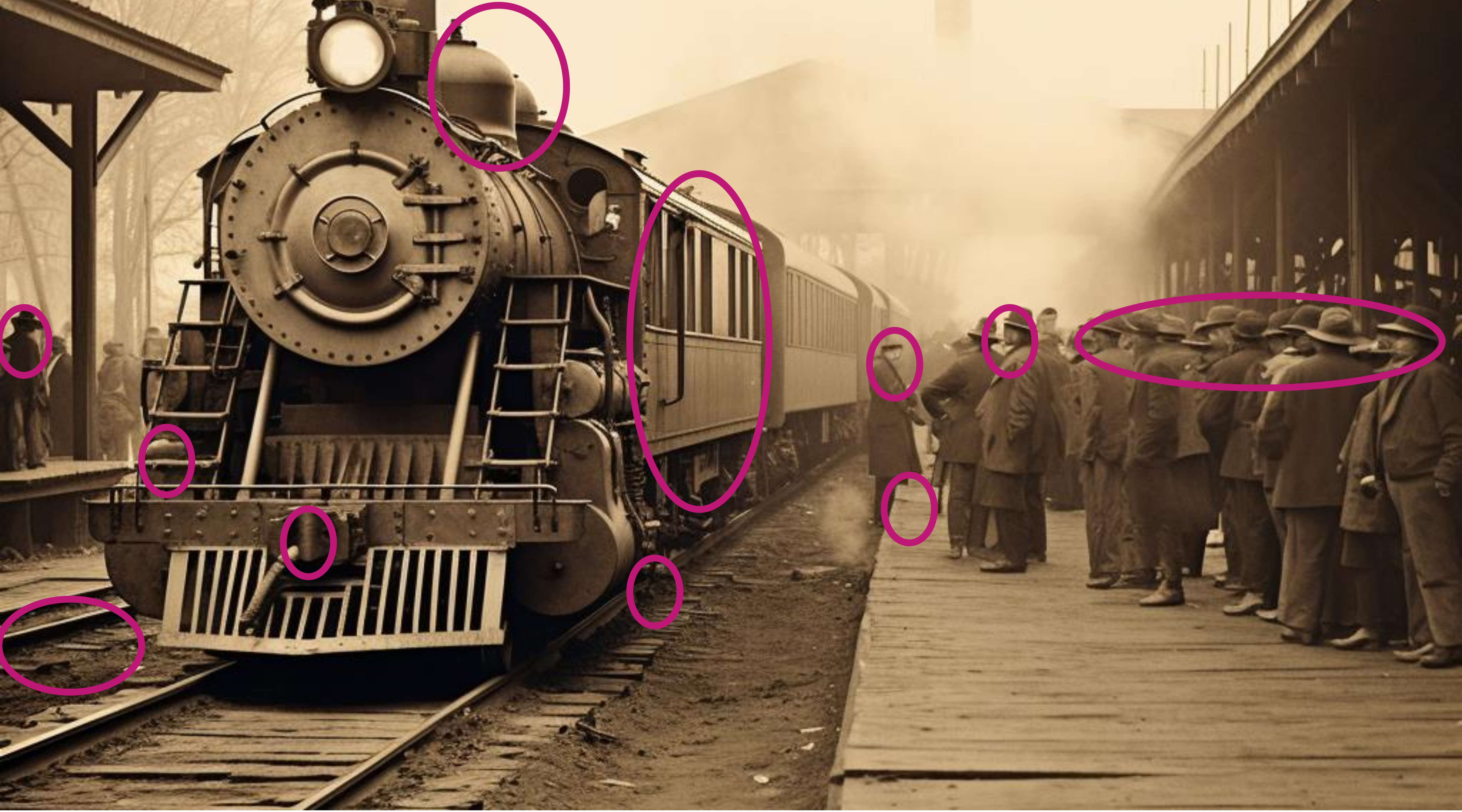
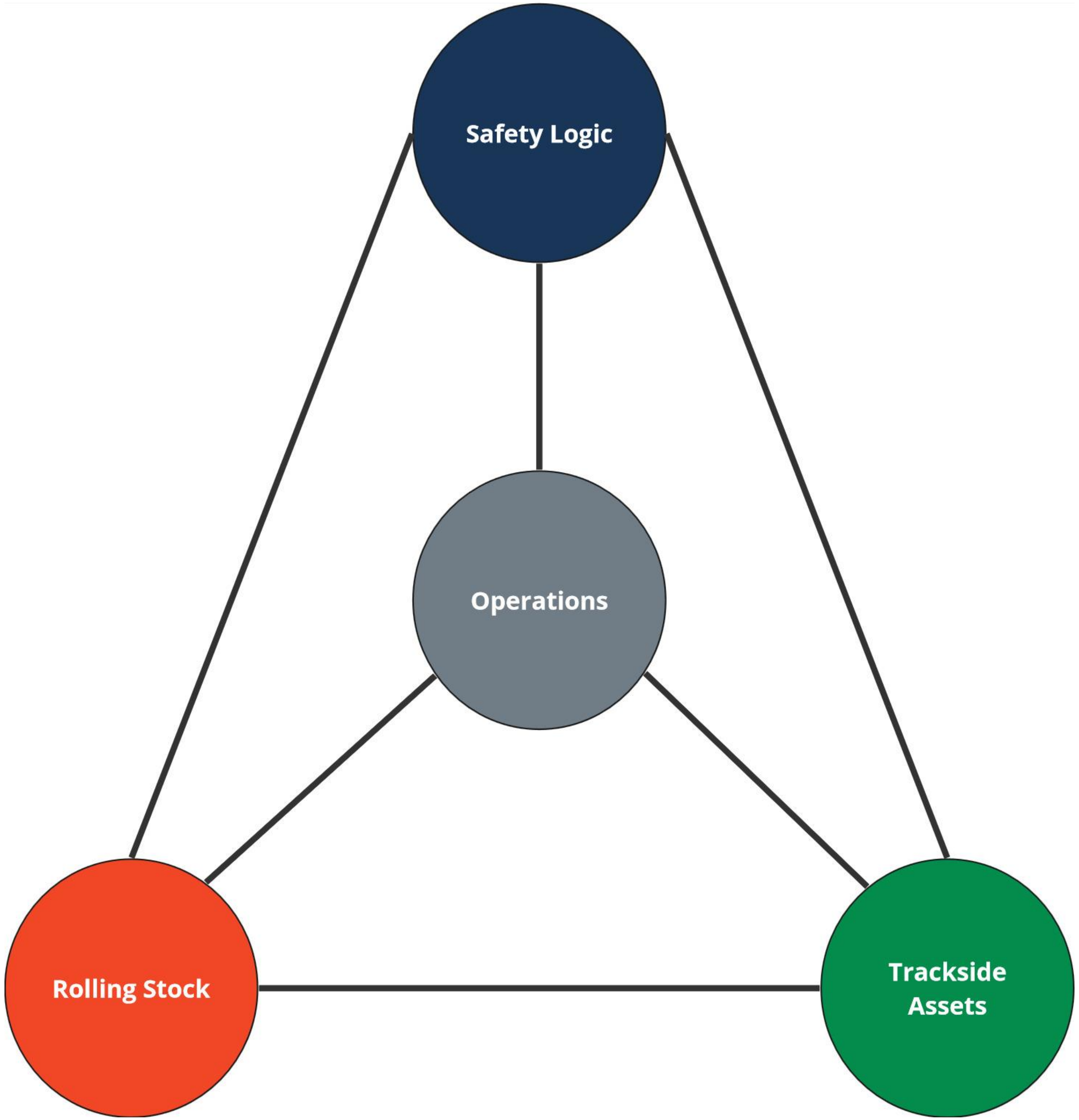
Generic Engineering Rules for ETCS L2 FS w/o Signals

