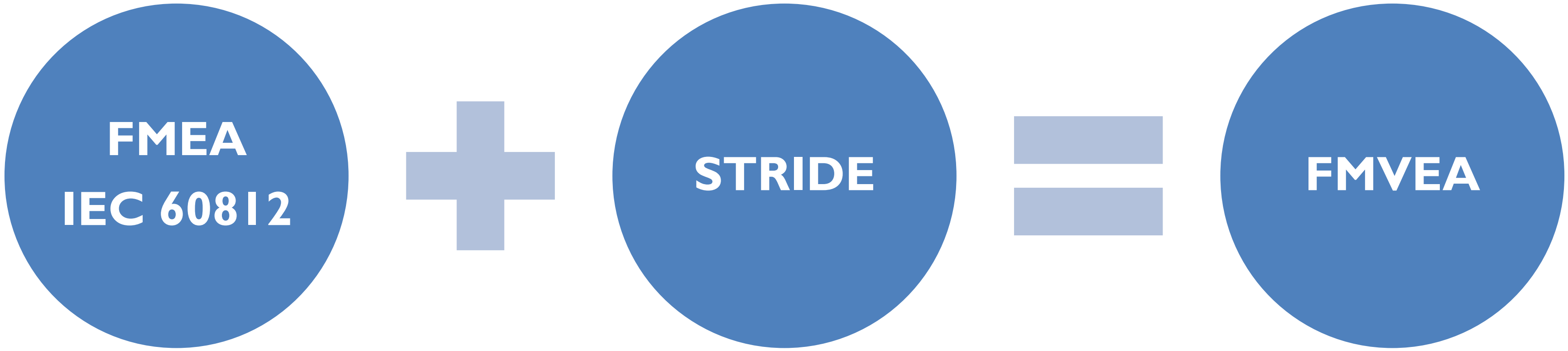
STRIDE method

- Used to model the attack vectors of the system

Security Aware Hazard Analysis and Risk Assessment (SAHARA)

- Security threats that may violate the safety goals are considered for the further safety analysis

Safety and Security Co-Engineering Method (FMVEA)



Integration through the combination of a conventional ***safety risk assessment method*** and a **variation** of the conventional safety risk assessment method (incorporating threat information based on the STRIDE model) for security risk assessment

Safety and Security Co-Engineering Method (FACT Graph)

Fault Tree + Attack Tree = FACT Graph

Integration through the combination of a conventional **safety *risk assessment method*** and a conventional **security *risk assessment method***

Analysis Methods for co-engineering

- Traditional component-centric methods
  - Design-stage risk assessment
  - E.g., fault/attack tree, failure mode and effect analysis (FMEA/FMVEA)
  - Challenging to deal with complex interactions among safety critical systems
- System-Theoretic Process Analysis for Security approach (STPA-Sec)
  - Emphasis on control loop, emergent system behavior
  - Limitations: not provide guidance on how to address the identified scenarios

Our Approach Overview

- A new hybrid method, Systems-Theoretic Likelihood and Severity Analysis (STLSA)
  – Top-down view of functional control structure of a system
  – Threat and failure scenarios with a semi-quantitative risk rating system
- Contributions
  – Leverage advantages of STPA-Sec (System-centric method) and FMVEA (Component-centric method)
  – A case study applying our proposed method, STLSA on a realistic train braking system

Original Methods – STPA-Sec

- STPA-Sec
  - Extension of the System-Theoretic Process Analysis (STPA) from safety community
  - Derived from the System-Theoretic Accident Modeling Process (STAMP)
  - Motivation
    - Considering 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 its ***functional control*** structure
      - Rather than focusing on threats and attacker properties such as intent and capability

Original Methods – STPA-Sec

- Delivery
  - A list of control actions in the system that may be unsafe/insecure
  - How those control actions may lead to unacceptable losses in one or more causal scenarios
- Gap
  - Not evaluate the relative likelihood or severity of impact for those causal scenarios
  - Not fully aligned with current safety/security standards

Original Methods – FMVEA

- FMVEA
  - Extension of the widely-used FMEA (Failure Mode and Effect Analysis)
  - Security related information, i.e., vulnerabilities, threat modes, and threat effects
- FMVEA Process

