Application of STAMP to Risk Analysis of High-speed Rail Project Management in the US

3/27/14

Soshi Kawakami

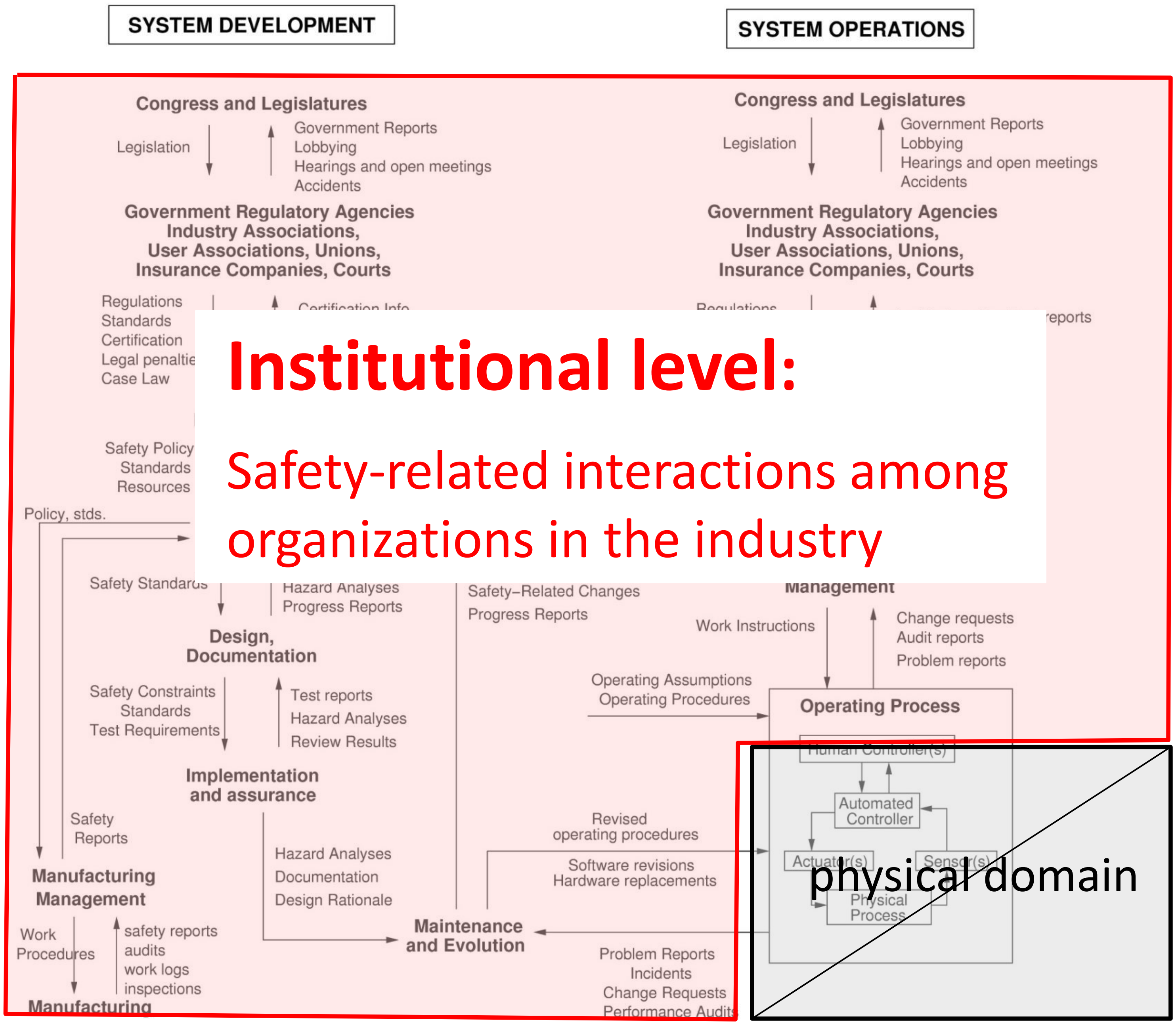
SM Candidate

MIT Engineering Systems Division

Systems Engineering Research Lab. (Aero. & Astr.)

Regional Transportation Planning and High-Speed Rail Research Group (CEE)

5/12/14 revision A



SYSTEM DEVELOPMENT
SYSTEM OPERATIONS
Congress and Legislatures
Legislation
Government Reports
Lobbying
Hearings and open meetings
Accidents
Government Regulatory Agencies
Industry Associations,
User Associations, Unions,
Insurance Companies, Courts
Regulations
Standards
Certification
Case Law
Safety Policy
Standards
Resources
Policy, stds.
Institutional level:
Safety-related interactions among organizations in the industry
Safety Standards
Hazard Analyses
Progress Reports
Safety–Related Changes
Progress Reports
Work Instructions
Change requests
Audit reports
Problem reports
Design,
Documentation
Safety Constraints
Standards
Test Requirements
Test reports
Hazard Analyses
Review Results
Operating Assumptions
Operating Procedures
Operating Process
Implementation and assurance
Safety
Reports
Revised operating procedures
Software revisions
Hardware replacements
Automated Controller
Hazard Analyses
Documentation
Design Rationale
physical domain
Manufacturing
Management
Work
Procedures
safety reports
audits
work logs
inspections
Maintenance and Evolution
Problem Reports
Incidents
Change Requests

Contents

- Motivation
  - Issue in the northeast corridor
  - Rail safety in the US
  - Institutional structure
- Research objectives
- Proposed Methodology (5 steps)
  - How to integrate CAST, STPA, and System Dynamics
- Conclusion

Contents

- Motivation
  - Issue in the northeast corridor
  - Rail safety in the US
  - Institutional structure
- Research objectives
- Proposed Methodology (5 steps)
  - How to integrate CAST, STPA, and System Dynamics
- Conclusion

● : High-speed rail (HSR) in operation [>155mph]

Source: UIC

American Recovery and Reinvestment Act of 2009 (ARRA)

- Economic stimulus package. $8B for HSR study and planning.

NEC: Northeast Corridor (Boston - DC)