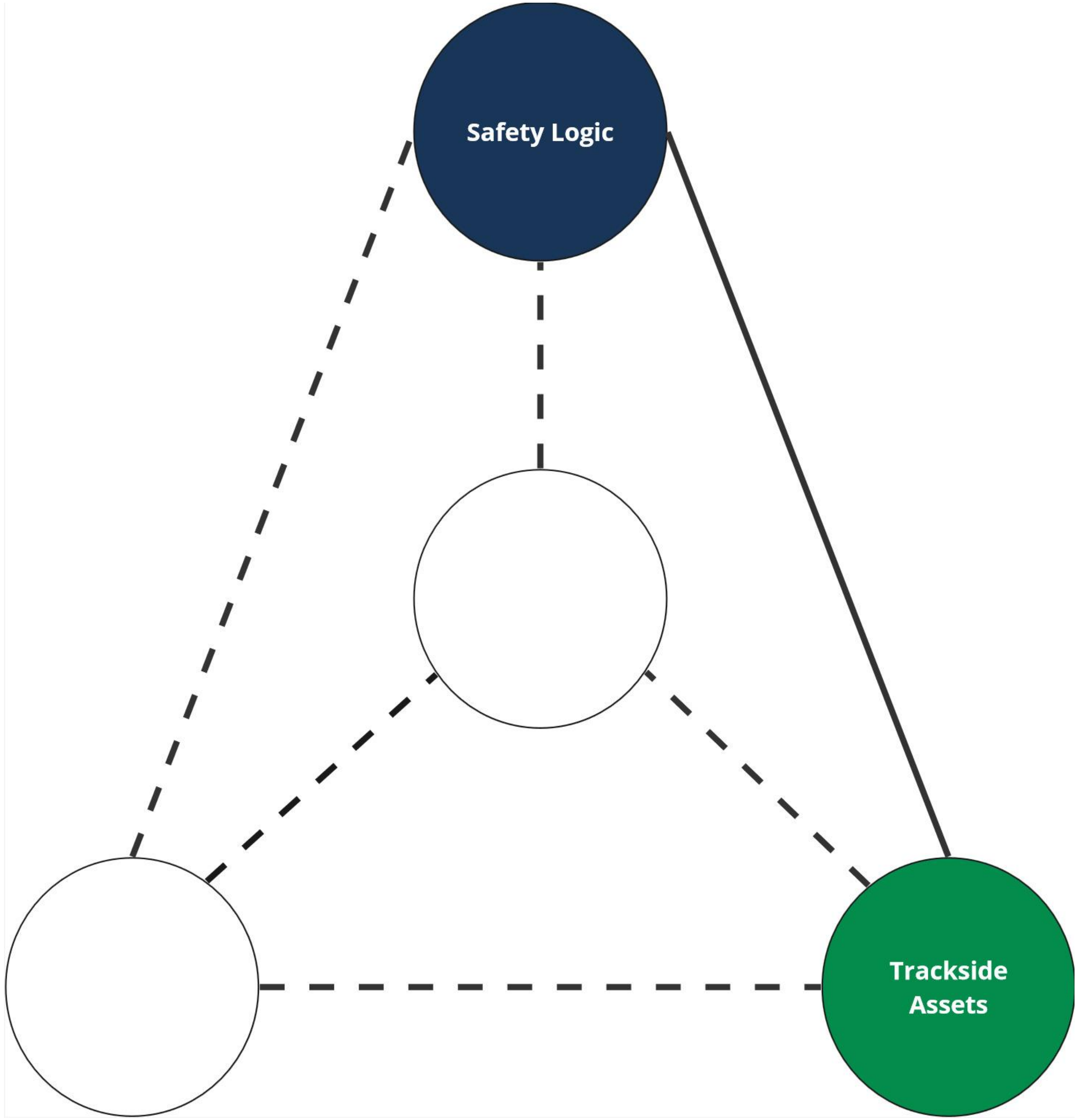
Planning and safety logic requirements

Systems Lab 21



Helsinki
Hamina Kotka
Turku Naantali
Tallinn
Oslo
Örebro
Stockholm
Ventspils
Riga
Gothenburg
Klaipeda
Aarhus
Malmö
Copenhagen
Trelleborg
Vilnius
Kaunas
Gdynia/Gdansk
Shannon-Foynes
Dublin
Kiel
Rostock
Cork
Bremerhaven
Szczecin/Swinoujscie
Hamburg
Bremen
Amsterdam
Berlin
Poznan
Utrecht
Osnabrück
Magdeburg
Warsaw
Rotterdam
Hannover
Frankfurt/Oder
Zeebrugge
Antwerp
Düsseldorf
Gent
Calais
Lille
Brussels
Cologne
Dresden
Wroclaw
Prague
Liege
Le Havre
Frankfurt
Würzburg
Ostrava
Katowice
Nuremberg
Mannheim
Luxembourg
Brno
Zilina
Stuttgart
Regensburg
Passau
Metz
Paris
Vienna
Bratislava
Strasbourg
Nantes/Saint-Nazaire
Munich
Wels/Linz
Tours
Dijon
Basel
Innsbruck
Budapest
Klagenfurt
Graz
Arad
Brașov
Sulina
Timișoara
Udine
Trieste
Lyon
Novara
Verona
Zagreb
Ljubljana
Bucharest
Constanța
Venice
Koper
Turin
Milan
Rijeka
Craiova
A Coruña
Gijón
Bordeaux
Toulouse
Bilbao
Genova
Bologna
Ravenna
Burgas
Sofia
Vitoria
La Spezia
Ancona
Valladolid
Marseille
Livorno
Perpignan
Zaragoza
Porto
Aveiro
Rome
Barcelona
Bari


Safety Logic
Operations
Rolling Stock
Trackside
Assets


Safety Logic
Trackside Assets

Agenda

1. Project Context (5’)
2. Overview Generic Engineering Rules (20’)
   a. Goals
   b. Constraints
   c. Approach
3. Next Steps (5’)

Introduction

Generic Engingeering Rules

Next Steps

Photo by Robert Noreiko on Unsplash

Our Mission

"

[...] to streamline the planning, testing and commissioning of Digital Rail Infrastructure up to a continuous, "perpetual" certification

"


