Integrating Arcadia-Capella MBSE along STPA for Early-Stage Safety Analysis in Railway Systems"

Early Safety Analysis for Critical Rail Systems

Agenda

INTRODUCTIONS

PROBLEM STATEMENT & OBJECTIVE

THE METHOD : MODEL BASED SYSTEMS ENGINEERING AND STPA

VALUE PROPOSITION & CONCLUSION

REFERENCES

Introduction

Ketaki Patwardhan

MBSE Lead-Automotive , Bluekei Solutions Pvt. Ltd.

Mtech Bits Pilani : Embedded Systems Design

E-mail: ketakipatwarthan@blue-kei.com

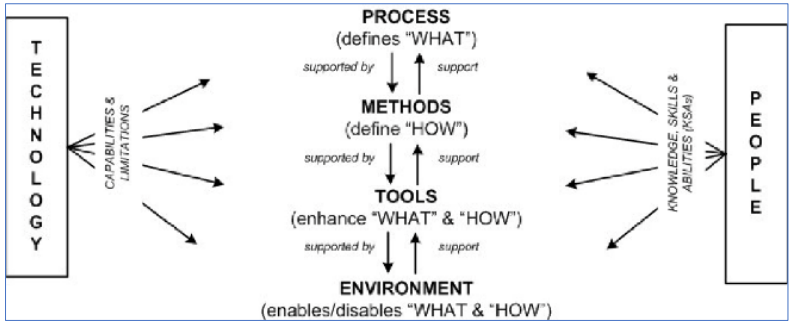
Digital Engineering with BlueKei Solutions

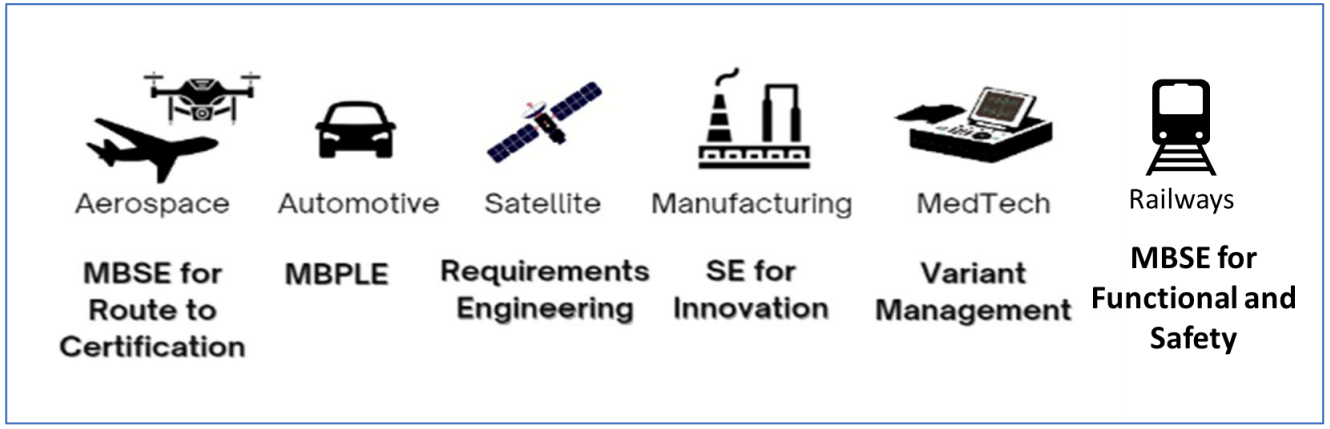
- ✓ **To** empower decision makers in transforming businesses digitally
- ✓ **By** helping to manage cost & schedule and efficiently develop systems,
- ✓ **Using** scientific SE methods and systemic approaches
- ✓ **While** maintaining design integrity and minimal rework.

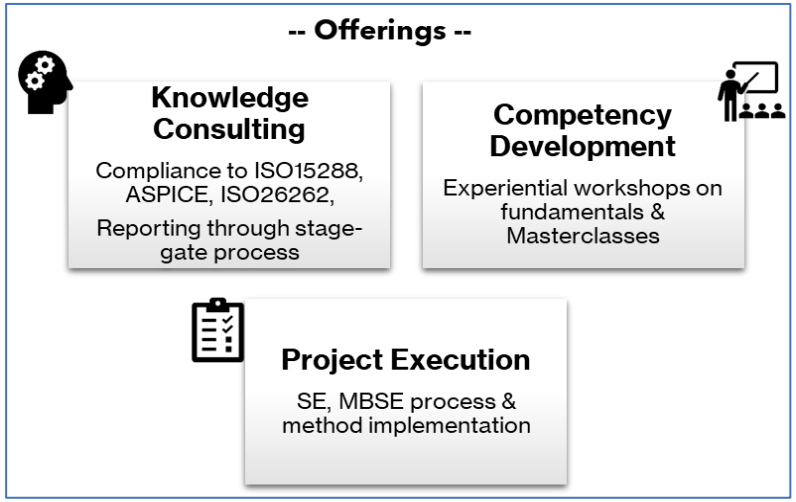
15+
Fortune 500 Companies Served

25+
Industry Experts

85%
Repeat Customers





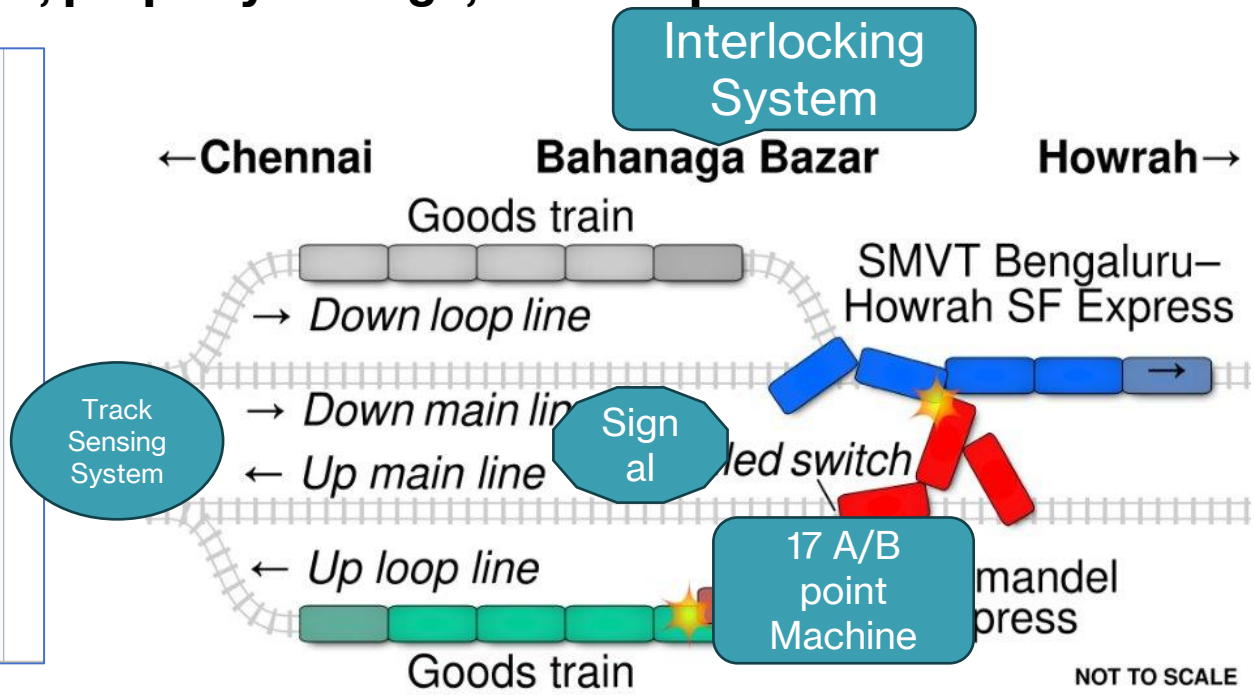


Problem Statement

Over the last five years alone, we've witnessed:

- **Over 350 precious lives lost and nearly 1,000+ serious injuries.**
- A staggering **₹300+ crore in operational losses, property damage, and compensation.**

Date	2 June 2023 around 19:00 IST (13:30 UTC)[1]
Location	Near Bahanaga Bazar railway station, Balasore, Odisha
Coordinates	21°20′17″N 86°45′52″E
Country	India
Line	Howrah–Chennai main line
Operator	South Eastern Railway zone
Owner	Indian Railways
Incident type	Collision, Derailment
Cause	Electronic interlocking defect due to signalling error[2][3]
Statistics	
Trains	3 trains • A goods train carrying iron ore • 12841 Coromandel SF Express between Shalimar and Chennai Central • 12864 SMVT Bengaluru–Howrah SF Express between SMVT Bengaluru and Howrah
Vehicles	Locomotive-WAP-7



https://en.wikipedia.org/wiki/2023_Odisha_train_collision#:~:text=On%202%20June%202023%2C%20the,near%20Bahanaga%20Bazar%20railway%20station.