Proposed corridors by FRA

Source : FRA vision for HSR 2009

Capacity Issue in NEC

Highly Congested

*volume/capacity > 95%

Highway Congestion

2002

2035

Source : Amtrak vision for NEC 2012

Capacity Issue in NEC

Acela Express

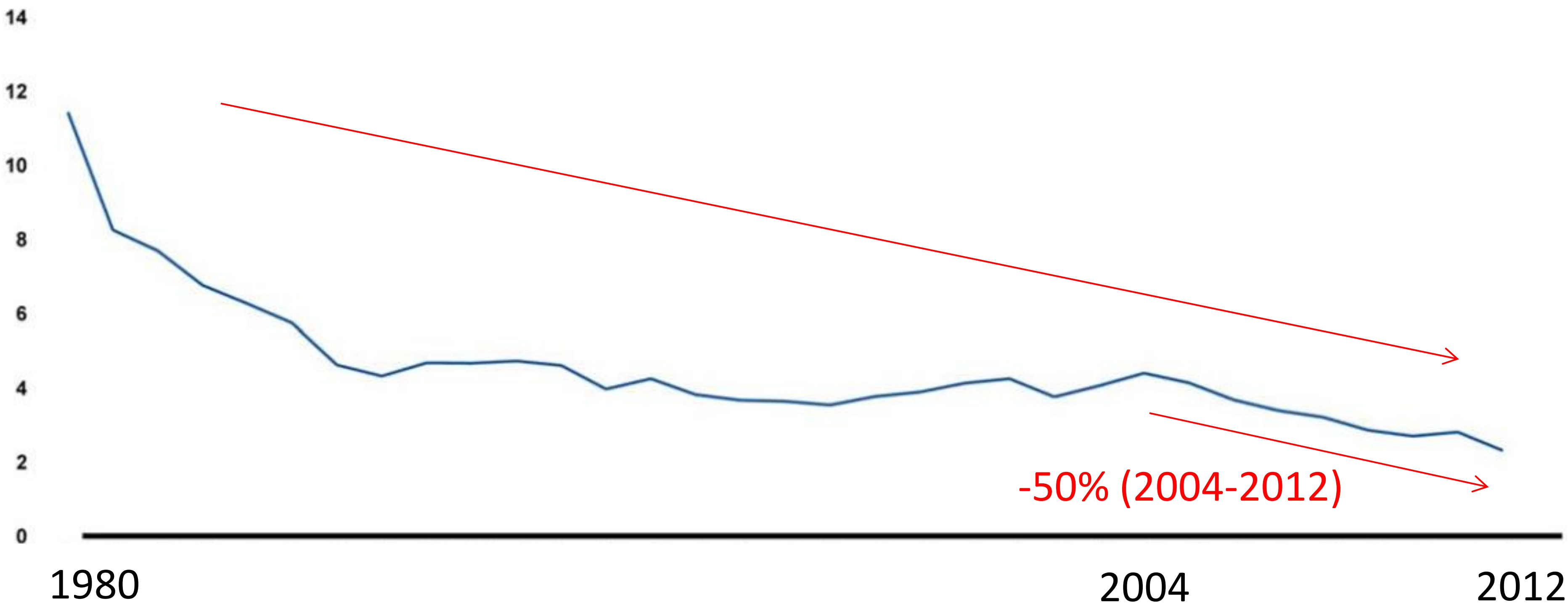
- Max. 240km/h (150mph)
- Ave. 135km/h (84mph)   due to poor condition of infrastructure

Source : Amtrak

Solution → new HSR

Rail Safety in the US

Train Accident Rate per Million Train Miles (US)



Source : FRA

However…

http://abcnews.go.com/US/train-derailment-ohare-airport-injures-32/story?id=23031525

source: wiki

source: wiki

...how safe?

Chinese HSR accident (2011)

http://www.democraticunderground.com/1002962288

http://www.telegraph.co.uk/travel/travelnews/10201894/Spanish-train-crash-the-quest-for-safer-rail-travel.html

Spanish HSR accident (2013)

...never happen in the US HSRs?

Key Safety Components for new HSRs in the US

1. Positive Train Control (PTC)
2. International-quality “service proven” trains
3. System Safety Program (SSP)

…but safe as a total system?

Institutional structure

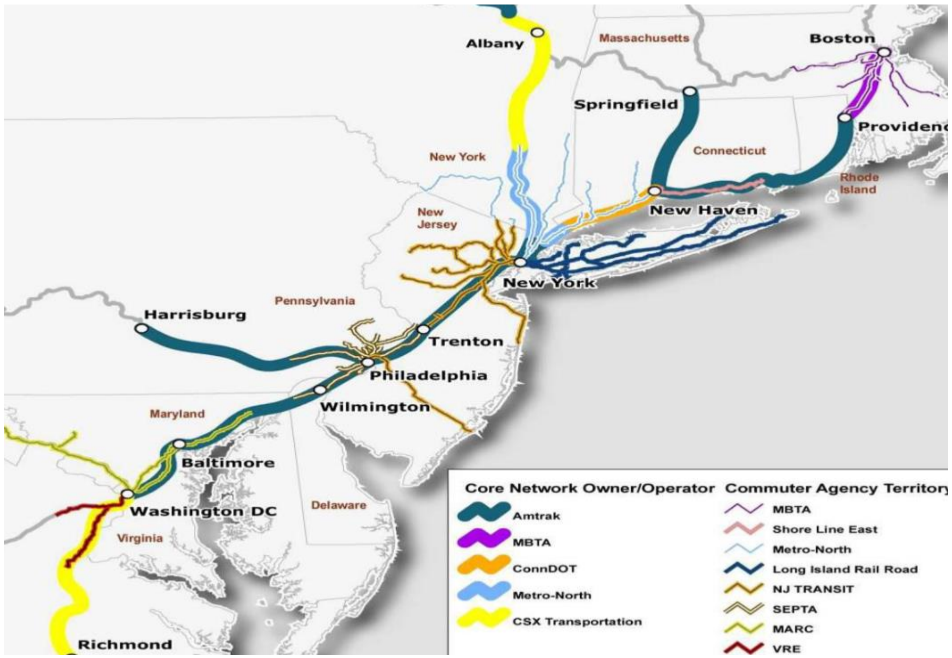
General key parameters

- Vertical structure : separation or integration
- Track : dedicated or shared
- Ownership : private or public
- Market Competition : yes or no

Different institutional structures require different safety constraints in the systems

Current NEC HSR

Source: NEC master plan



One of the most complex structures in the world

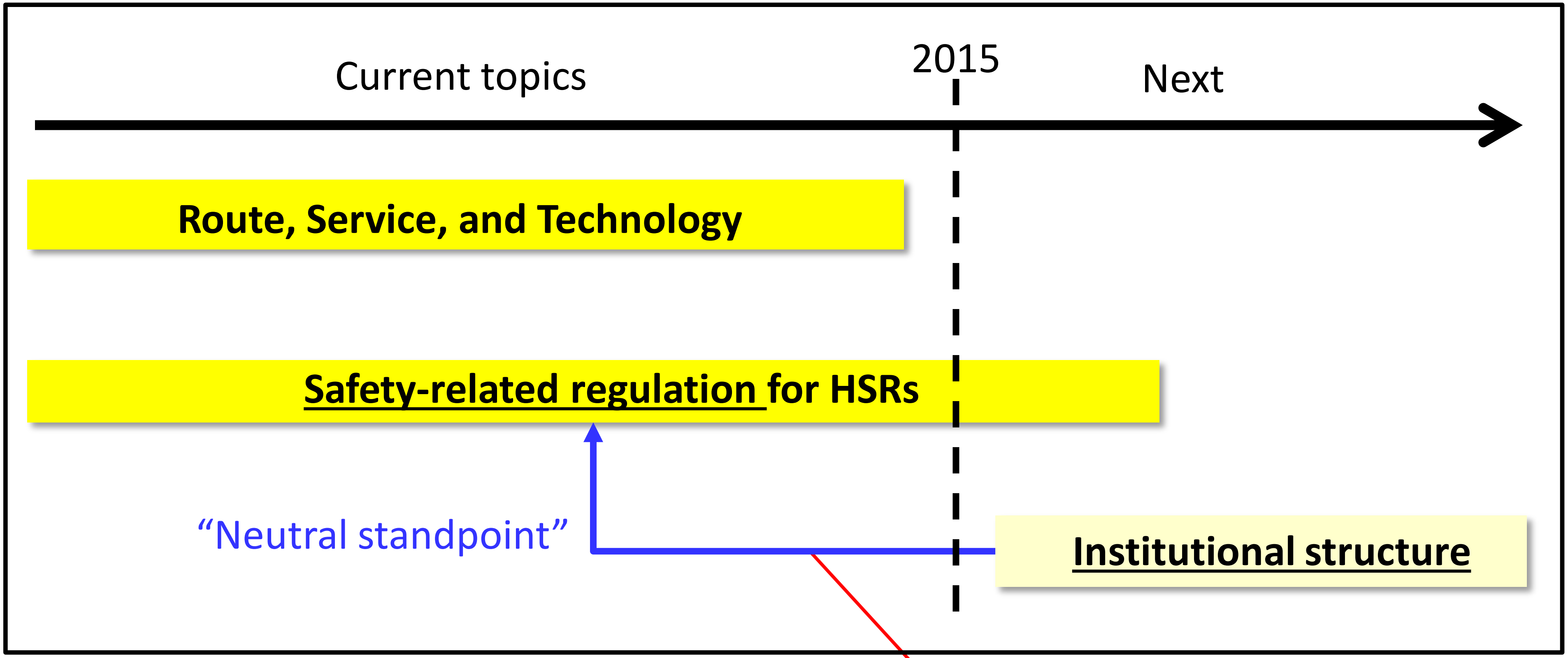
New NEC HSR

Many alternatives of institutional structures are currently discussed

However…

Issue in new NEC Design

Timeline of Project Design



Need to incorporate specific alternatives as safety-related factors?