HPI
Hasso
Plattner
Institut
Digital Engineering · Universität Potsdam
Lab

Europe's Rail

Europe's Rail

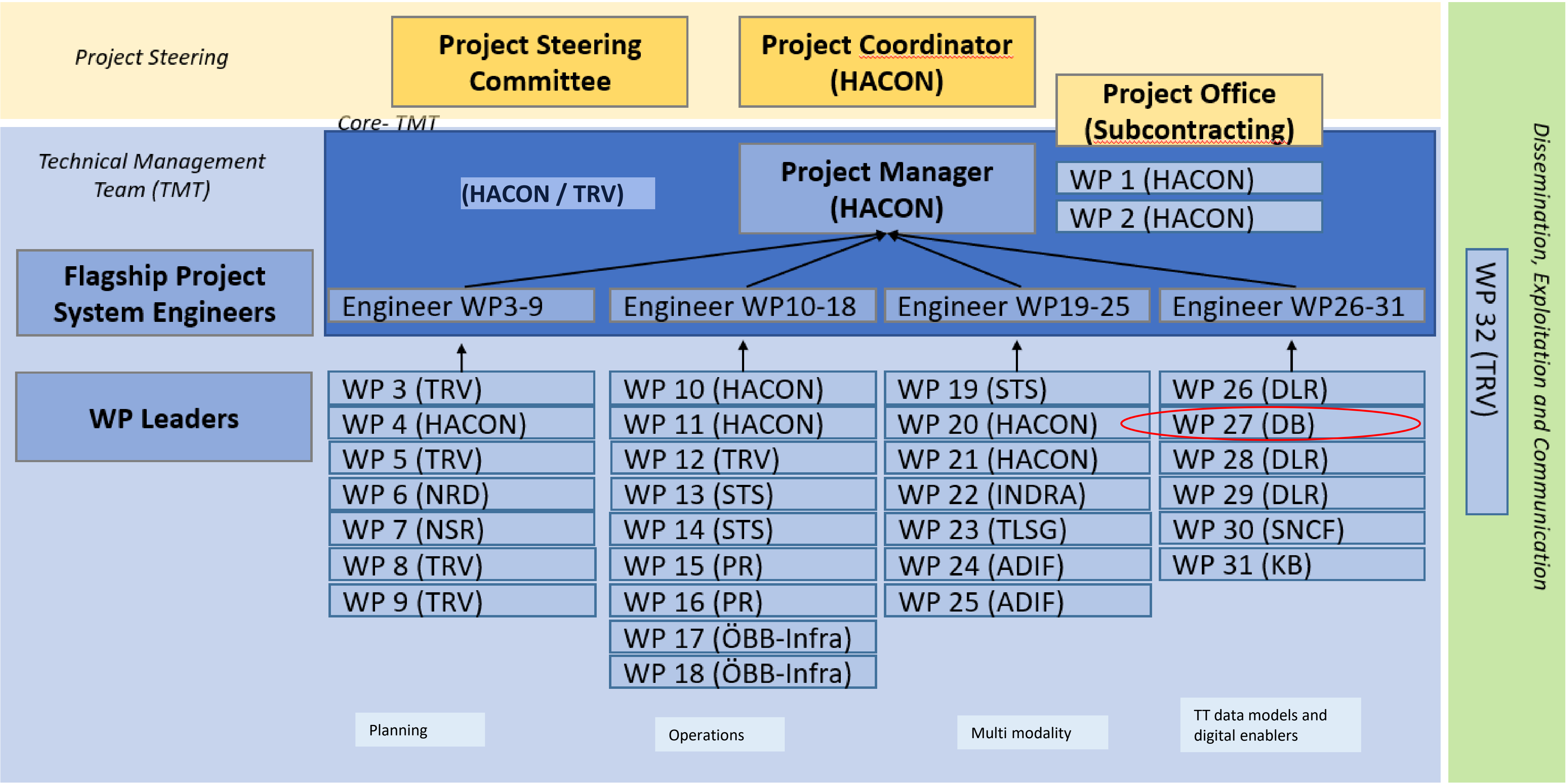
Flagship Area 1:

Network management planning and control & Mobility Management in a multimodal environment

FP1 MOTIONAL

European Rail Network and Mobility Management

Project Structure



WP 27 Tasks

27.1	Harmonised input data build the “Single Source of Truth	- Analysis of input data for construction projects, starting from CCS+ and its EULYNX Datamodel - Analysis of digital twin approach along the production process to operational phase based in BIM - Specification of the attributes required by the digital twins by users involved in design, construction, and maintenance. The specification must be per mode of acquisition (e.g. drone, train, etc), speed of acquisition, number of points minimum track length - Use cases for data models, common data format for the planning, engineering, maintenance, and operation process
27.2	Feature Extraction	- Access to the available data e.g., Point Clouds, geographical data, condition data, video frames, etc. - Automatic patterns and objects recognition software development - Object detection and extraction - Data update and change detection to digitalize their evolution as it is being built
27.3	Harmonized Engineering Rules	Starting from relevant data extracted from available data models (e. g. EULYNX Datamodel for CCS+) and set to standard format, the processes of planning by applying harmonized engineering rules for ETCS and ATO will be developed (incl. tooling) Definition of Asset Information Requirements (AIR) during the production process
27.4	Engineering	The planning result will be used for more efficient system integration by co-simulation and test automation The result and use cases are developed and tested based on a railway station project Five reference implementation projects for ETCS L2 or LR will be planned according to the findings, process and tooling of this WP
27.5	Deployment	- Evaluation of the possibilities to implement the EULYNX data model for the control, command and signalling system. - Developing a data platform for object and information management supporting data continuity in the production process of a railway station.
27.6	BIM Standard	- Adequate definition of information requirements in a human and machine-readable manner - Development of methods and standards for updating the Digital Twins for management purposes - Combining construction data acquired by different methods, from various sources and in different formats with DT