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

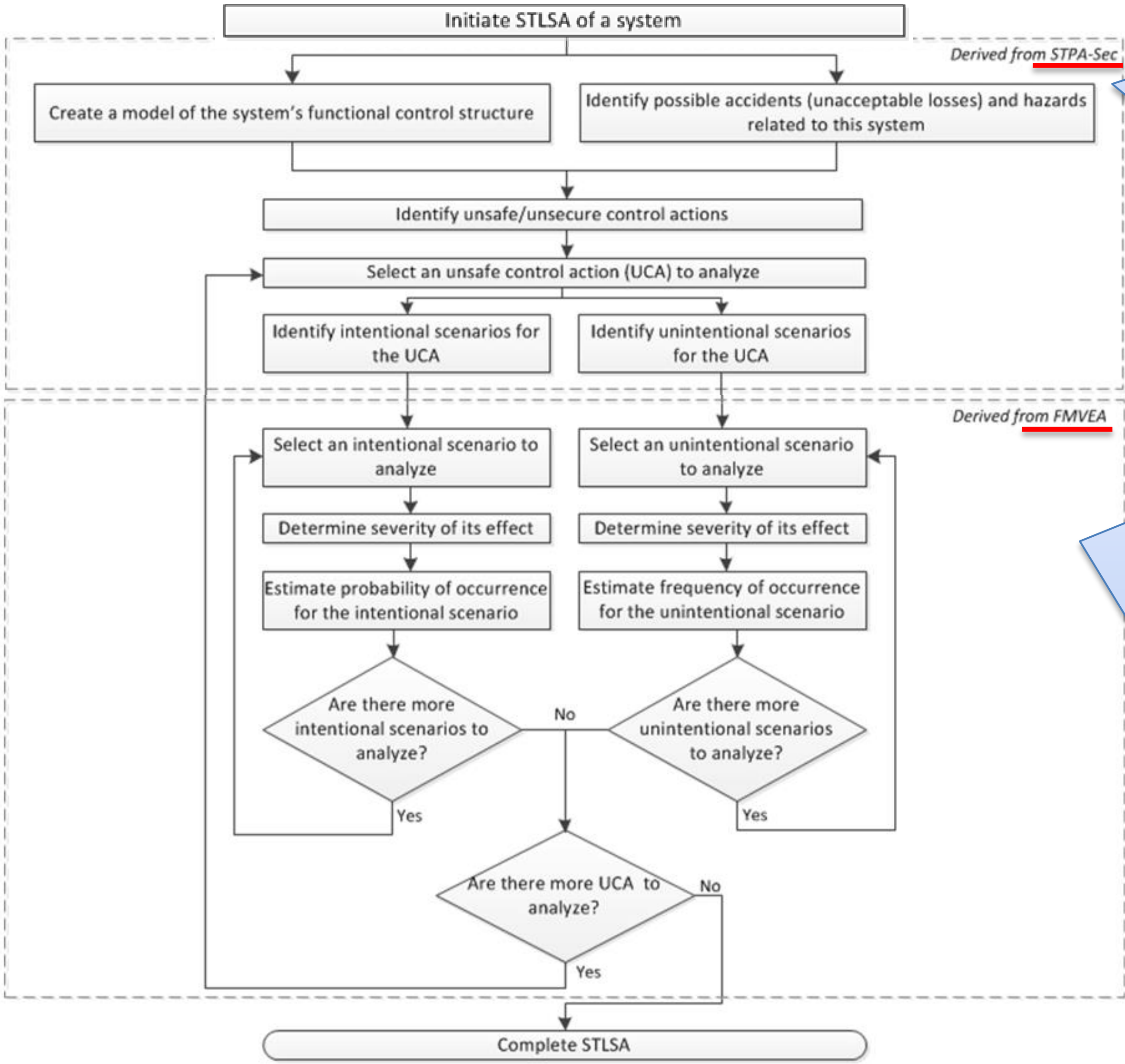
Original Methods – FMVEA

- Component-centric analysis method
  - Based on component failure
- Challenges
  - Scalability: For large systems, it's not sufficient to consider lower level failures and threats (especially those with complex interactions or emergent behaviour)
  - Multiple failures: It's far more plausible in a deliberate attack
  - System effect is not made explicit