Research Objectives

1. Develop a system-based safety risk analysis methodology based on lessons learned from past accidents for complex systems such as HSR systems

2. As a case study, the new HSR project in the NEC is analyzed by the proposed method with a specific focus on its institutional structure. The final goal of this research is to provide specific suggestions about safety management and regulation in the NEC HSR for project planners.

Contents

Identified requirements

- Based on system-based lessons, not a single cause, learned from past key accidents
- Analyze a complex sociotechnical system
- Focus on an institutional level
- Deal with many alternatives of institutional structures

Oh Yes! STAMP!

Key research papers

Paper 1:

Risk Management Approach for CO_2 Capture Project

(Samadi, 2012) **presented in STAMP workshop 2013*

Paper 2:

Risk Analysis of NASA Independent Technical Authority

(Leveson 2005, Dulac 2007)

Proposed Methodology

Step 1:
Accident analysis (CAST)

Step 2:
Control Model development
(generic model and alternatives)

Step 3:
Risk analysis (STPA)

Step 4:
Risk analysis (System Dynamics)

Step 5:
Organize results

Expected Research Output

1. Unsafe controls and their causal factors for each alternative of the NEC HSR. System requirements and safety constraints to prevent them.
2. Weaknesses of key safety regulations applied to the NEC HSR

These outcomes can be valuable for the actual institutional design process as important decision-making criteria.

Proposed Methodology

Step 1:
Accident analysis (CAST)

Step 2:
Control Model development (generic model and alternatives)

Step 3:
Risk analysis (STPA)

Step 4:
Risk analysis (System Dynamics)

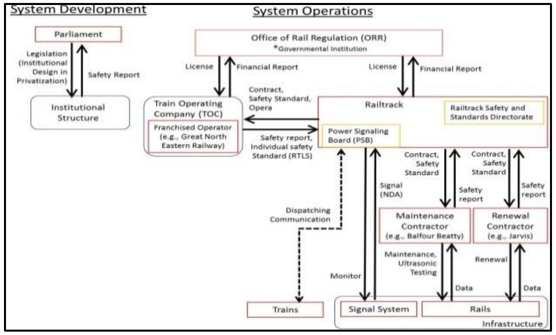
Step 5:
Organize results

Step 1: Accident Analysis (CAST)

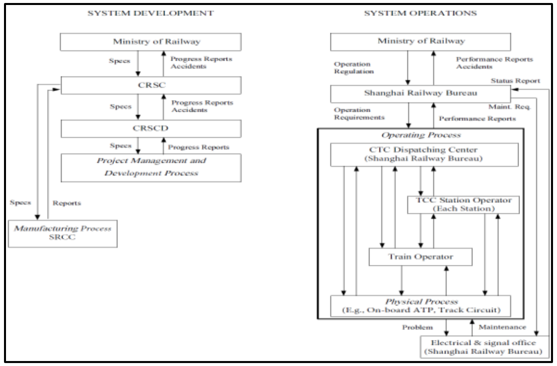
1) Choose accidents (Hatfield in UK, Wenzhou in China)
2) Develop their safety control models.
3) Identify inadequate controls, causal factors, and required constraints
4) Identify common safety constraints required at an institutional level

→ System-based lessons learned from past accidents

CAST
(UK)



CAST
(China)



Output of step1

system constraints

- Maintenance
  - …
- Train Operation
  - …
  - …
- Company management
  - …
  -

Proposed Methodology

Step 1:
Accident analysis (CAST)

Step 2:
Control Model development
(generic model and alternatives)

Step 3:
Risk analysis (STPA)

Step 4:
Risk analysis (System Dynamics)

Step 5:
Organize results

Step 2: Model development and gap analysis

1) Develop a generic HSR model.
2) Develop safety control models for three NEC alternatives.
3) Compare 1) with 2), and identify structural differences

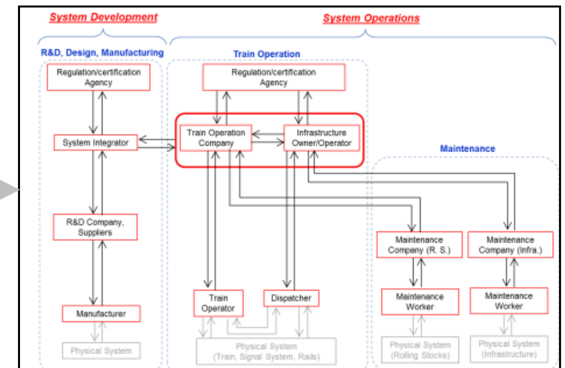
System definition (top-down)

Accidents
→System High level hazards
→ System requirements and constraints
- …
- …
- …
- …
- …
- …

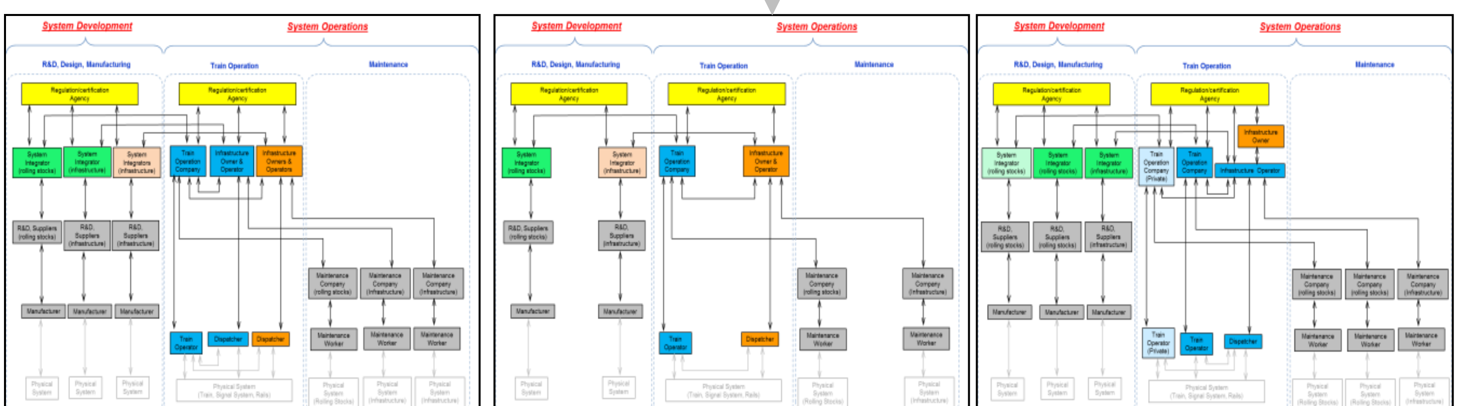
Input from step1

General railway industrial structure (simple)