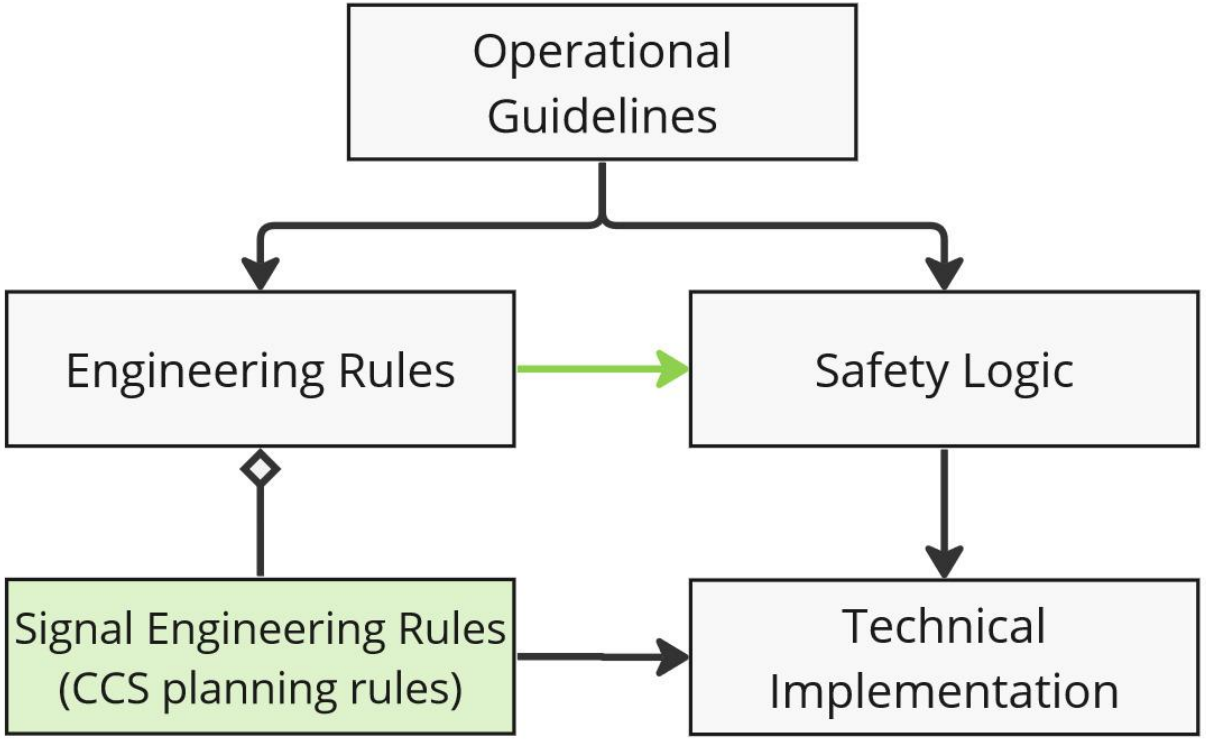
Introduction

Generic Engingeering Rules

Next Steps

Photo by Robert Noreiko on Unsplash

Differentiation and Interfaces



Differentiation and Interfaces

- **(Signal) Engineering Rules** = Specifications and guidelines for the planning of safety-relevant lineside assets in space for signalling, command and control

- **Safety Logic** = Specifications for the core of a functionally safe system, executing and/or supervising the safety functions

Differentiation and Interfaces

- **(Signal) Engineering Rules** = Specifications and guidelines for the planning of (often safety-relevant) lineside assets in space for signalling, command and control

- **Safety Logic** = Specifications for the core of a functionally safe system, executing and/or supervising the safety functions

Rules = Requirements

- Must be testable:

Rules = Requirements

- Must be testable:

Decidable

Rules = Requirements

- Must be testable:

Decidable

Unambigious

Rules = Requirements

- Must be testable:

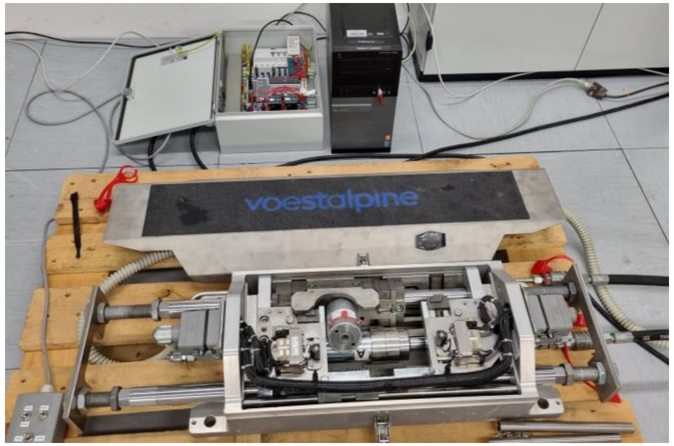
Decidable

Unambigious

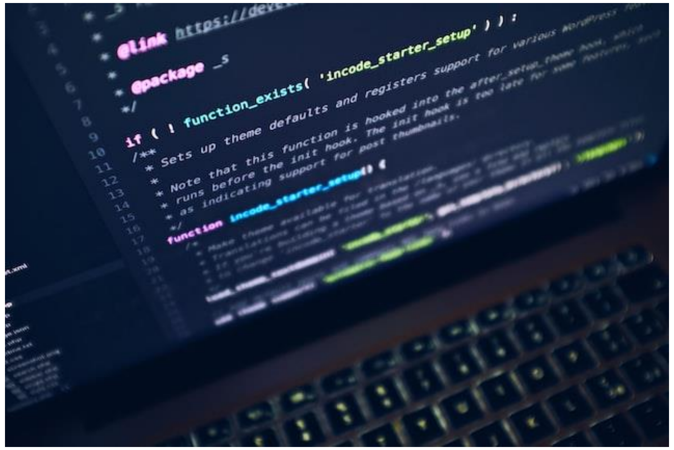
Consistent

Three Primary Goals

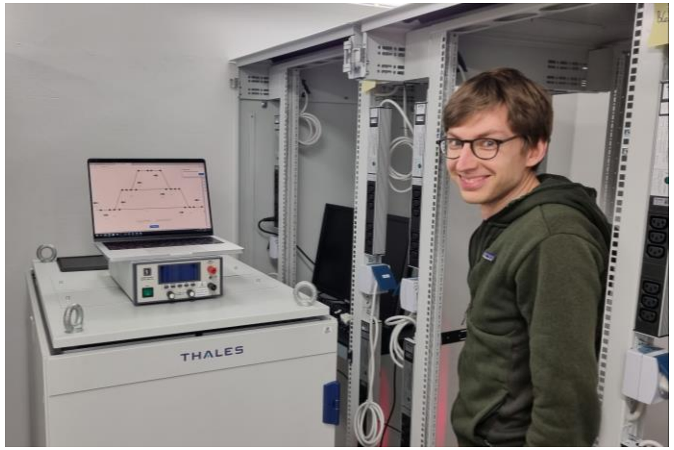
(1) Harmonized Signal Engineering Rules



(2) Advancing the SD1 Data Model (ERDM)



(3) Automated Planning and Plan Checking PoC



Approach

1. Disruptive rather than evolutionary
2. Greenfield with new lines in mind
3. Simplicity over completeness
4. Modularity (add-in logic, e.g. for optimal TVPS length calculation)
5. No national legacy

International Input

1. Operational Guidelines (DK, DE, …)
2. Signal Engineering Guidelines (NO, DE, …)
3. Research Publications (NL, BE, FR, DE, FI, DK…)
4. Expert feedback (AT, HU, DE, NO, …)
5. Reviews (EUG)

Scope for Engineering Rules

- ETCS L2 only
- No shunting/parking areas (for now)
- Limited ETCS modes: FS, OS, SR (and modes irrelevant to planning like NP, IS, TR...)
- Proof-of-concept via simplified planning and plan checking algorithm

Fundamental Assumptions

All movement is supervised movement

- Coupling of trains is done in OS (supervised)
- Non-supervised movement modes, LS, UN.. not permitted
- Mode SR is a fallback with additional restrictions (switch to SR only possible with central authority, similar to ATO GoA4)

Safe Start

- Trains are taken into operation in Trusted Areas or with help of Cold Movement Detection, i.e. switch to L2 FS is possible before entering the open track