Objective

- To: Deliver a safe and reliable Interlocking System
- By: Implementing MBSE Arcadia Approach
- Using: Safety assessment like STPA
- While: Continuously iterating Unsafe Control Actions for Human in loop Errors and Interlocking faults at logical layer

MBSE Arcadia Workflow

Capella
Open Source MBSE Solution

A field proven comprehensible and extensible MBSE tool to design better system architectures

ARCADIA — Methodology & high level concepts & view points

Purpose-built to provide the notation, diagrams to fit the arcadia approach

*Method & a Tool ! → aligns with the **ISO IEC IEEE 15288** Technical processes*

Perspective	Objective
Operational Analysis	What the stakeholders need to accomplish
System need analysis	What the system has to accomplish for the stakeholders
Conceptual architecture	How the system will work to fulfill expectations
End-product breakdown structure	How the system will be developed and built

Operational Analysis

Define Stakeholder Needs and Environment

Capture and consolidate operational needs from stakeholders
Define what the users of the system have to accomplish
Identify entities, actors, roles, activities, concepts

System Analysis

Formalize System Requirements

Identify the boundary of the system, consolidate requirements
Define what the system has to accomplish for the users
Model functional dataflows and dynamic behaviour

STPA Analysis

Develop Safety Requirements

Identify losses and hazards, define control structure
Identify unsafe control actions and loss scenarios
Specify mitigation constraints and requirements

Logical Architecture

Develop System Logical Architecture

See the system as a white box
Define how the system will work so as to fulfill expectations
Perform a first trade-off analysis

Physical Architecture

Develop System Physical Architecture

How the system will be developed and built
Software vs. hardware allocation, specification of interfaces, deployment configurations, trade-off analysis

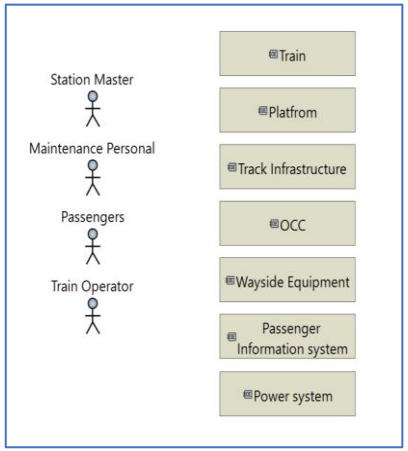
EPBS

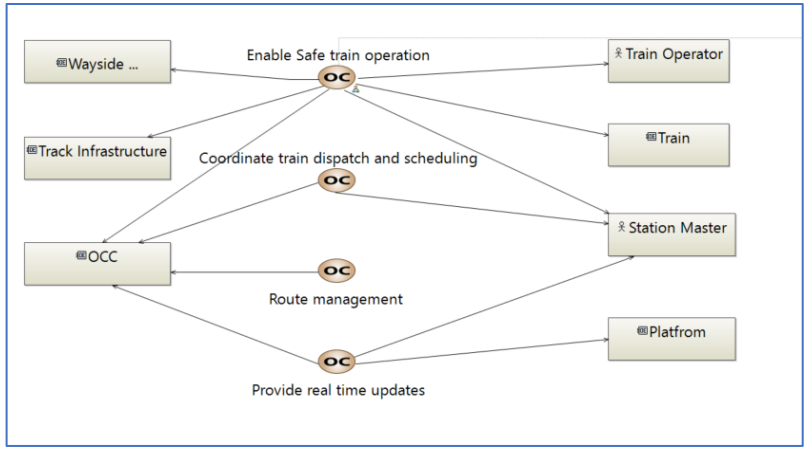
Formalize Component Requirements

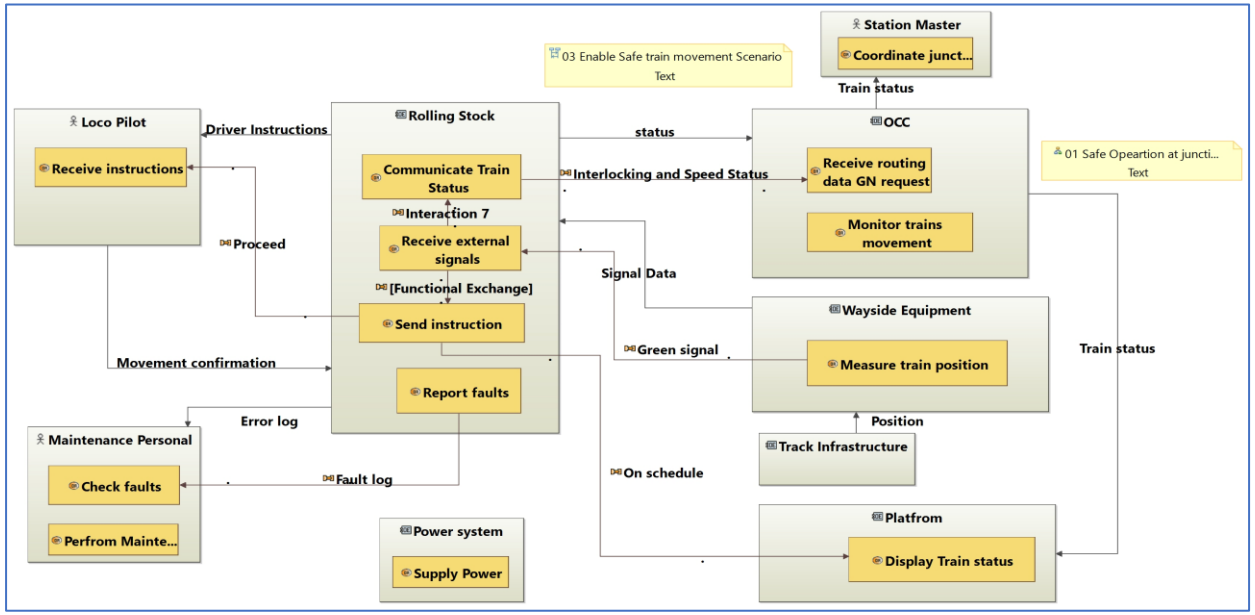
Manage industrial criteria and integration strategy: what is expected from each designer/sub-contractor
Specify requirements and interfaces of all configuration items

Operational Analysis (OA)

- Identify the stakeholders as entities and actors
- Identify /Define the Operational Capabilities (OC) (i.e What the Needs)
- Trace OC to Entities/Actors
- Define High Level Activities-Primary Activities
- Group the Activities under Scenarios