STLSA Combination

- Combine desirable characteristics
  - Component-centric approach
  - System-centric approach
- Systems-Theoretic Likelihood and Severity Analysis (STLSA)

A Hybrid Method of STLSA



The high level (functional) control models as well as the guide words and phrases

An familiar rating process for evaluating the risk of causal scenarios

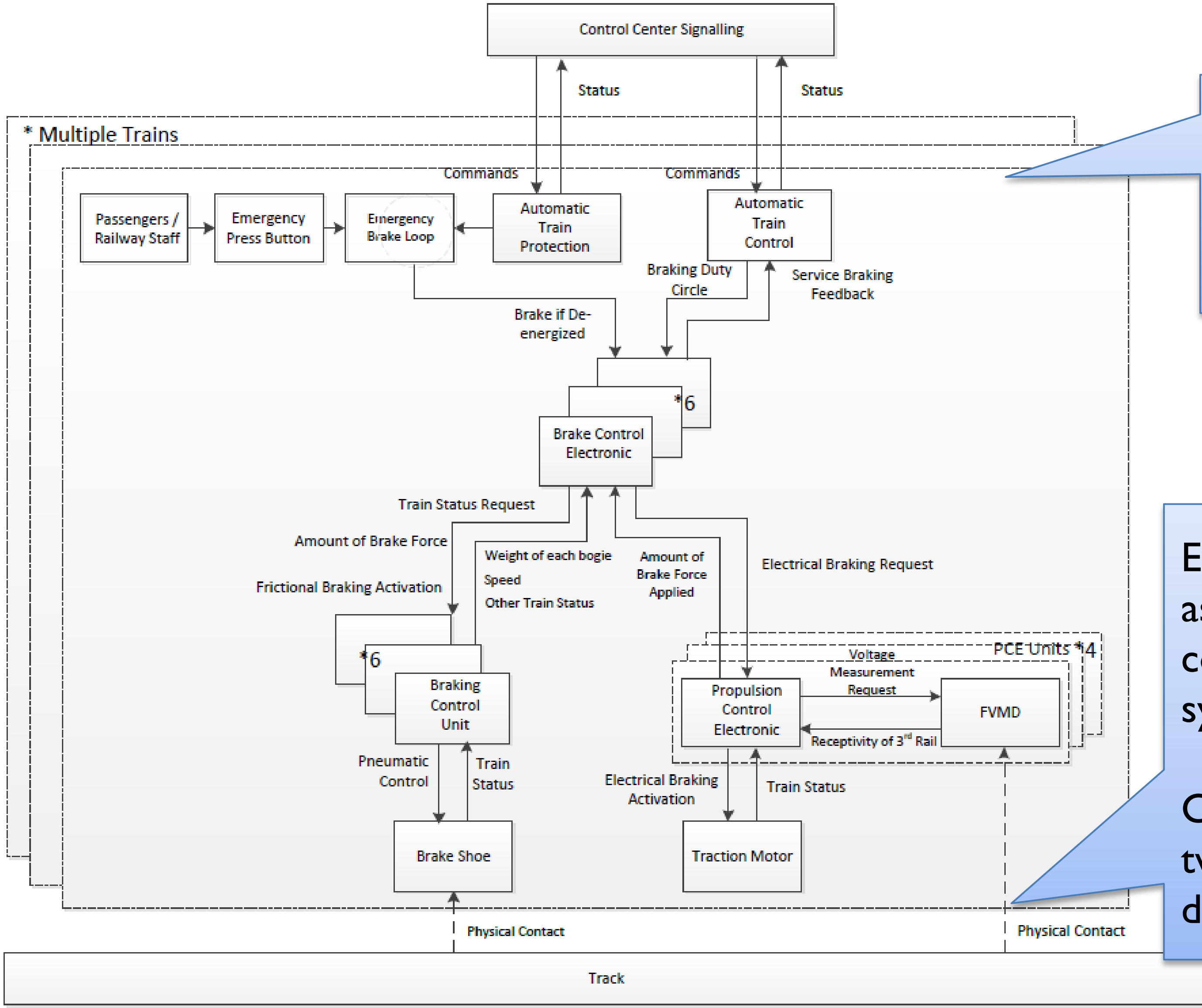
- Product of a scenario's severity and the likelihood of occurrence
- Rating scales from existing railway standards
- Other industries (e.g., aviation) may have alternate rating systems that are already familiar to practitioners, and that could be applied within STLSA