No Flank Protection

- Flank protection exists only at the border of the modeled area (e.g. to protect from non-supervised movement in shunting/parking areas and “legacy” tracks)

No Planned Overlap

- Interlocking MAY dynamically calculate routes and overlap based on vacancy proving (RBC sends SvL != EOA) but overlap is not planned during CCS planning

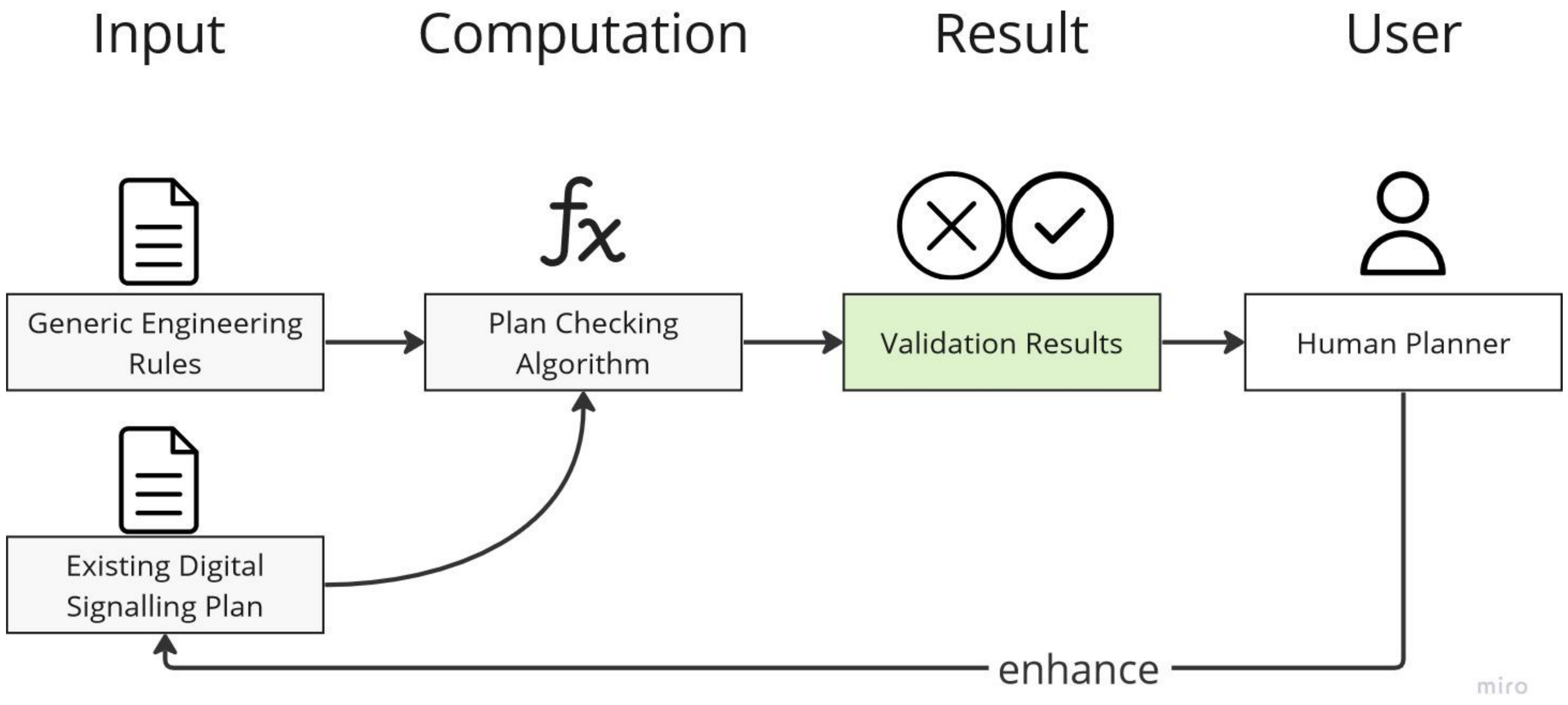
Challenges

- No harmonized EU operational rules yet (but generalizable input available, e.g. DK rulebook)
- Conflicting, simultaneous requirements (human planner vs. algorithmic solutions)
- Lack of available, open implementations (capacity, cost optimization)
- SD1 still in early development

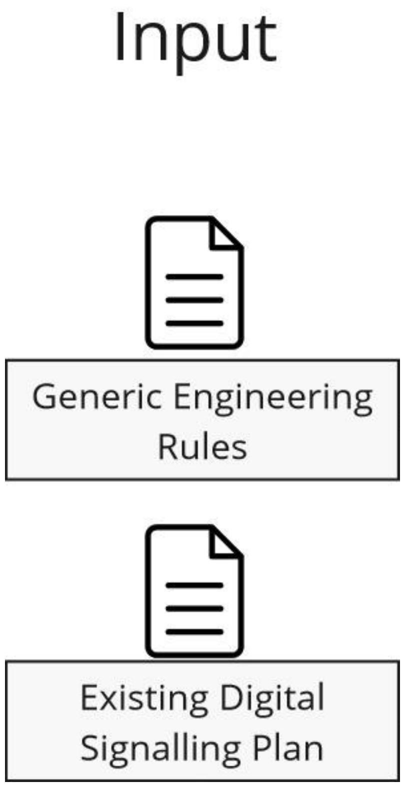
First Engineering Rules Phases

1. PoC Plan Checking
2. PoC Plan Generation
3. Long-Term Vision

Proof of Concept (Phase 1)