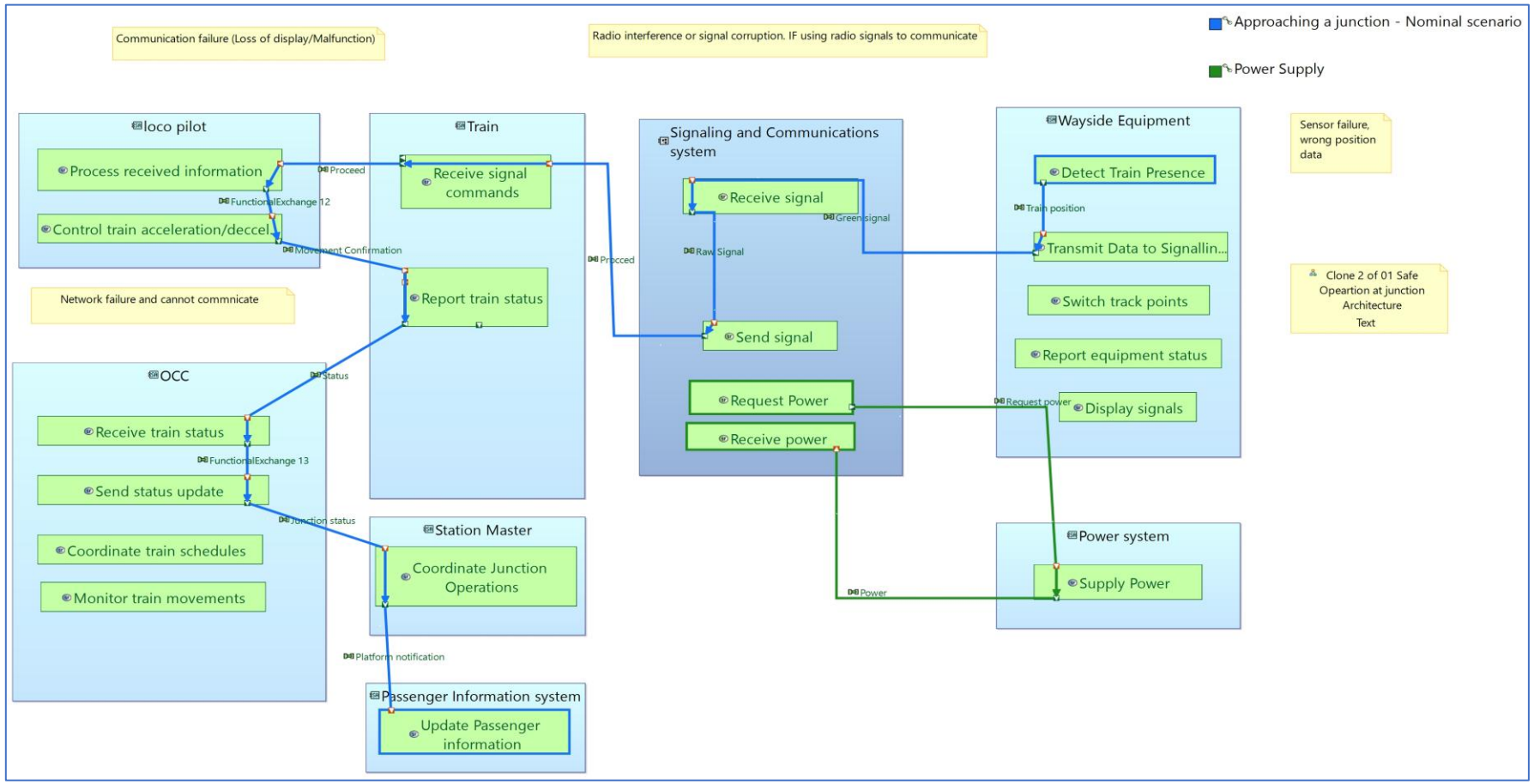




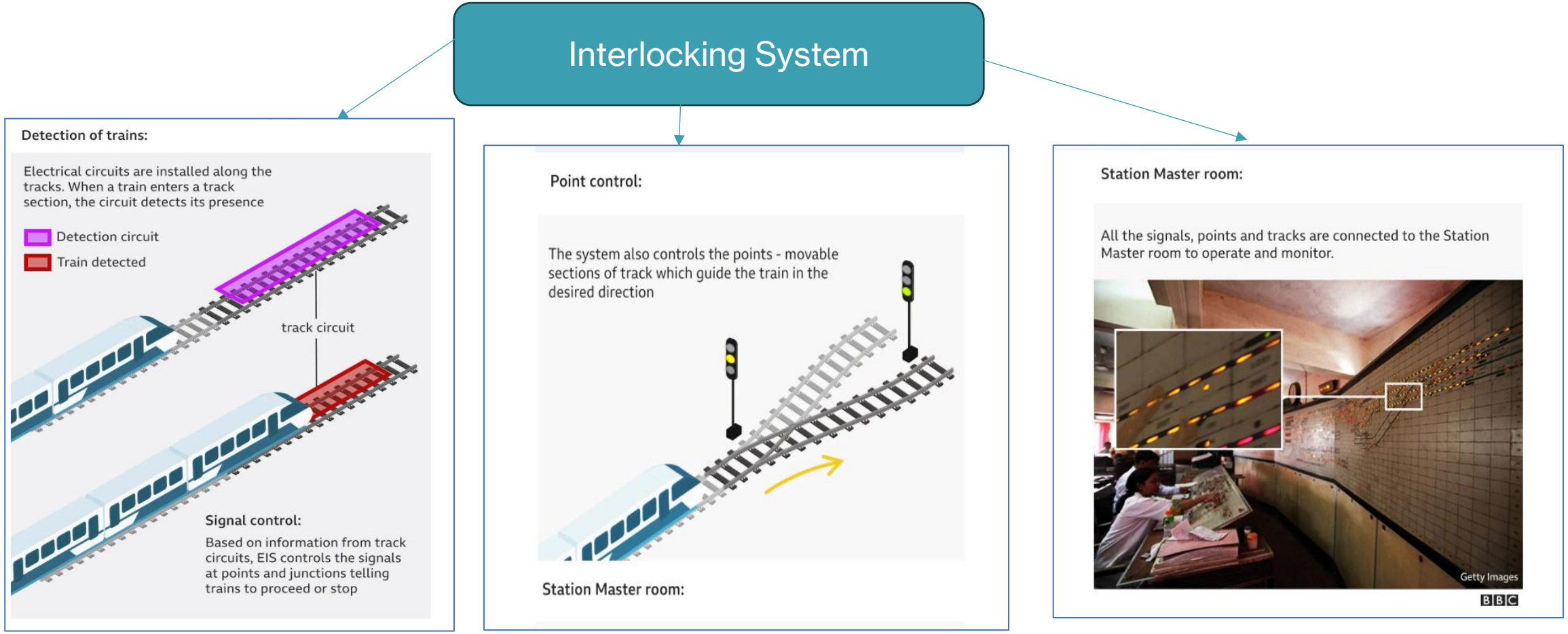


System Analysis (SA)

- Add functions and functional exchanges expanding the usecase of **OA/SA**
- Built **Functional chains** describing the scenario



Interlocking System



Logical Architecture

Operational Analysis
System Analysis
Logical Architecture
Physical Architecture
EPBS

LA

How the system will be designed to fulfill the user expectations

Data Exchanges across

logical components involved

Component exchanges

Function exchanges

Some Logical functions

Route Checking

Track verification

Lock Route

How will it work for user?