Generic model

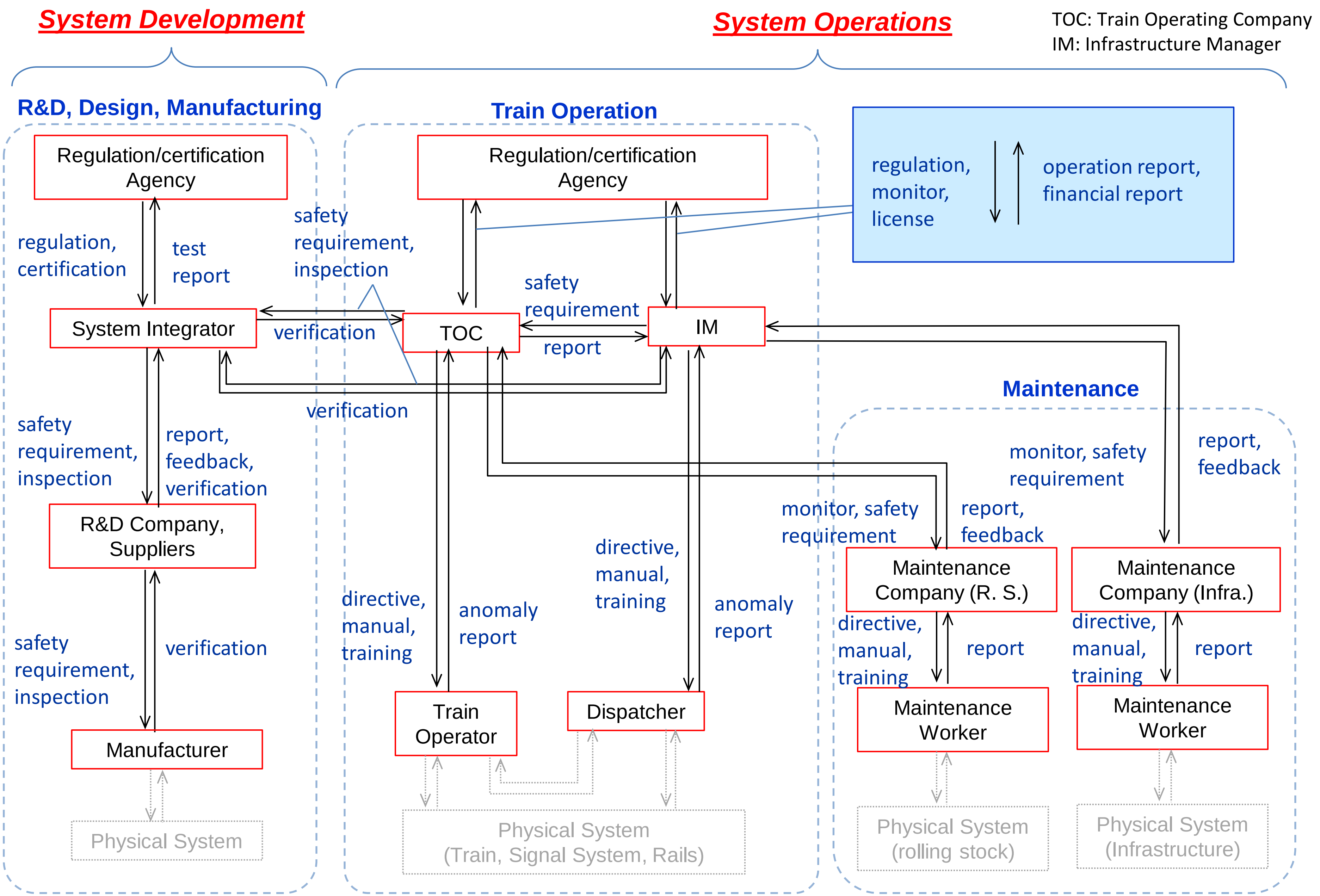


Paper, publication reviews



Alternatives 1-3 (NEC HSR - specific)

Generic HSR Model = base model



Preliminary Risk Analysis (Comparative Analysis)
[Generic vs. 3 NEC alternatives]

Clarify the impact of structural difference (=additional complexities, which could provide unsafe controls) on safety constraints

Requirements Constraints (+ lessons)

Generic vs. Alternative 1

Generic vs. Alternative 2

Generic vs. Alternative 3

System Requirements / Safety Constraints			Potential risks in Alternative 1 (Multi-ownership / Update)	Potential risks in Alternative 2 (Vertical Separation / New)	Potential risks in Alternative 3 (Open Access/New)
Domain	Major Categories	Detailed Items			
Train Operation	I. Safety-related technical and managerial decision-making and its implementation must be based on correct, complete, and up-to-date information, complying with state-of-the-art safety standards and regulations.	i. State-of-the art safety standards and regulation regarding train operation must be established, implemented, enforced, and maintained.			
		ii. Qualified third parties must develop the state-of-the art safety standards and regulations regarding train operation, being independent from programmatic aspects such as cost and schedule of the system development/operations and other stakes of other agencies. They must evolve safety standards and regulations as needed.			
		iii. A regulatory structure is necessary to monitor, evaluate, and certify safety-critical managerial decision-making and its implementation in train operation.			
		iv. Correct, complete, and up-to-date information about the physical system and train operation must be available and used in safety-related technical and managerial decision-making and its implementation in train operation. (lesson 2.1.5.4)			Having multiple TOCs could cause inadquate sharing of operation data and issues which could influence the safety of the other TOCs' opeareation.
	II. Safety considerations must be critical in technical and managerial decision-making and its implementation	i. Safety-related technical decision-making in train operation must be independent from programmatic considerations, including cost, schedule, and performance. (lesson 2.1.2.1)			Having market competition among multiple TOCs could make them more concerned with cost, schedule, and performance, which could lower the priority of safety.
		ii. Managerial decision-making in train operation must be appropriately done, taking into account the criticality of safety-related technical decision.			
		iii. Technical and managerial decision-making and its implementation in train operation must continuously pursue future improvement of the system safety based on safety-related data and experience acquired through train operation.(lesson 2.1.5.2)			Having multiple TOCs could cause inadquate sharing of operation data and issues which could be applied to the inprovement of the system safety, and disorganization of system safety improvement.
	III. Safety-related technical and managerial decision-making and its implementation must be done by qualified personnel and agencies	i. Technical decision-making in train operation must be credible (executed using credible personnel, technical requirements, and decision-making tools).	Partially vertically separated strcture could technical decision maker's acquisition of broad knowledge of the system, thereby lowering the credibility of the decision.	Vertically separated strcture could technical decision maker's acquisition of broad knowledge of the system, thereby lowering the credibility of the decision.	Partially vertically separated strcture could technical decision maker's acquisition of broad knowledge of the system, thereby lowering the credibility of the decision.
		ii. Technical decision-making in train operation must be clear and unambiguous with respect to authority, responsibility, and accountability.	Having multiple infrastructure operaters could cause ambiguous allocation of safety responsiblities.		
		iii. All safety-related managerial decisions in train operation, before being implemented, must have the approval of the technical decision-maker assigned responsibility for the technical decisions.			
		iv. Mechanisms and processes must be created that allow and encourage all employees and contractors to contribute to safety-related decision-making in train operation.	Having multiple infrastructure operaters and partially vertically separated structure could cause inefficient communication or miscommunication in the decision making process.	Vertically separated structure could cause inefficient communication or miscommunication in the decision making process.	Having multiple TOCs and partially vertically separated structure could cause inefficient communication or miscommunication in the decision making process.
		v. All operators involved in train operation must be well-trained enough to identify any system failure and to manage emergent situations. (lesson 2.1.2.1)			
		vi. The skill levels and experience levels of individual operator and financial/managerial capability of agencies involved in train operation must be evaluated, certified, and constantly-monitored.(lesson 2.1.5.1)	Having multiple infrastructure operaters could cause difficulty in managing the skills of the individual operator comprehensively.		Having multiple TOCs could cause difficulty in managing the skills of the individual operator comprehensively.
		i. High-quality system hazard analyses of train operation must be created.			
		ii. Personnel must have the capability to produce high-quality safety analyses.			
		iii. Engineers and managers must be trained to use the results of hazard analyses in their decision-making in train operation. (lesson 2.1.3.2)			
		iv. Adequate resources must be applied to the			