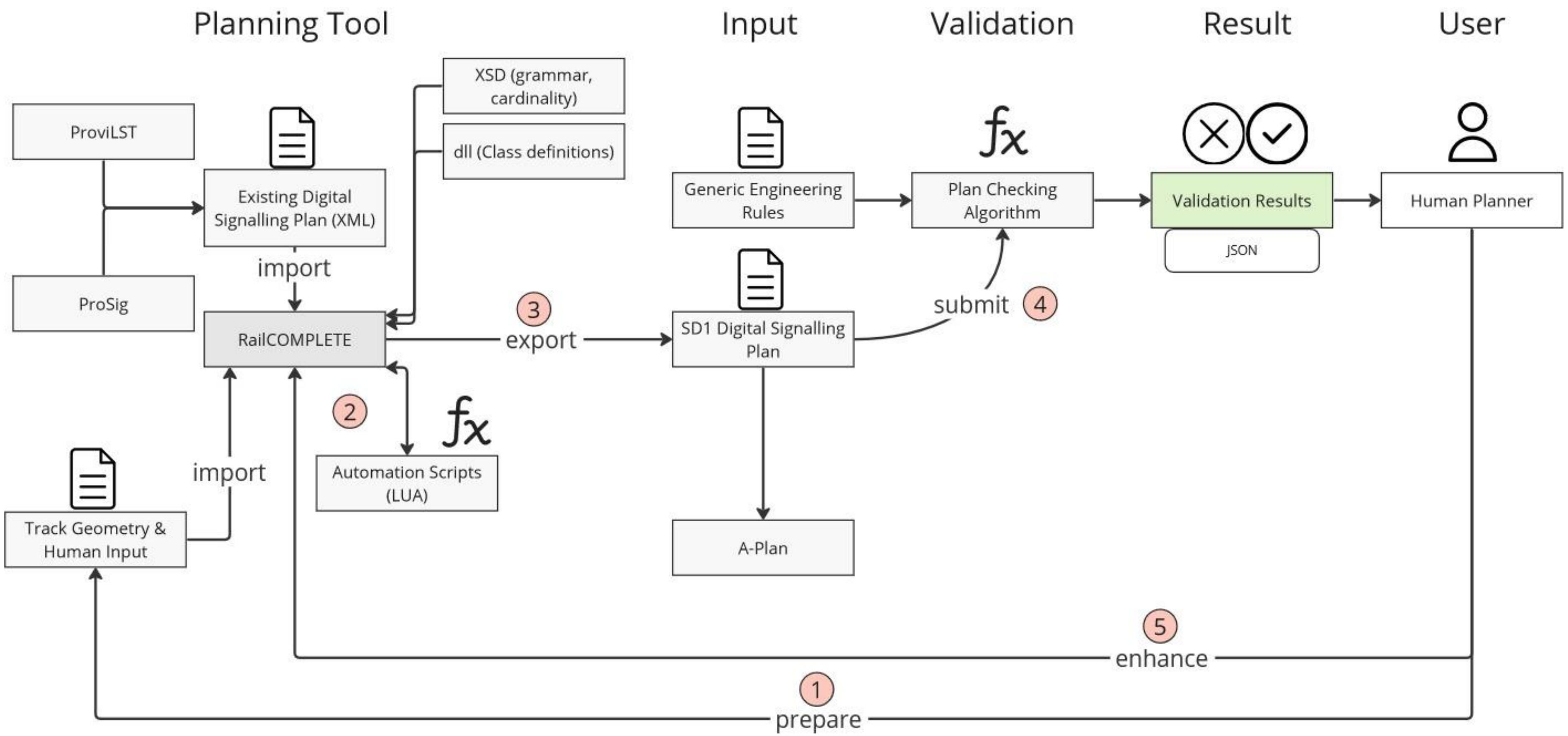


Phase 1 - Requirements

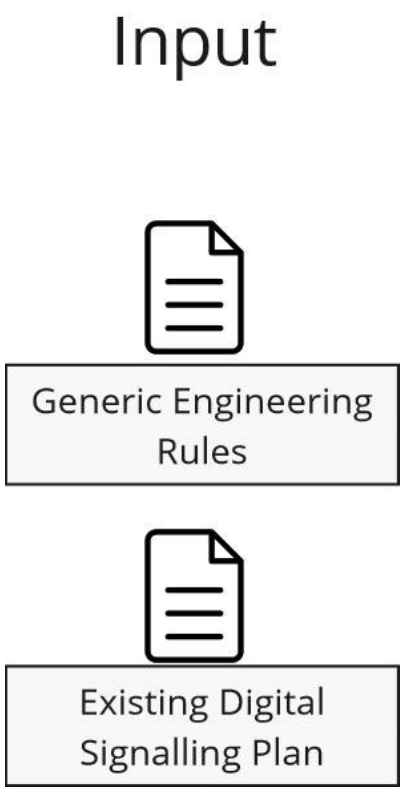


- Every property used in engineering rules is *decidable*
- Domain of the data model is expressive enough for the rules
- Existing planning document with necessary data

Proof of Concept (Phase 2)

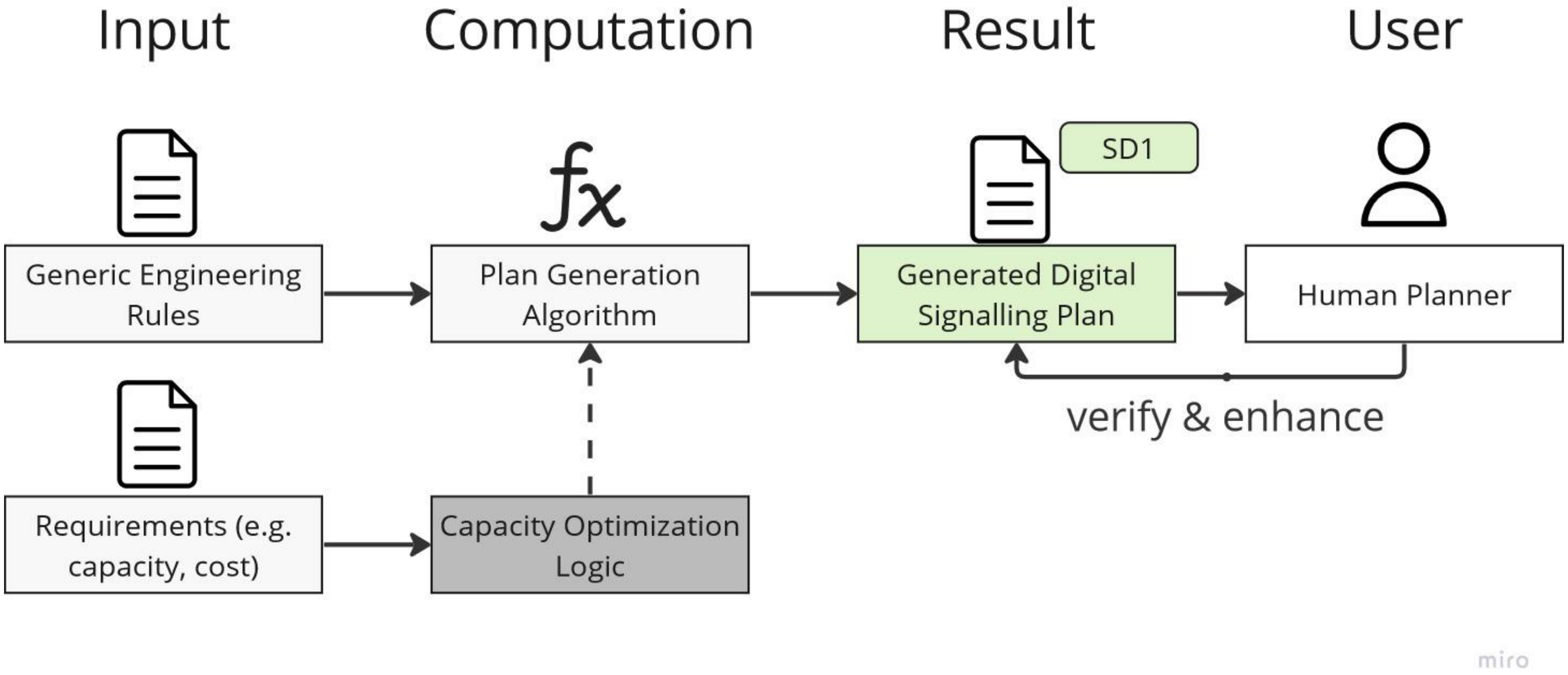


Phase 2 – Requirements (add.)