Some Function Exchanges

Vacant Route Signal

Visual Green Alert

Some Logical components

Interlocking System

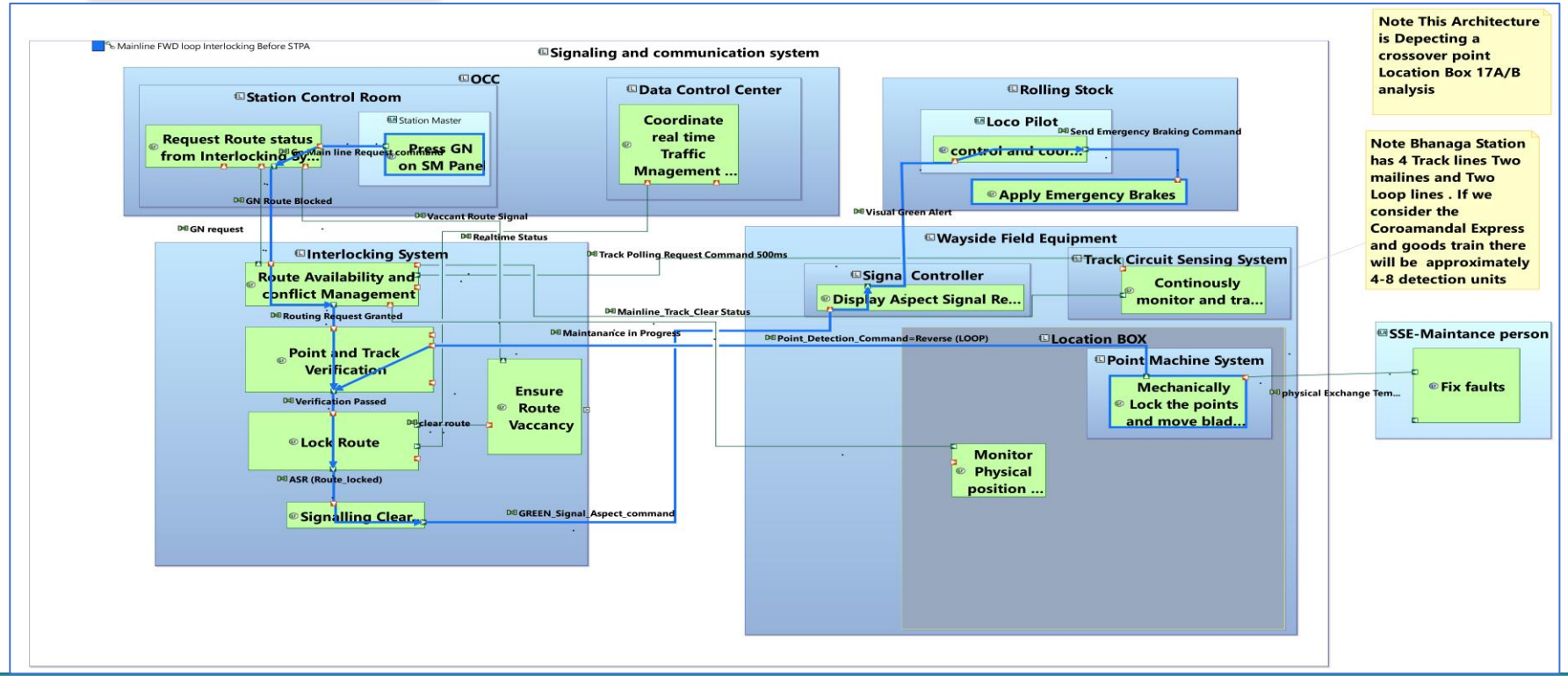
Track Sensing System

Rolling Stock

Is this architecture safe?

Are there missing critical items ? components/Actors, functions, functionexchanges?

*With this model , now being a **Single Source of truth** across teams , STPA is leveraged to answer these questions..*



STPA

Safety Analyses

- Functional Hazard Analysis (FHA,HARA)
- Fault Tree Analysis (FTA)
- Failure Modes and Effects Analysis(FMEA)

Classical safety approaches

& many more...

- Component centric
- Linear cause-effect chains
- Human Interactions and impact of other system on System is not effectively evolved.

Technical limitations

- Systems Theory → safety, a control issue
- Software Human Interactions
- Early life cycle adaptability
- Well suited for architecture analysis
- Feedback loops and control structures
- interactions

Controller

Control activity

Feedback

Process/ Plant

Developed at MIT, Boston

All verticals

Purpose	***Identify accidents and hazards***
Hierarchical Modeling	***Construct the plant-control model***
UCA	***Identify unsafe control actions***
Loss Scenarios	***Identify causal factors and control flaws***

Steps of STPA

Not just component flaws rather errors In integration, software error and human errors also under consideration

STPA Capella Plugin Process

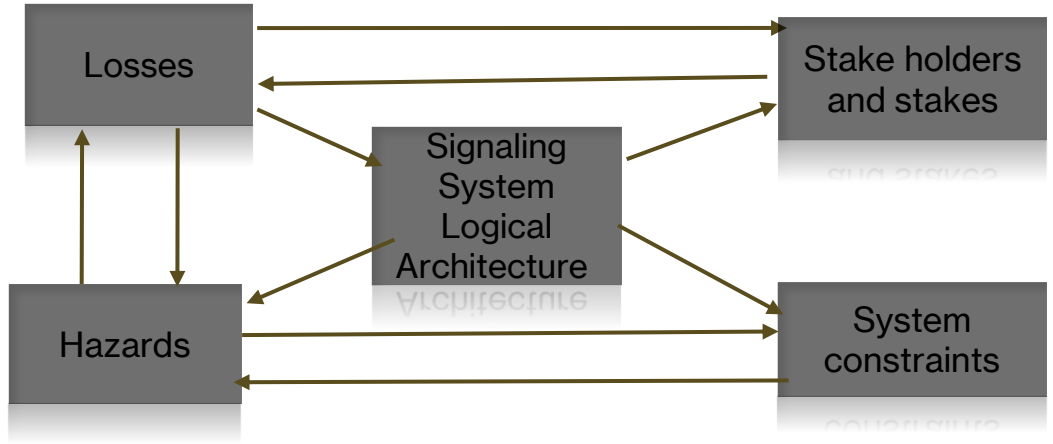
	Name	Stakes	Hazards
(L-01)	Loss of life or injury passengers, responders , Loco I	[ST-01, ST-04, ST-02, ST	[H-01, H-02, H-03]
(L-02)	Infarstructure damage to Rolling Stock , Interlocking S	[ST-02, ST-07]	[H-01, H-03]
(L-03)	Operational disruption and Loss of Trust	[ST-03, ST-02, ST-05, ST	[H-01, H-03]
(L-04)	Authorized Misrouted Mainline Movement	[ST-03, ST-04, ST-08, ST	[H-04, H-01]

1) Purpose of Analysis

2) Model the control structure

3) Identify UCAs

4) Identify Loss Scenarios



	Name	Losses
(SH-01)	**Loco Pilot**	
ST-01	life At threat	[L-01]
(SH-02)	**OCC**	
ST-02	Trains movement and coordination	[L-01, L-02, L-03, L-04]
(SH-03)	**Station Master**	
ST-03	wayside and internal safety at stake	[L-03, L-04]
(SH-04)	**Passengers**	
ST-04	Loss of life	[L-01, L-04]
ST-05	Trust is at stake due to inconvience	[L-03]
(SH-05)	**Power system**	
ST-06	infastructure at stake	[L-03, L-04]
(SH-06)	**Maintenance Personal**	
ST-07	Trust is at stake	[L-01, L-02, L-03]
(SH-07)	**Rolling Stock**	
ST-08	InfraStructure Damage	[L-04]

	Name	Losses	System-Level Constraints
(H-06)	Track Circuit Failure	[L-01, L-04]	[SC-03, SC-01]
(H-05)	No ATP Kavach verify failsafe behaviour	[L-02, L-04]	[SC-05]
(H-04)	Signal Passed at Danger(SPAD) distance not monitored	[L-04]	[SC-02, SC-03]
(H-03)	Signal Circuit Alterations due to Manual Intervention	[L-01, L-02, L-03]	[SC-03]
(H-02)	Wrong/Misleading Signal	[L-01]	[SC-02]
(H-01)	Train proceeds to occupied loop route Mismatch point Infastrcture Fail	[L-02, L-03, L-01, L-(	[SC-01]

	Name	Hazards	Res
(SC-01)	Routes must be mutually Exclusive no conflict simulateanously	[H-01, H-06]	[]
(SC-02)	Interlocking should prevent unsafe point Movement	[H-02, H-04]	[]
(SC-03)	verification logic must recheck and Verify validate the UCR, N/R point machine command	[H-03, H-06, H-04]	[]
(SC-04)	signal aspect must accurately reflect route status	[H-04]	[]
(SC-05)	ATP units or KAVACH to be installed to minimise the imapct earlier	[H-05]	[]

The table keeps evolving with multi-disciplinary teams

All interconnected and a basis for the next step

Model items → Stake holders → Stake → Losses → Hazards and constraints

The control structure will be investigated in the next slide....