Proposed Methodology

Step 1:
Accident analysis (CAST)

Step 2:
Control Model development
(generic model and alternatives)

Step 3:
Risk analysis (STPA)

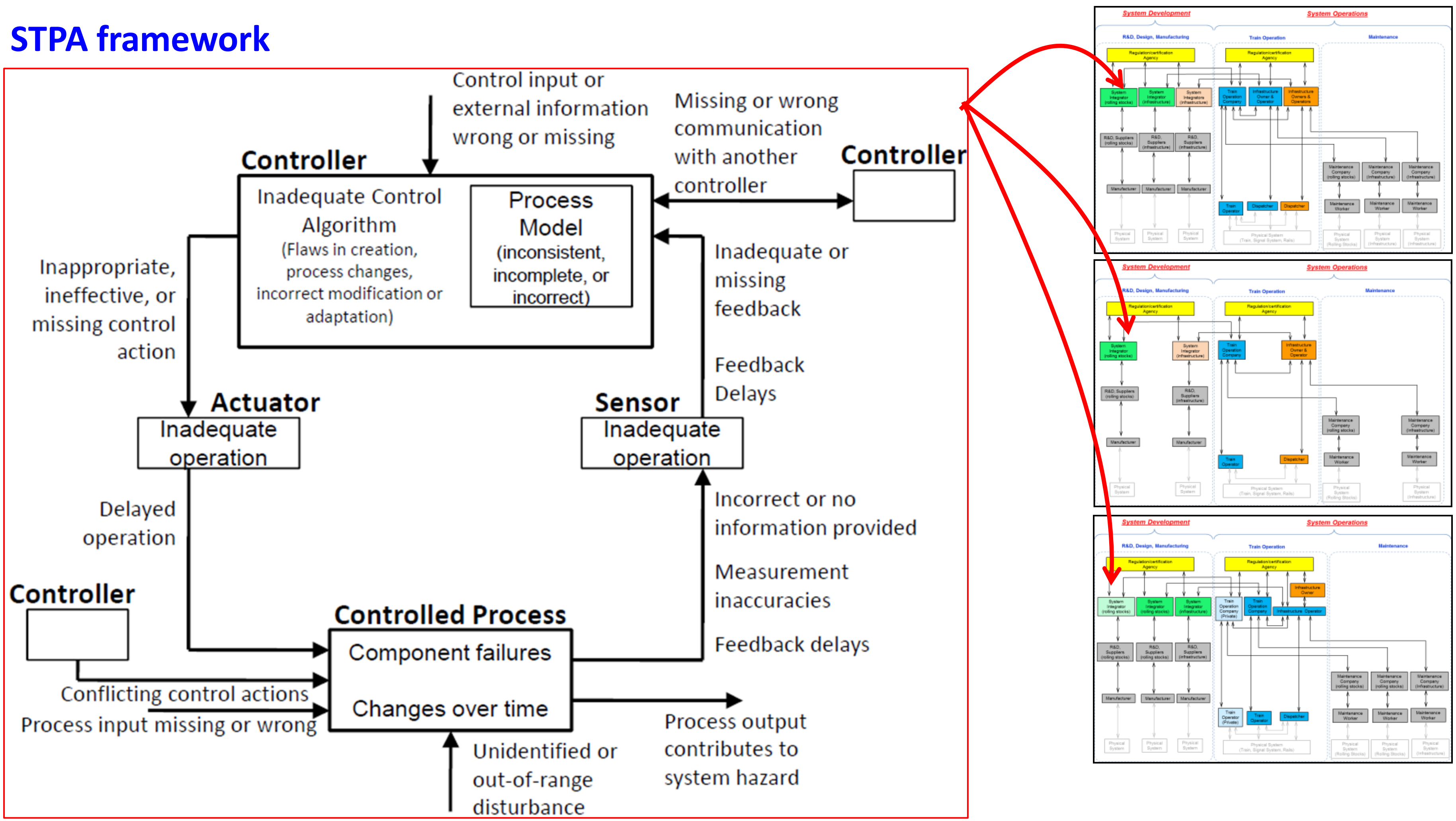
Step 4:
Risk analysis (System Dynamics)

Step 5:
Organize results

Step 3: Risk Analysis 1 (STPA of the NEC HSR)

1) Identify causes of hazards.
2) Identify causal factors, in the context of the actual NEC's approach

STPA framework



58 types of NEC-specific risks are Identified

Controller	Controlled Entity	Risk	Type of Causal Factor	Type of Risk	Alt. 1	Alt. 2	Alt. 3
Regulation/certification Agency	System Integrators (rolling stock, infrastructure) *Partilally applicble to Train Operating Company [Amtrak], Infrastructure Owners/Operators	1	Inadequate process model	General	x	x	x
		2	Incorrect process model	Immediate	x	x	x
		3	Inadequate decision making algorithm	General	x	x	x
		4	Inadequate feedback	Immediate	x	x	x
		5	Wrong input	General	x	x	x
		6	Wrong input	General	x	x	x
		7	Inadequate process model	General	x	x	x
		8	Inadequate process model	General	x	x	x
System Integrators (rolling stocks or infrastructure)	R&D Company/Suppliers (rolling stocks or infrastructure)	9	Inadequate process model	Immediate	x	x	x
		10	Inadequate input	Immediate	x	x	x
		11	Inadequate process model	Immediate	x	x	x
		12	Inadequate process model	General	x	x	x
		13	Missing input	Immediate	x	x	x
		14	Inadequate process model	General	x	x	x
		15	Inadequate control algorism	General	x	x	x
R&D Company/Suppliers (rolling stocks or infrastructure)	Manufacturers (rolling stocks or infrastructure)	16	Inadequate control algorism	General	x	x	x
		17	Missing input	General	x	x	x
		18	Process failure	Immediate	x	x	x
Regulation/certification Agency	Train Operating Company, Infrastructure Owners/Operators (or Infrastructure Owner and Infrastructure Operator)	19	Inadequate process model	General	x	x	x
		20-1	Inadequate control algorism	General	x		
		20-2	Inadequate control algorism	General		x	
		20-3	Inadequate control algorism	General			x
		21	Inadequate process model	General	x	x	x
Train Operating Company	Train Operator	22	Inadequate process model	General	x	x	x
		23	Inadequate feedback	General	x	x	x
		24	Conflicting control action	General	x		
	Maintenance Company (rolling stocks)	25	Inadequate feedback	Immediate	x	x	x
		26	Inadequate feedback and inadequate process model	Immediate	x	x	x
		54	Inadequate decision making algorithm	General			x
		27	Inadequate process model	Immediate	x	x	x
		28	Inadequate feedback	Immediate	x	x	x