STLSA Process

- Start with an STPA-Sec analysis
- With a number of ways in which several aspects are enhanced to better address complex interactions.
- More details are shown in the context of our case study
  - Functional control structure
    - System
    - Environment
  - Multiple instances of actors & components in the system.
  - Extended guide word analysis for intentional scenarios

ADSC
ADVANCED DIGITAL SCIENCES CENTER

Case Study- Control Model



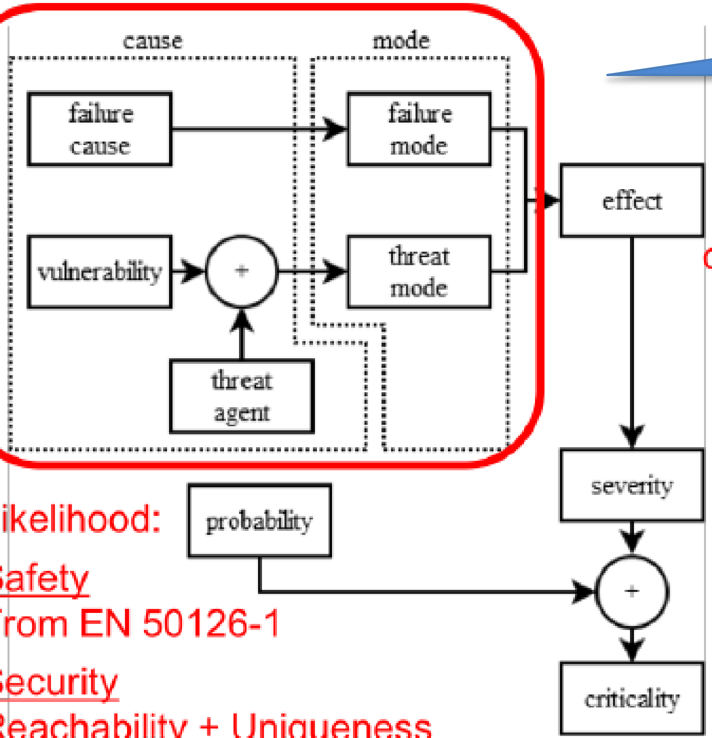
Multiple instances of actors & components in the system

Explicitly indicates which aspects of the functional control structure are in the system/in the environment.

Connections between the two are indicated with dashed edges.

STLSA-Rating System

From STPA-Sec process



Likelihood:

Safety
From EN 50126-1

Security
Reachability + Uniqueness

Inferred by functional control structure

From EN 50126-1

Interface
- Failure mode in FMVEA
- A causal scenario for an unsafe/insecure control action

- A failure mode has an effect
- An effect has a severity associated with it
- Effect : from the functional control structure

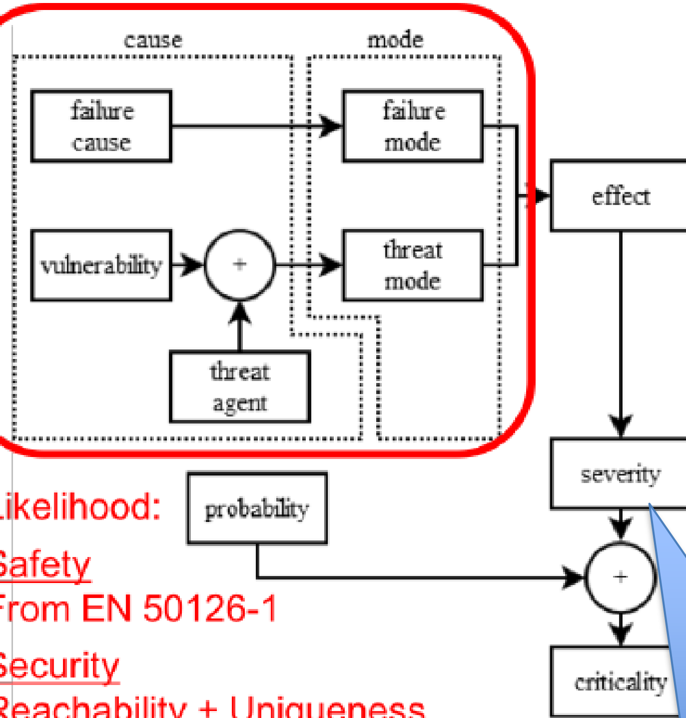
Severity: assigned a rating
- Railway safety standard EN 50126-1
- 4 levels: 1(Insignificant) to 4 (Catastrophic)