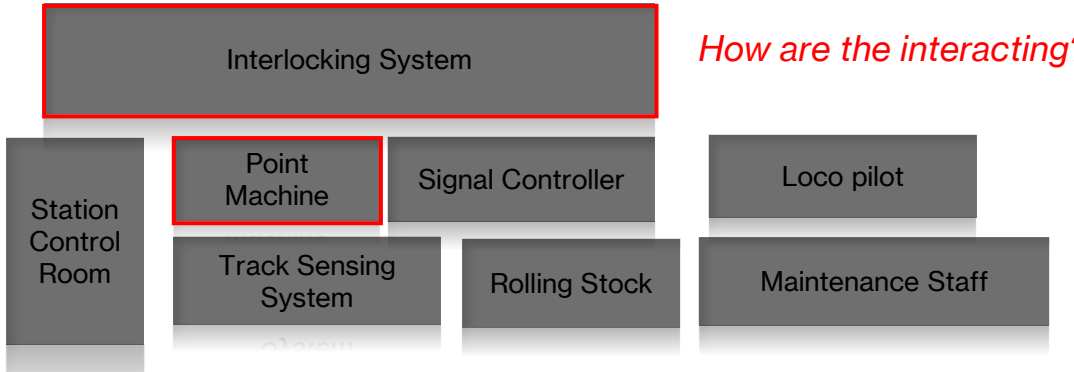
Modeling & Analysis Cont'd...

1) Purpose of Analysis

2) Model the control plant

3) Identify UCAs

4) Identify Loss Scenarios



How are the interacting?

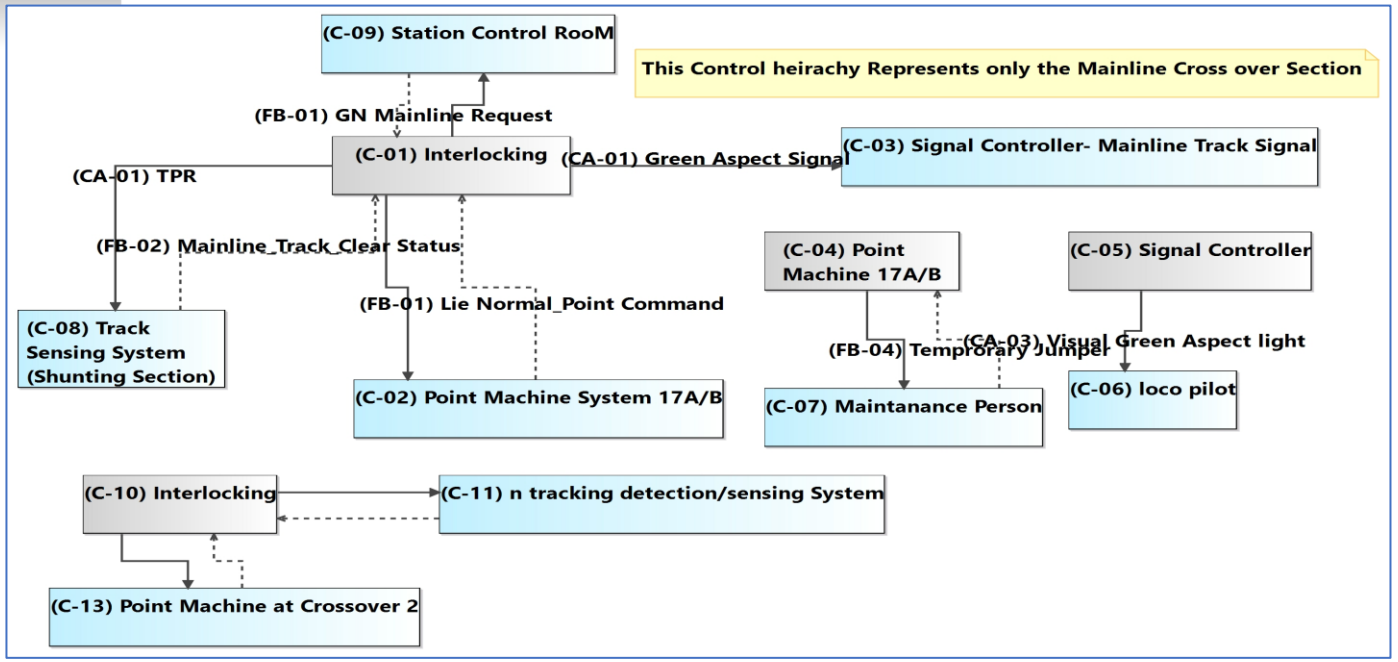
What are the control actions?

What is the feedback loop?

What will render this interaction unsafe ?

What are missing in the control and feedback paths

we will see that in the next step



Modeling & Analysis Cont'd...

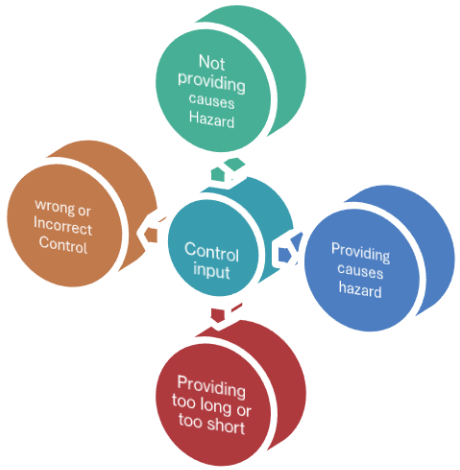
1) Purpose of Analysis

2) Model the control structure

3) Identify UCAs

4) Identify Loss Scenarios

When can a control activity and feedback loops be unsafe?

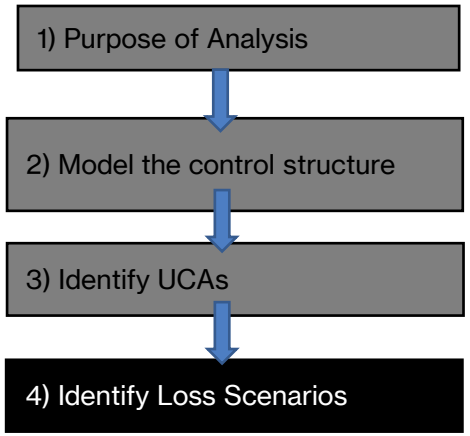


	Name	Violated Constraints	Hazards
FB-01	Lie Normal_Point Command		
Not providing causes hazard			
UCA-03	Point machine fails to move points when commanded	[SC-02, SC-03]	[H-03]
Providing causes hazard			
UCA-01	Detection contacts send "Normal" signal when physically in "Reverse" p	[SC-04]	[H-04]
pped too soon, applied too lo			
UCA-02	Interlocking Doesnt Detect wrong Wiring at location BOX	[SC-03]	[H-03]
ong timing or order causes haz			
UCA-04	Points move during temporary jumper placement (maintenance)	[SC-01]	[H-01, H-06, H-07]
CA-01	Green Aspect Signal		
Not providing causes hazard			
Providing causes hazard			
UCA-06	Shows green when route checking relay shows false "safe"	[SC-03, SC-04]	[H-04]	[]
ong timing or order causes haz			
UCA-05	GREENFalse trueGreen lamp lights when final relay has NOT picked up	[SC-04, SC-03]	[H-04]	[]
pped too soon, applied too lo			
UCA-07	Green aspect remains even after relay drops (lamp stuck on)	[SC-04]	[H-04]	[]