Proposed Methodology

Step 1:
Accident analysis (CAST)

Step 2:
Control Model development
(generic model and alternatives)

Step 3:
Risk analysis (STPA)

Step 4:
Risk analysis (System Dynamics)

Step 5:
Organize results

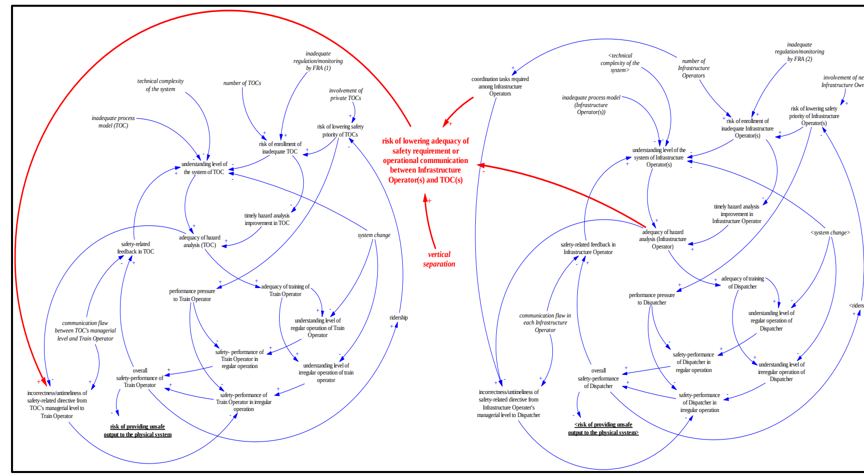
Why System Dynamics model?

- Integrate interrelated causal relations of some risks identified in STPA
- Incorporate indirect causal factors and impact of multiple changes within the entire safety control structure.
- Provide information about positive/negative feedback loops in causal relations (dynamic behavior)
- Help understand causal relation visually

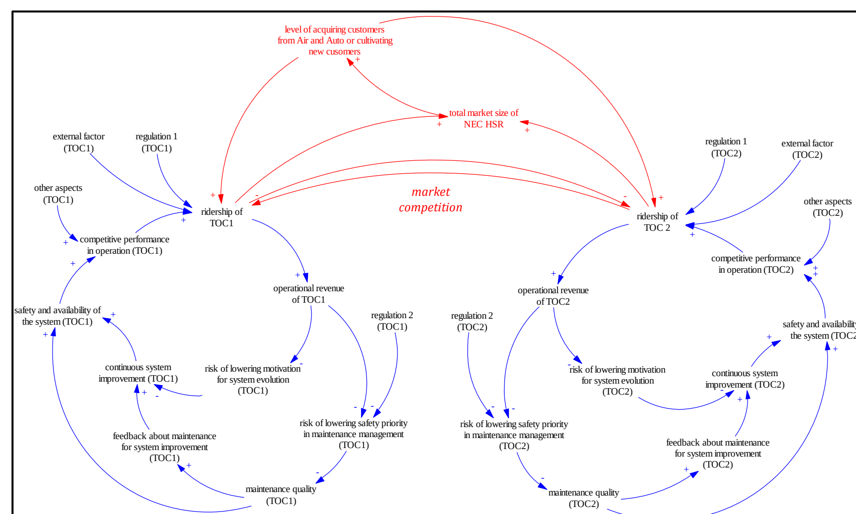
Step 4: Risk Analysis 2 (SD-based analysis of the NEC HSR)

1) Develop a System Dynamics model, integrating the causal relations of the key risks identified in Step 3.
2) Analyze the detailed causal relations.

Risk 23, 24, 33, 34, 37, and 58 → **Focus 1: Coordination in operation**



Risk 39, 53, and 54 → **Focus 2: Market competition**



Proposed Methodology

Step 1:
Accident analysis (CAST)

Step 2:
Control Model development
(generic model and alternatives)

Step 3:
Risk analysis (STPA)

Step 4:
Risk analysis (System Dynamics)

Step 5:
Organize results

Step 5: Organize the results

Discuss weaknesses of regulations applied to the NEC HSR.

- System Safety Program (49 CFR 270, proposed rule in 2012)
- Passenger Equipment Safety Standard ("certification", 49 CFR 283.111)
- Buy American Act (41 U.S.C. §§ 8301–8305)
- Etc.

E.g., System Safety Program (49 CFR Part 270, proposed rule in 2012)

No.	SSP Items	Weaknesses
1	Purpose and scope of system safety program	
2	System safety program goals	
3	Railroad system description	Risk * could be ...
4	Railroad management and organizational structure	
5	System safety program implementation plan	
6	Maintenance, inspection and repair program	
7	Rules compliance and procedures review	Risk * and ** are not conciderd ...
8	System safety program employee/contractor training	
9	Emergency management	
10	Workplace safety	

+ Prioritize risks and design safety constraints (in practice)

Conclusion

- Developed a STAMP-based risk analysis methodology with a specific focus on past accidents' lessons and institutional structures.
- As a case study, the HSR project in the NEC is analyzed. Three alternatives of the institutional structure are taken into account. As a result,
  - 58 NEC-specific risks are identified in STPA.
  - With SD model, their causal relations are further analyzed.
  - Several weaknesses of regulations for HSR systems are identified.

This research suggests that project planners for the NEC HSR adopt this methodology and analyze risks with experts from diverse organizations involved in the project, thereby harmonizing risk managements performed by these diverse organizations in a consistent way.

Questions?