STLSA-Rating System

Safety
- Frequency score
- Suggested in EN 50126-1
- 6-tier, ranging from highly improbable (1) to frequent (6)

Security [1]
- System susceptibility
  How easy it is for a potential adversary to connect to and acquire knowledge about the system

From STPA-Sec process



Inferred by functional control structure

From EN 50126-1

Likelihood:

Safety
From EN 50126-1

Security
Reachability + Uniqueness

0 = no network
1 = temporary connected private network
2 = normal private network,
3 = public network

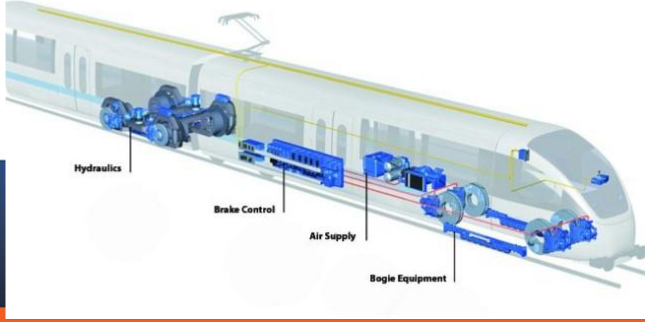
1 = restricted
2 = commercially available
3 = standard

Common between failure (safety) and threat (security) modes

[1] 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.

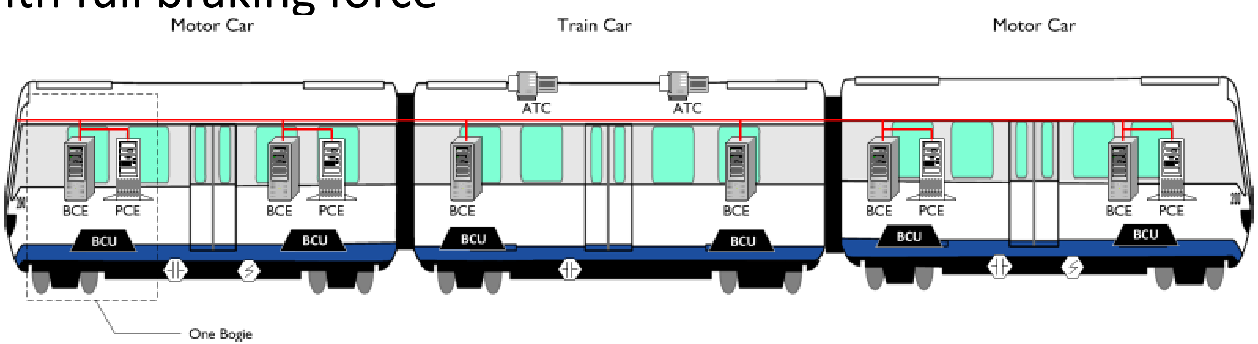
Case Study – Train Braking System

- Train Braking System Overview
  - Most safety-critical subsystem
    - Service and emergency braking processes
  - Multiple process of activating/controlling various braking actions, shared components
  - Complex safety and security challenges inherent in this system
    - *Incident 1: Oil leakage on the track*
    - *Incident 2: Signalling interference from a nearby train*