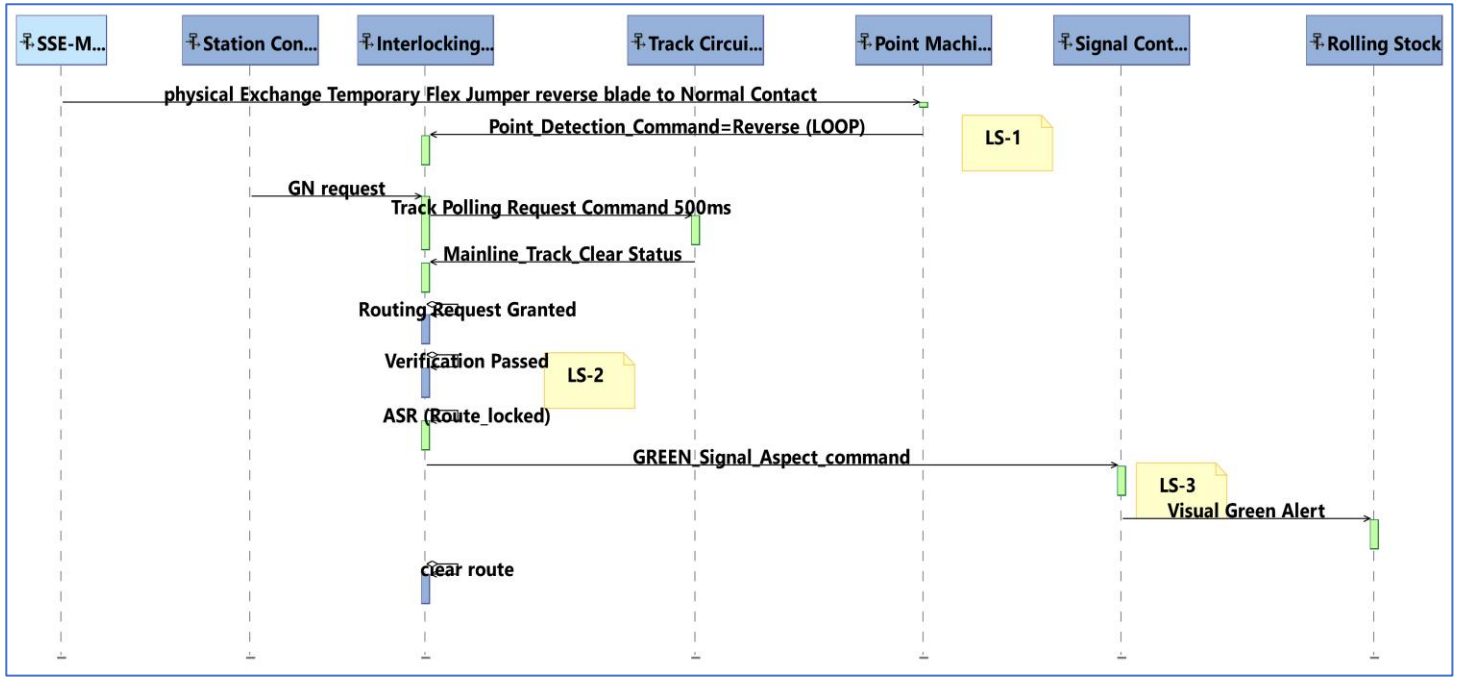
Unsafe actions → violated constraints → Hazards → losses → stakes → stakeholder → Capella element → S&TC → Interacting Systems

Now we see the recommended actions to mitigate these flaws in design !

Modeling & Analysis Cont'd...



What loss scenarios can occur due to UCAs and what constraints are violated?



What how can we mitigate them?

	Name	Control Action
(LS-01)	Inadequate Maintance procedures , human negligence wrong Jumper Leading to corrupted feedback	
(LS-02)	And independent Sensor relay interlocking cannot detect fault single contact used 21WNR relay lied completel	FB-01 (Point Machine System)
(LS-03)	No wiring Supervision , Resistance Change not Detected	
(LS-04)	No tamper Detection , Maintance Person opens location without Lockout apply incorrect labeling	

Tamper Switch for Detection of Human Interference

Authorization for maintenance complete then only Route Requested

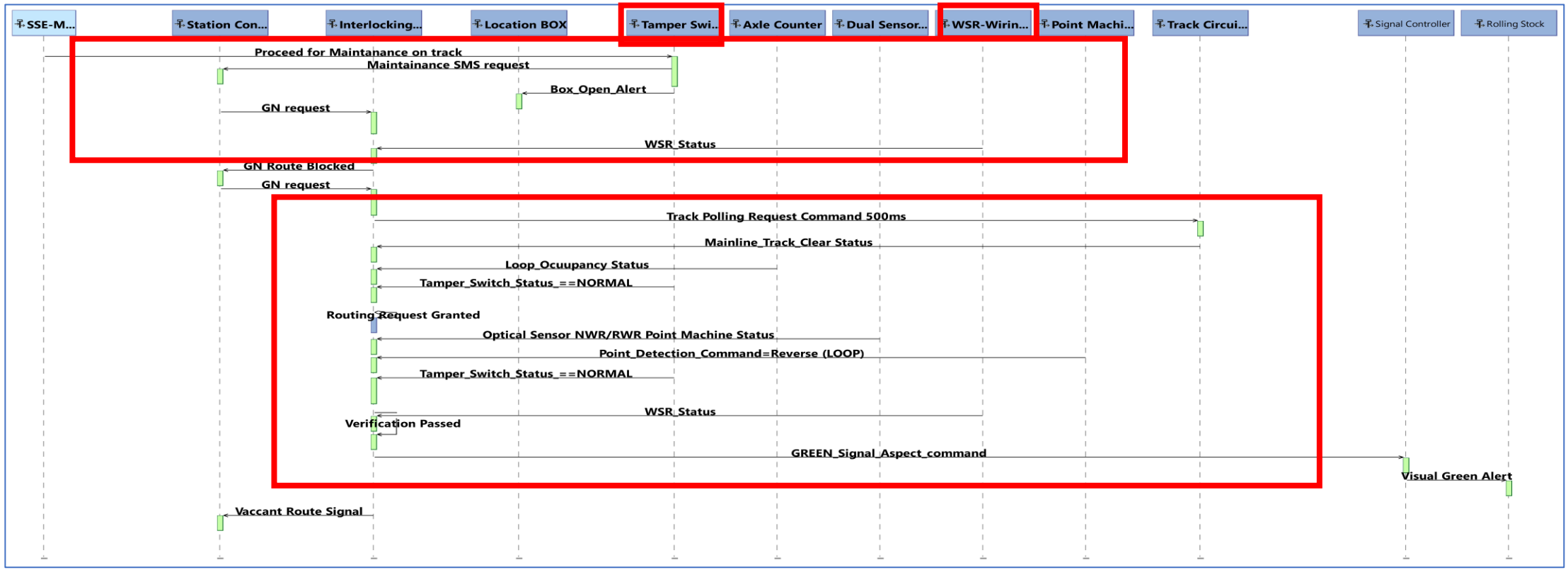
Double Failsafe Verification needed

Newer functions , and its requirements – Newer components ?

Loss Scenario Analysis Mitigation

We try to Apply MBSE to identify mitigation actions on existing architecture

- *Example Track Status Monitoring using Axle Counters help check wagon on track effectively*
- *Wiring Resistance Check for any change in signalling cable done during maintenance and prevent the Stationmaster from entering loop Line Request is blocked for Interlocking*
- *Dual Sensor for Point Machine as redundant method to ensure verification*



Modeling & Analysis - Observations and improvements

Key Lesson:
Safety is achieved not just through logical correctness, but through physical integrity verification at every interface.