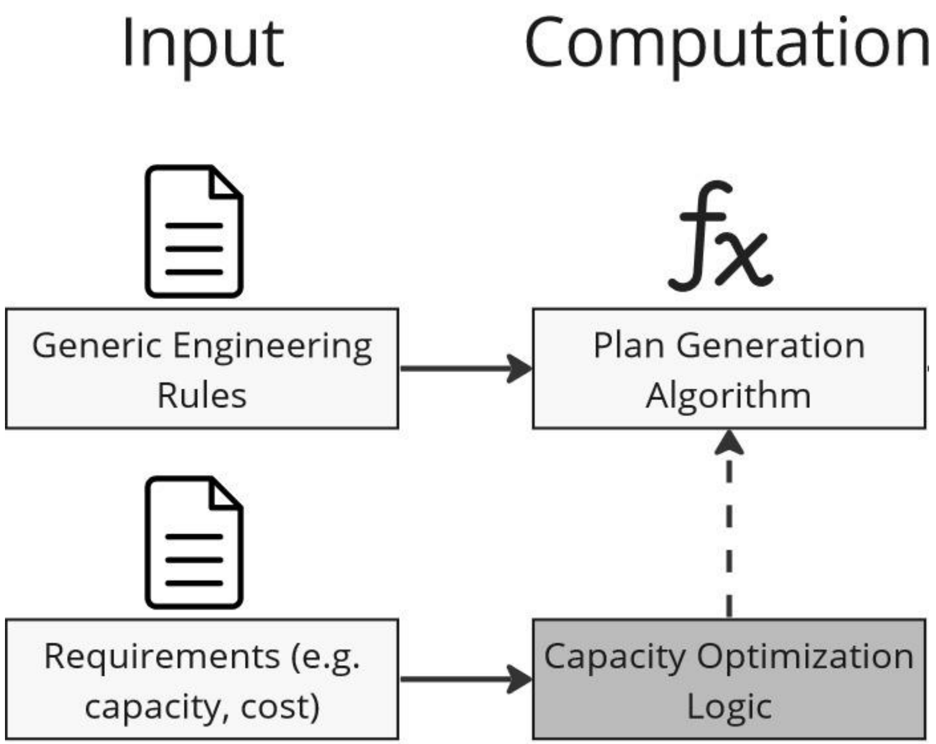
- Track geometry, catenary, speed profiles etc. defined (pre-planned)
- Manual steps (e.g. operational stop locations, definition of L2 area borders)
- Default values, algorithms and simplifications (to be replaced in later phases)

Vision



Input
Computation
Result
User
SD1
Generic Engineering Rules
Plan Generation Algorithm
Generated Digital Signalling Plan
Human Planner
verify & enhance
Requirements (e.g. capacity, cost)
Capacity Optimization Logic
miro

Vision - Requirements



- An optimal TVPS and Balise calculation algorithm exists (related work: TU Darmstadt & DB Netz)
- Requirements (capacity, cost, other parameters) are machine-readable
- Planning and capacity optimization logic share an interface (modularity)

Vision

- A DSL (domain specific language) for railway signalling requirements exists, which can generate plan validation and/or generation logic
  - Alternatively: a full reference implementation of the Generic Engineering Ruleset and all relevant constraints exists

- An optimal* capacity and cost algorithm exists

- A (learned) system exists which can evaluate possible plans and refine until the optimal plan has been found (according to design parameters)

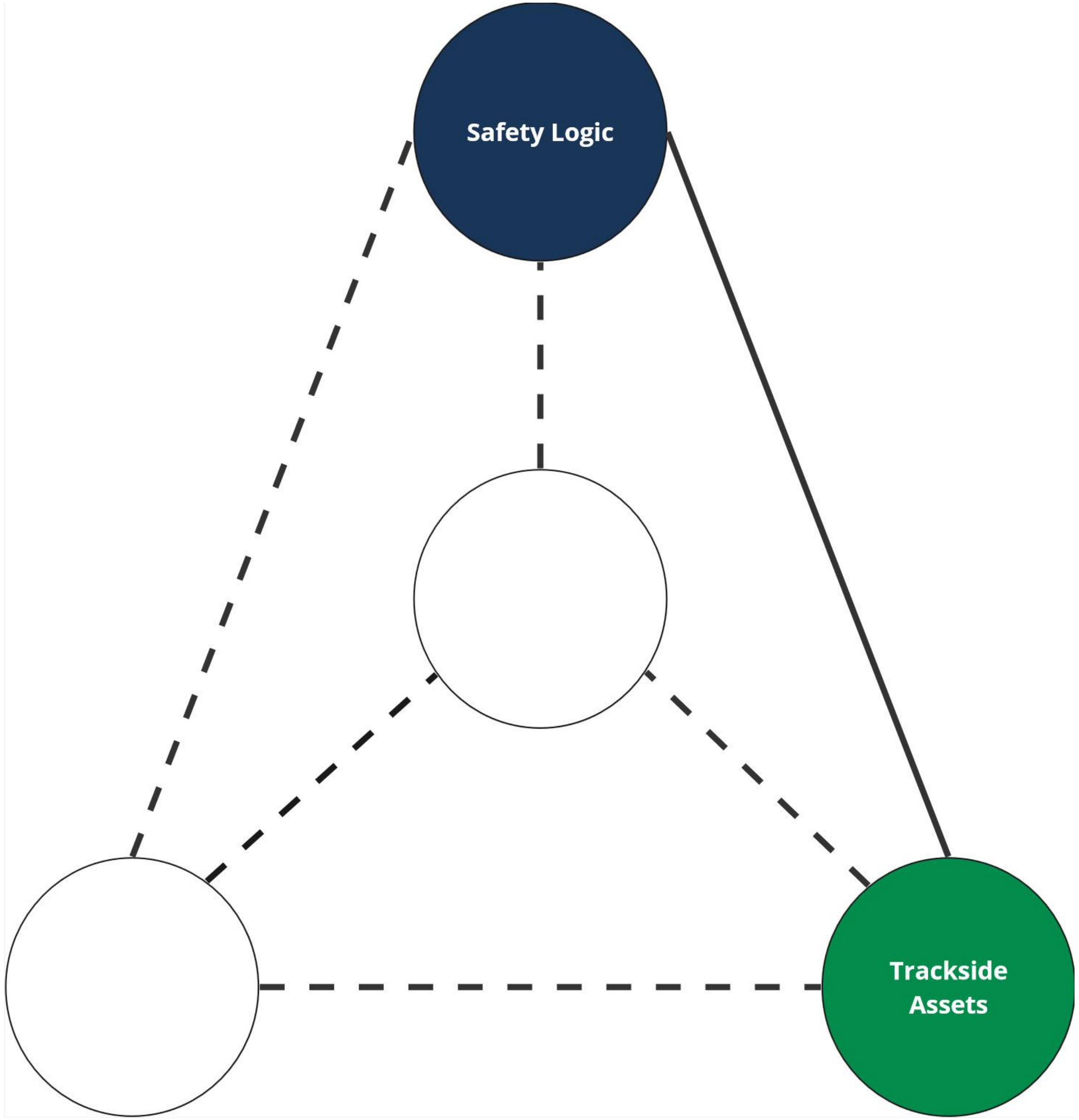
* locally optimal, so long as infrastructure projects are planned and executed line-by-line