Soshi Kawakami
soshi@mit.edu

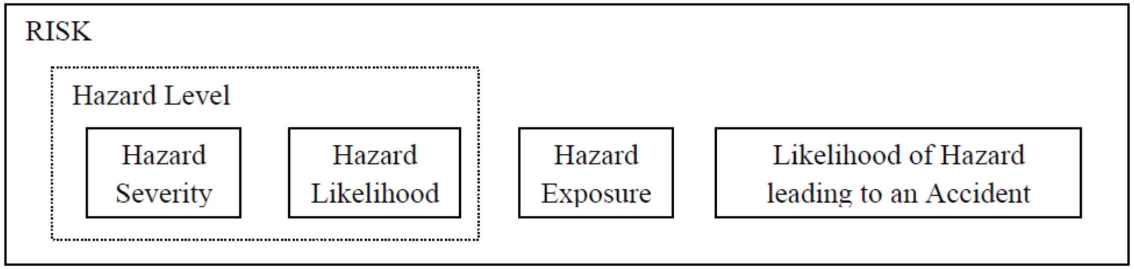
Terminology

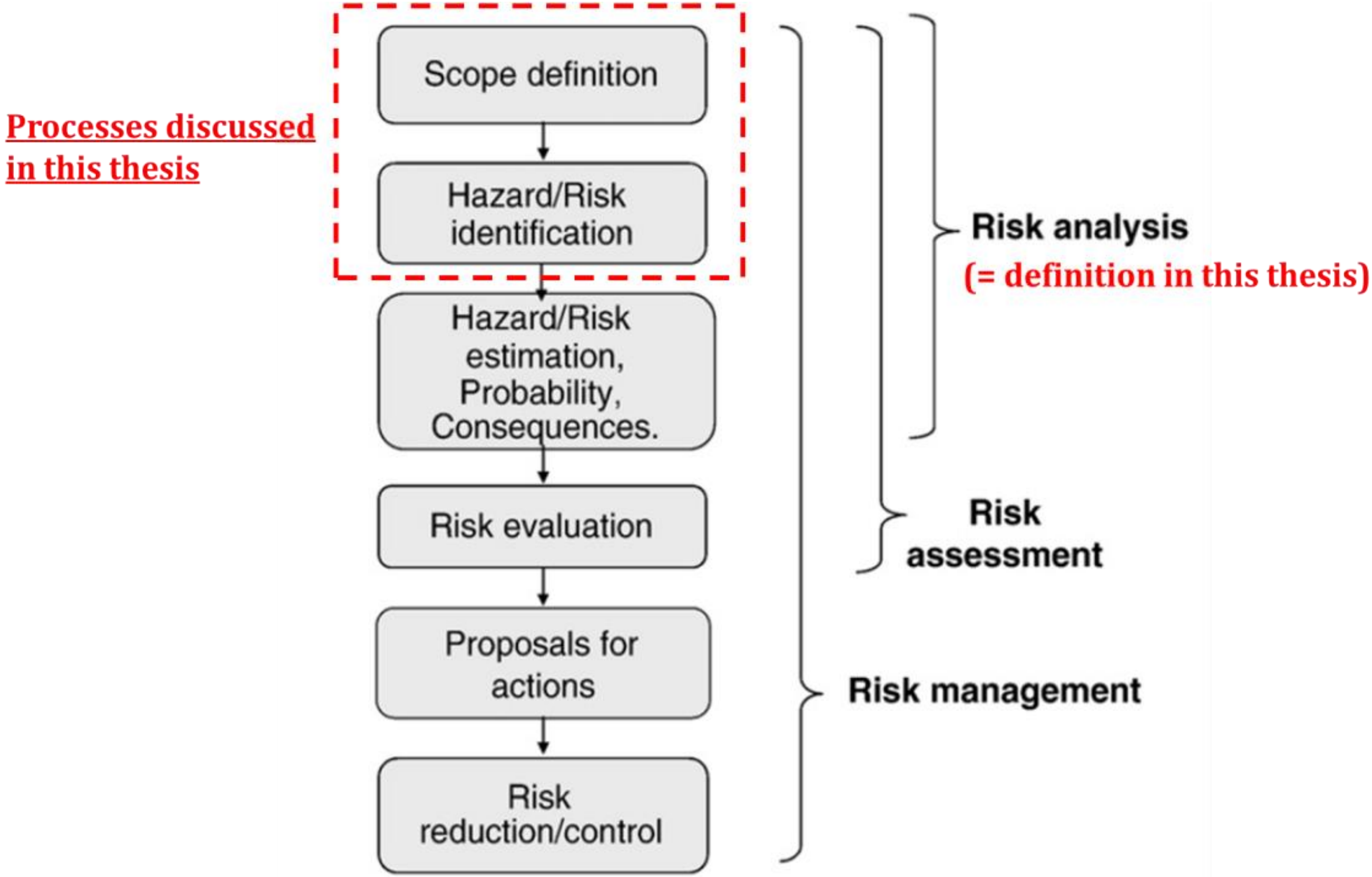
Accident: An undesired and unplanned event that results in loss of human life or human injury.

Hazard: A system state or set of conditions that, together with a particular set of worst-case environmental conditions, will lead to an accident (loss)

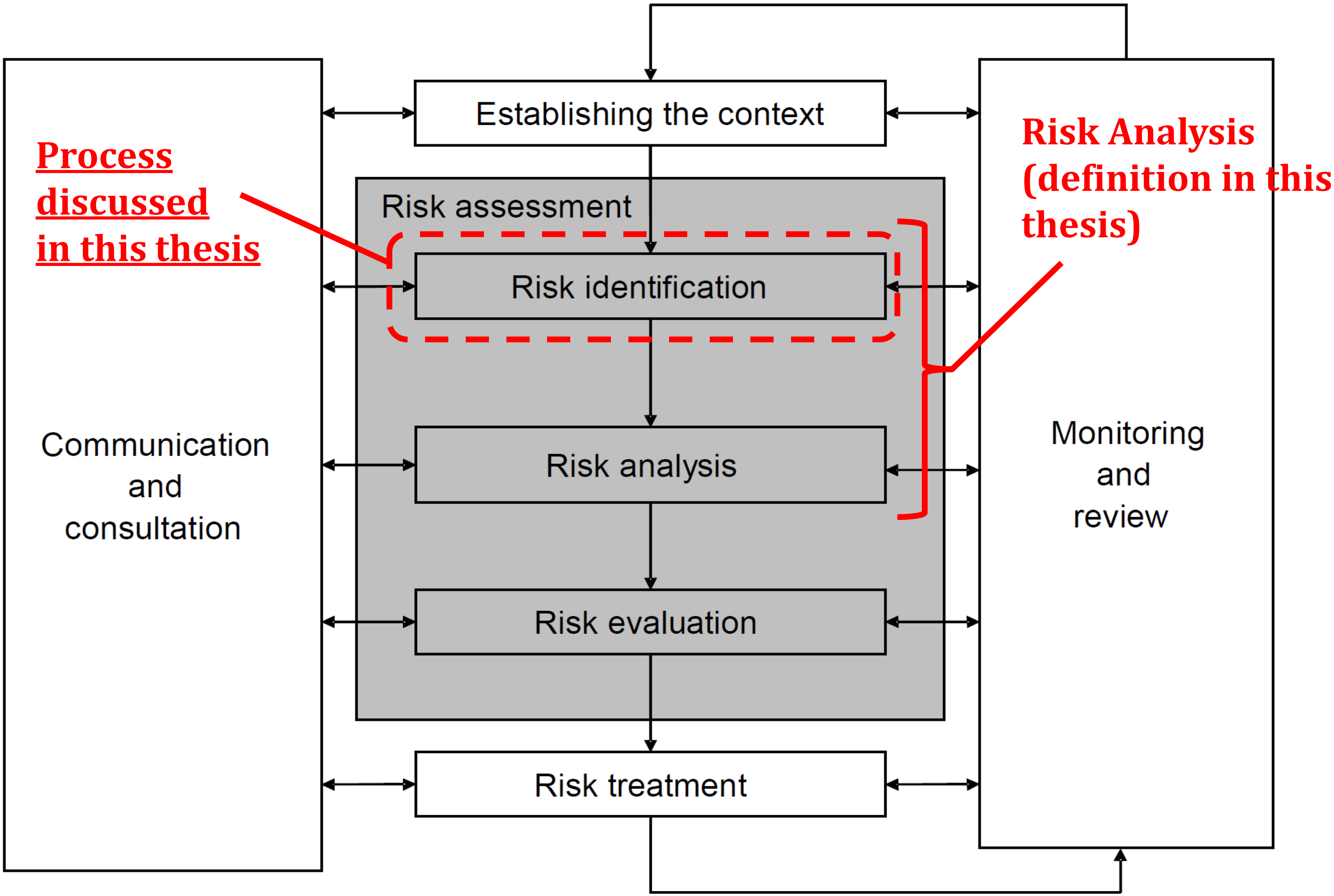
Risk: Risk is the hazard level combined with the likelihood of hazard leading to an accident (sometimes called danger) and hazard exposure or duration (sometimes called latency) . Specifically, this research refers to a system state that has an *unsafe control action(s)* and its *causal factor(s)* identified in the context of the actual NEC HSR's situation, which could lead to an accident, as a safety *risk* of the NEC HSR