Logic develop ment

basis refines

STPA Analysis

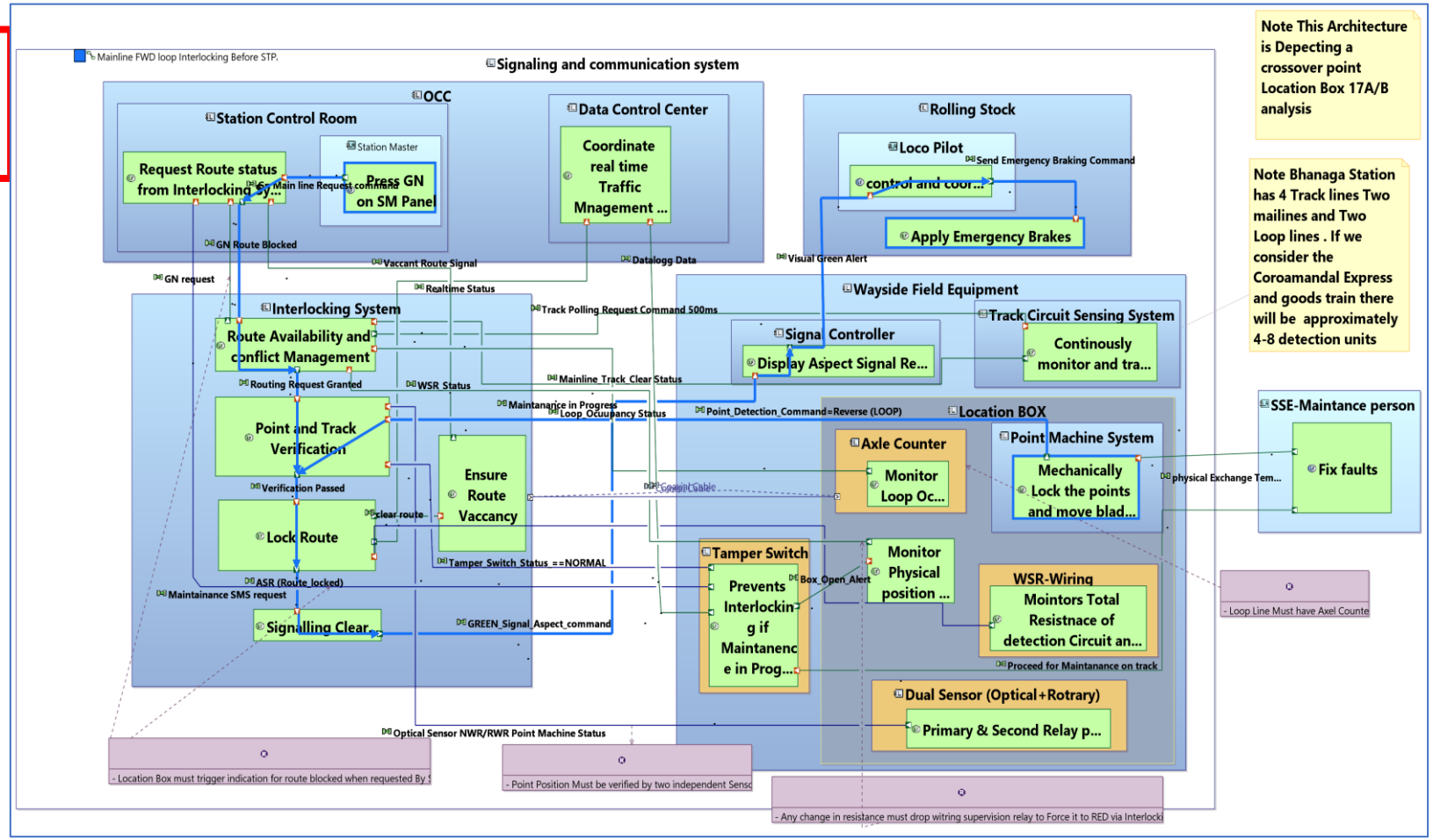
Model Upgrades

- Mitigation requiremen ts
- Newer functions
- Function exchanges
- Components

Architecture correctness

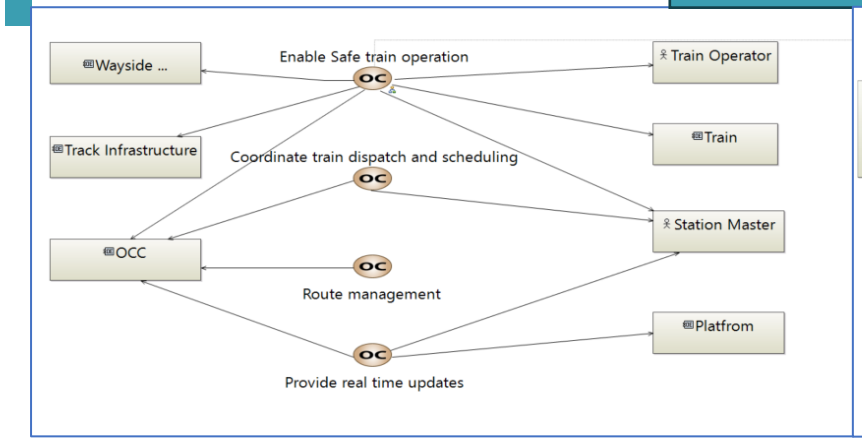
..and that's how we see the value!

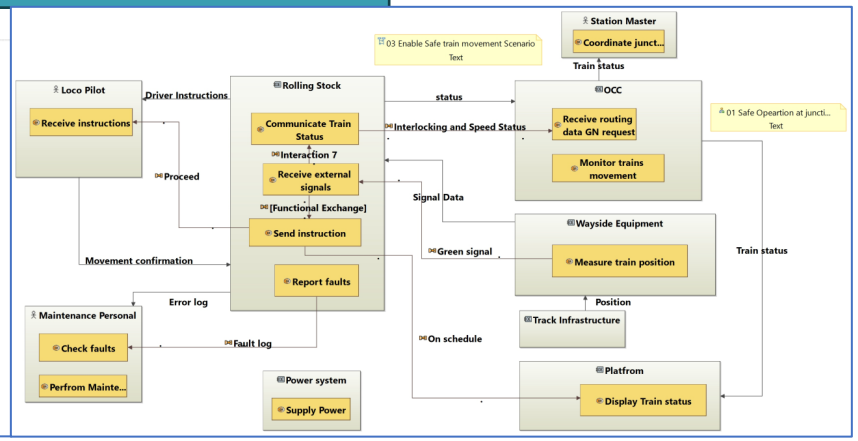
Tools, methods , process to build better architectures for tomorrow