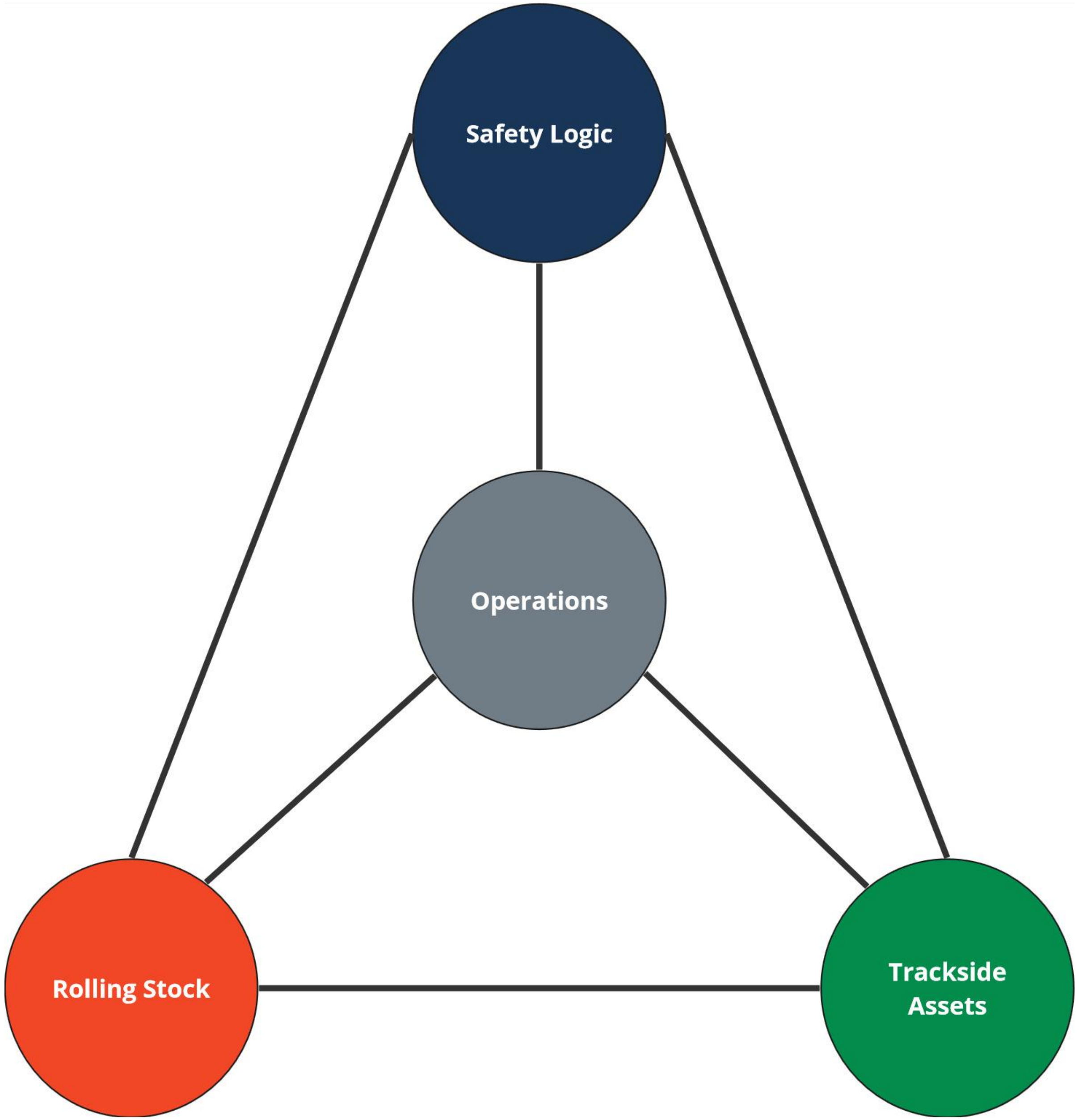
Scope

Generic Engingeering Rules

Next Steps

Photo by Robert Noreiko on Unsplash

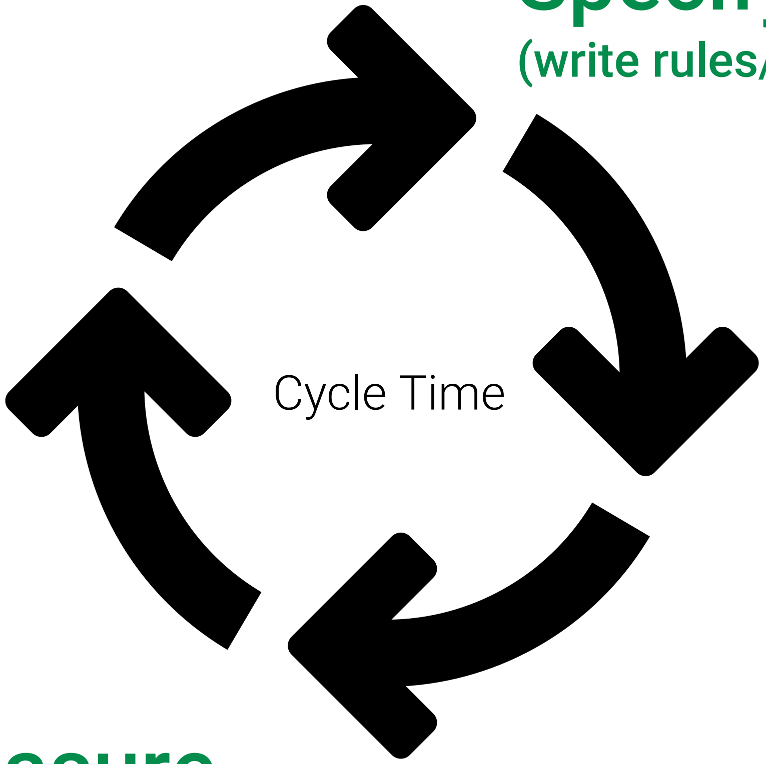

Safety Logic
Trackside Assets


Safety Logic
Operations
Rolling Stock
Trackside
Assets

Next Steps (Long-Term)

- Formalization of Generic Safety Logic
- Capacity / Cost Analysis
- Integration with Harmonized Operational Rules

Cycle Time


Specify
(write rules/test)
Build
(plan / operate)
Measure
(run tests, capacity / cost analysis)
Learn
(change)
Cycle Time

Benefits

- **Faster Cycle Time** = Reduced Cost + Better Quality Plans

- **Formalization** = lower complexity, fewer defects

- **Generic solutions** = access to a larger, European market
- Extensible Digital Process:
  - Integration of digital planning process and data into CTMS analysis
  - Adaptible to drop-in optimization logic
  - Familiar tooling

Thanks!

We appreciate feedback!