Case Study- System Description

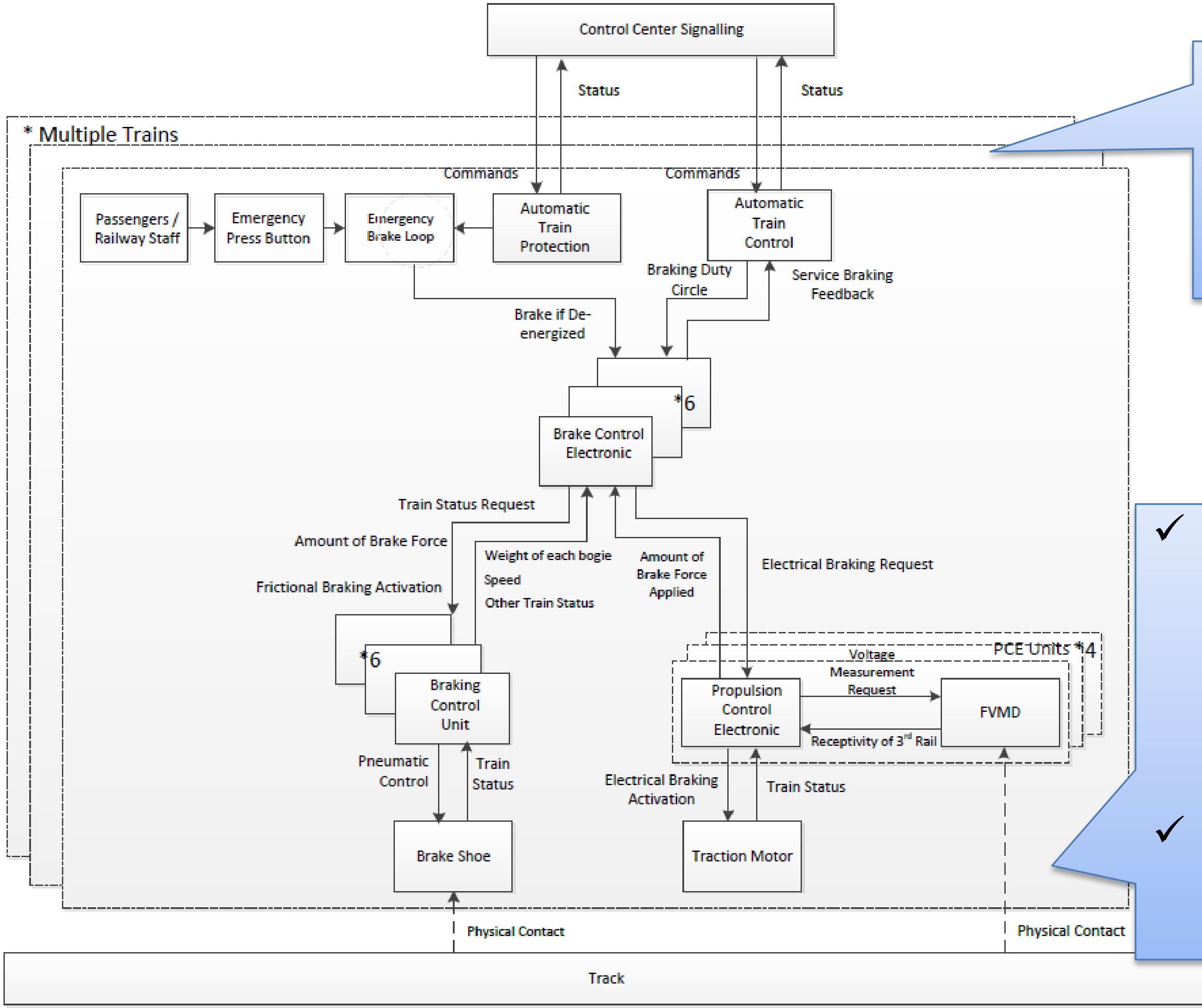
- A typical train
  - Three cars
  - Overlays the key components of braking system
- Service braking
  - Electrical braking
    - Activated in early phase
    - Energy saving purpose, No impact to train operation, fully compensated by frictional braking
  - Frictional braking
    - Activated at mid speed
    - Train operation will be affected if frictional braking fails to be conducted properly
- Emergency braking
  - Emergency braking loop
  - Frictional brake with full braking force



Case Study- Control Model

- Identify main entities
  - Automated controllers
  - Cyber and physical components
  - Human factors
- Control loops
  - Interactions among entities
  - Controllers -> Controlled process: actions/commands
  - Controllers <- Controlled process: feedback/responses
  - Flaws/inadequacies in control loops could possibly lead to unsafe control actions and hazardous states

Case Study-Hierarchical Control Structure



- ✓ Multiple instances of actors & components in the system

- ✓ Explicitly indicates which aspects of the functional control structure are in the system/in the environment.