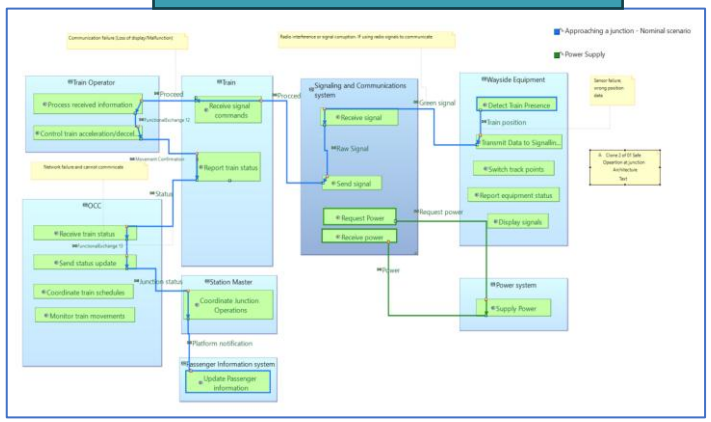
Overview

Operational Analysis



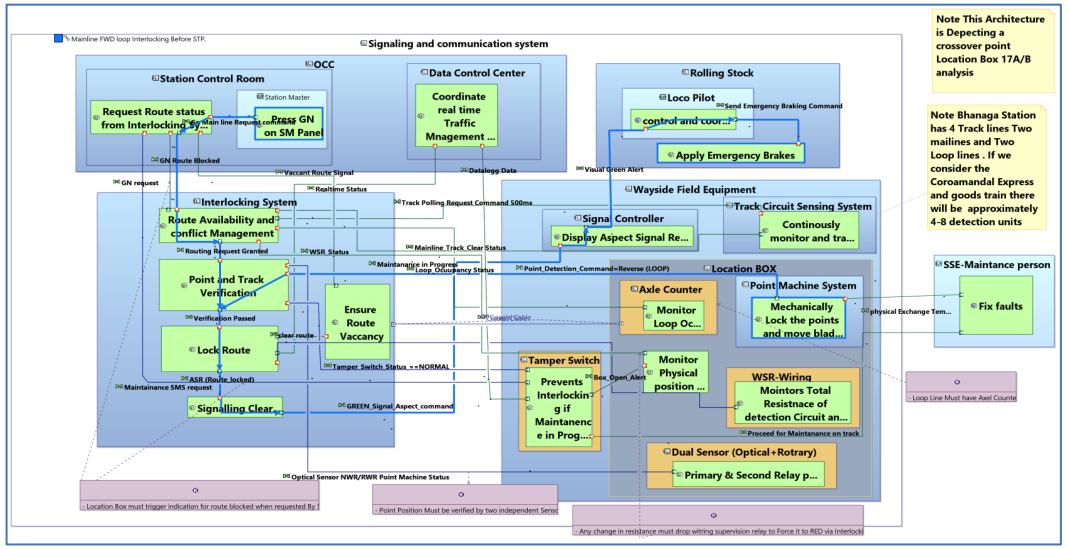


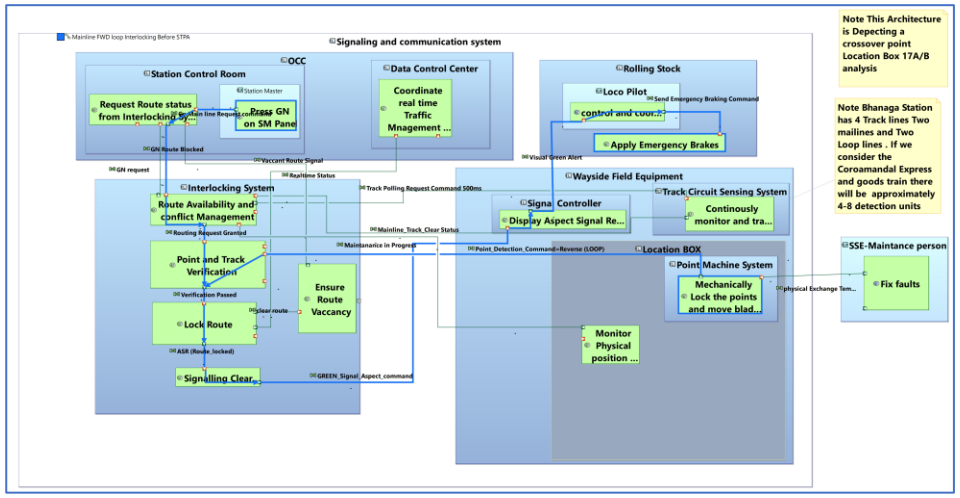
System Analysis



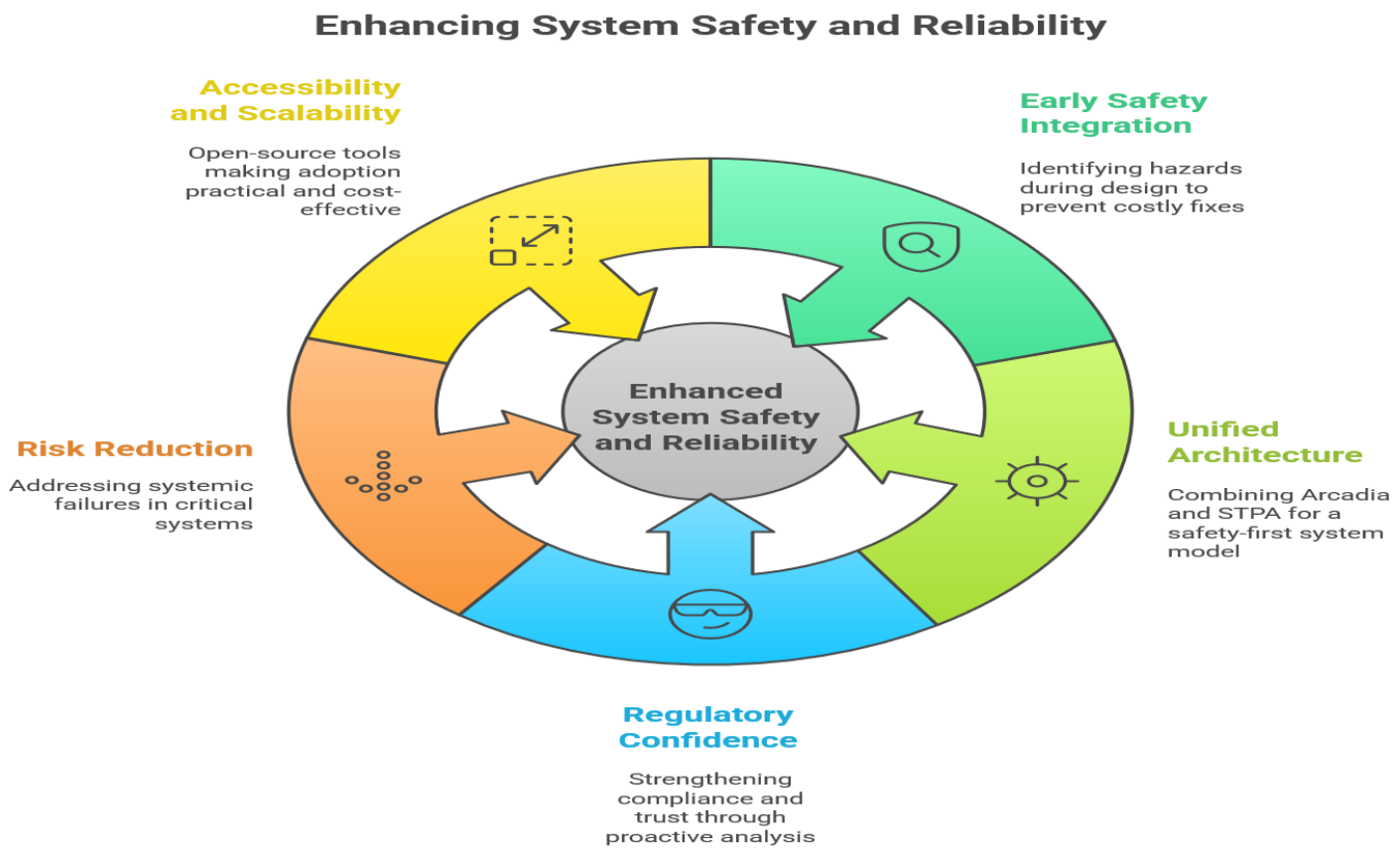
Logical Architecture

STPA Safety Assessment





Value Proposition



Conclusion

- Problem Statement for Rail Application ✓
- Logic Architecture Design ✓
- The Pain area – Safety & economics ✓
- Safety Analysis ✓
- Observations ✓
- Enabling Design improvements ✓

challenges

- Complex design
- Heavy Cost
- Operating economics
- Human Safety
- - ilities

Better , safer architecture

- MBSE
- SE
- STPA
- Safety flaws in the model
- Design-changes
- Safety requirements
- Architecture validation Arcadia)

Final Take-Aways for the audience

- A state of the art system for Rail applications
- Little to No cost Solution
- Leaner Proactive safety analysis methods
- Reusability and Scalability Across Similar Products

https://en.wikipedia.org/wiki/Kavach_(train_protection_system)#/media/File:TCAS_Stationary_Master_Computer.jpg

Thankyou

Questions?

References

- Insights on India. (2024). Railway accident data (2019–2024). ***https://www.insightsonindia.com/2024/10/03/railway-accident-data-2019-2024/***
- Leveson, N. (2011). Engineering a Safer World: Systems Thinking Applied to Safety. MIT Press.
- Abdulkhaliq, A., et al. (2017). Comparison of the FMEA and STPA safety analysis methods–a case study. Software Quality Journal, 26(4), 1493–1518.
- Slowey, K. (2024). Application of the System-Theoretic Process Analysis (STPA) technique to enabling systems in the rail industry. INCOSE International Symposium, 34(1), 728–742.
- Thomas, J., et al. (2023). Applying STPA-based methodology supported by Systems Engineering models to a UK rail project. Safety Science, 167, Article 106275.
- Fleming, C. H., et al. (2013). Safety assurance in NextGen and complex transportation systems. Safety Science, 55, 173–187.

Thank you

www.blue-kei.com