- ✓ Connections between the two are indicated with dashed edges.

Case Study- Accidents Identification

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.

- Safety related losses
  - Exclude other losses, e.g., financial/operational
- Examples
  - **A1: sequential brake processes fail to connect in an appropriate way → train's smooth operation can no more be ensured**
  - A2: Regeneration phase of electrical braking → 3rd rail voltage is too high or too low → Damage to traction power system
  - A3: Collision with objects or other trains
  - A4: Stop in the middle of a tunnel/Miss the platform

Case Study-Hazards Identification

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)

- Example
  - Individual cars sense weight → brake with different force accordingly
  - Corresponding equipment (e.g., BCE, BCU) are dedicated to control the braking process for each bogie
  - Couplings of cars could suffer from excessive extrusion force or separating force
  - Inadequate control in this process (H1) leads to the damage of relevant equipment (A2)

Case Study-Unsafe Control Actions

Unsafe Control Actions

Contexts under which control actions could be unsafe and lead to hazardous status

All the control loops in hierarchical control structure are reviewed

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

4 types of UCA (STPA-Sec)

Case Study – Intentional/Unintentional Causal Scenarios

A few possible causal scenarios for UCA-3

"U": Unintentional scenarios
"I " Intentional scenarios

Assess the severity and likelihood of causal scenarios (Section 3)

Rate "R" and "U" according to train brake management case

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.

Exhaustive checklists → A starting point

Common causes calls for extra attention and efforts

Reachability
- Internal cyber components
- Not public accessible
- Private network

Uniqueness
- Most - Restricted
- Process/operations/Sensors – commercially available

Discussion

- Reconciling perspectives from STPA-Sec and FMVEA
  - A system-level view of unsafe and insecure control actions
  - Greater support for structured risk assessment
  - Grounded in standards such as EN 50126-1 for railway applications
- Safety and Security in the system development lifecycle
  - Ideally starting from beginning (design phase)
  - Operation phase (e.g., our project with Singapore railway operator)
    - System upgrade and improvement
    - System audit

Conclusion

- A new hybrid method STLSA
  - Identify and evaluate safety/security risks
    - Unsafe situations posed by the environment's impact on system control actions, e.g., oil on the track
  - Prioritize high-risk issues for remediation
    - High S and p/f score
- Tool Support
  - A large number of control loops and causal scenarios
  - Assist with creating/maintaining/tracking assessment documentation
- On-going work
  - New plugin in XSTAMPP, an open-source platform for safety engineering designed
  - Support a more comprehensive safety and security co-engineering process as proposed in STLSA

Key Reference

- The SMRT incident, e.g., https://smrt.com.sg/News-Room/Announcements-News-Releases/News-Detail/articleid/908/parentId/212/year/2016?category=News
- Young, W., & Leveson, N. (2013, December). Systems thinking for safety and security. In *Proceedings of the 29th Annual Computer Security Applications Conference* (pp. 1-8). ACM.
- Macher, G., Höller, A., Sporer, H., Armengaud, E., & Kreiner, C. (2015, September). A combined safety-hazards and security-threat analysis method for automotive systems. In *International Conference on Computer Safety, Reliability, and Security* (pp. 237-250). Springer, Cham.
- Sabaliauskaite, G., & Mathur, A. P. (2015). Aligning cyber-physical system safety and security. In *Complex Systems Design & Management Asia* (pp. 41-53). Springer, Cham.
- Schmittner, C., Gruber, T., Puschner, P., & Schoitsch, E. (2014, September). Security application of failure mode and effect analysis (FMEA). In *International Conference on Computer Safety, Reliability, and Security* (pp. 310-325). Springer, Cham.
- Temple, W. G., Wu, Y., Chen, B., & Kalbarczyk, Z. (2017, September). Reconciling systems-theoretic and component-centric methods for safety and security co-analysis. In *International Conference on Computer Safety, Reliability, and Security* (pp. 87-93). Springer, Cham.

Thank You!

Yue WU
wu.yue@adsc.com.sg