Safety: The freedom from accidents or losses



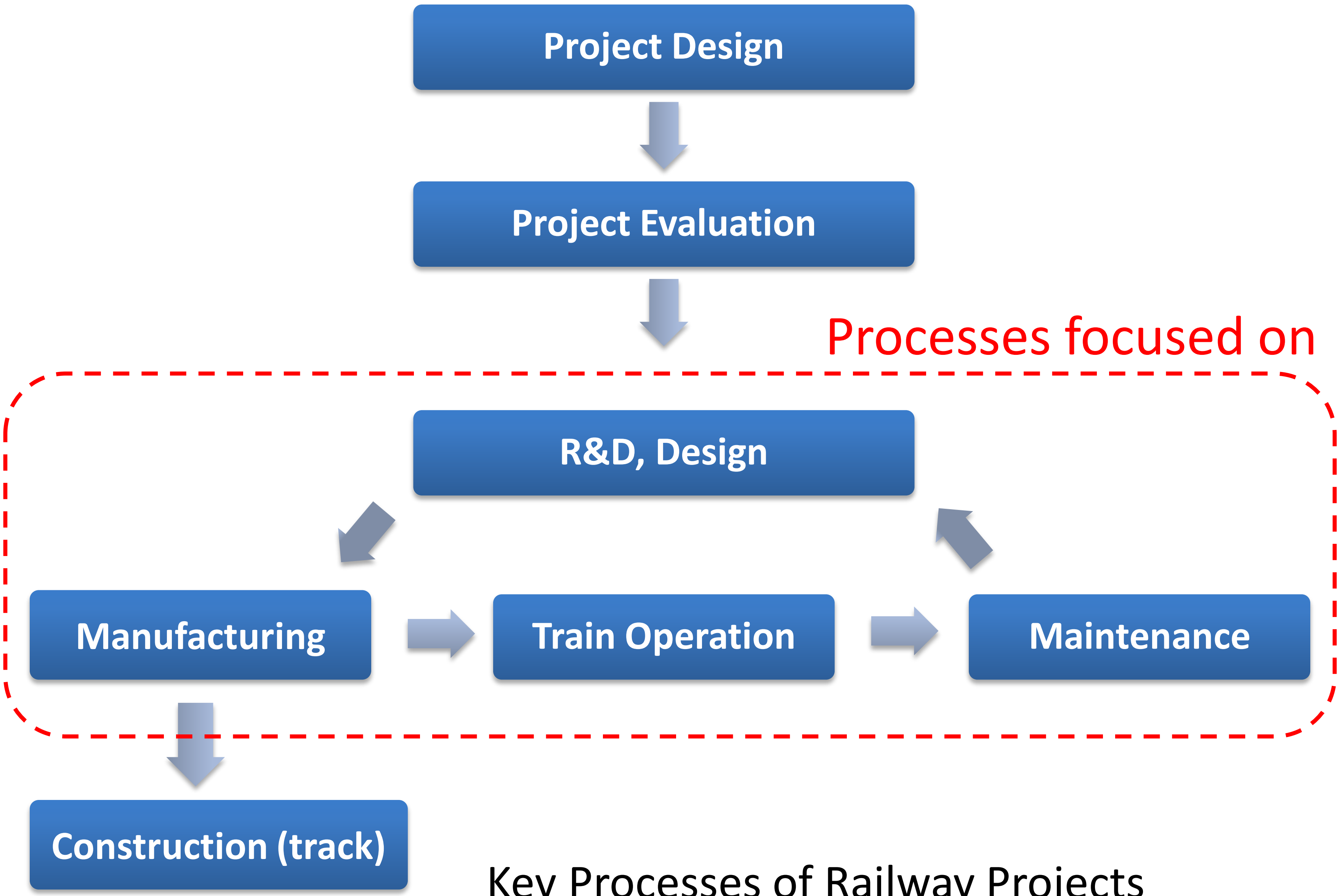


Discussed processes in this thesis as risk analysis, in the context of ISO 60300-3-9

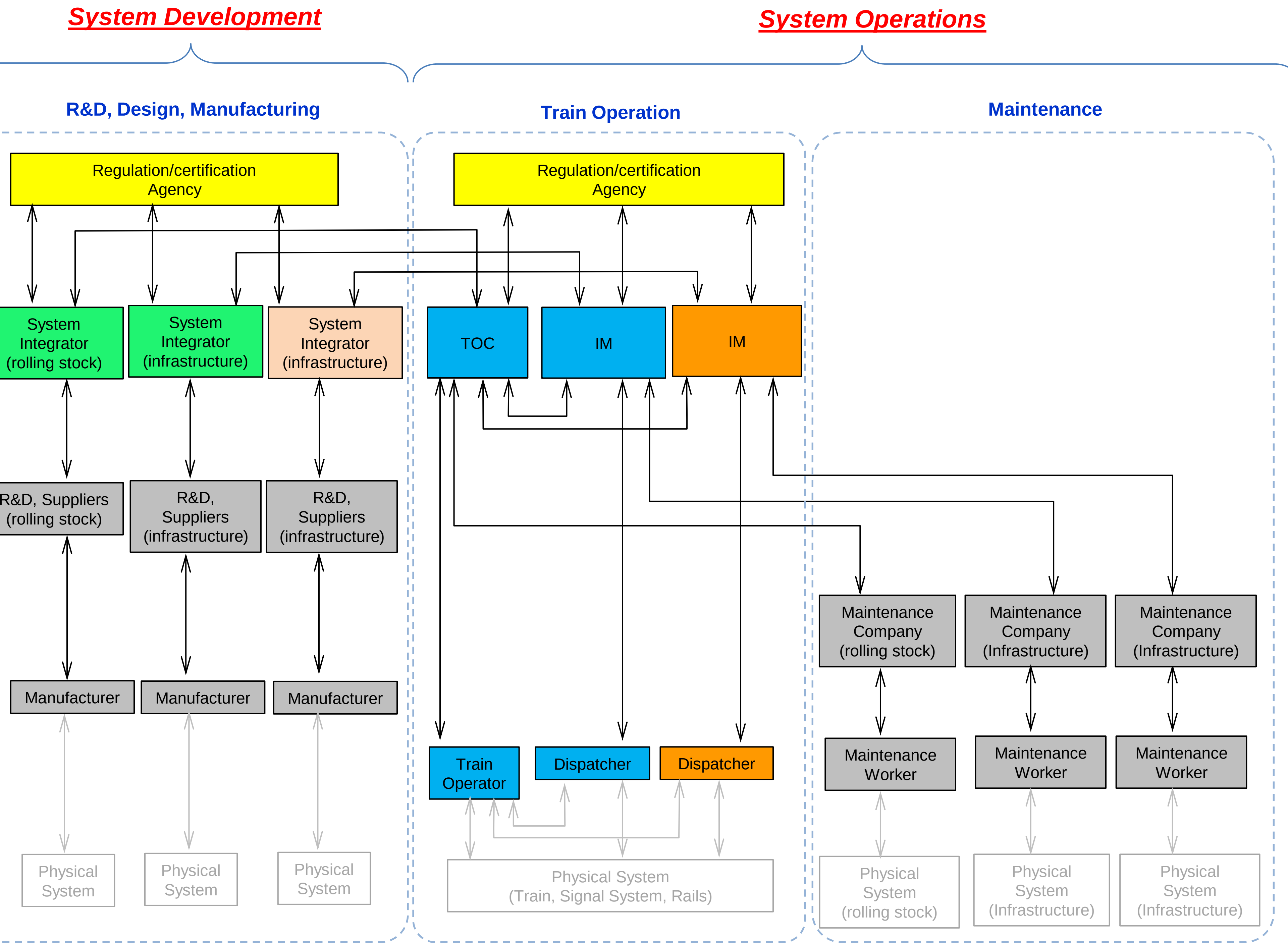


ISO 31000 (2009)

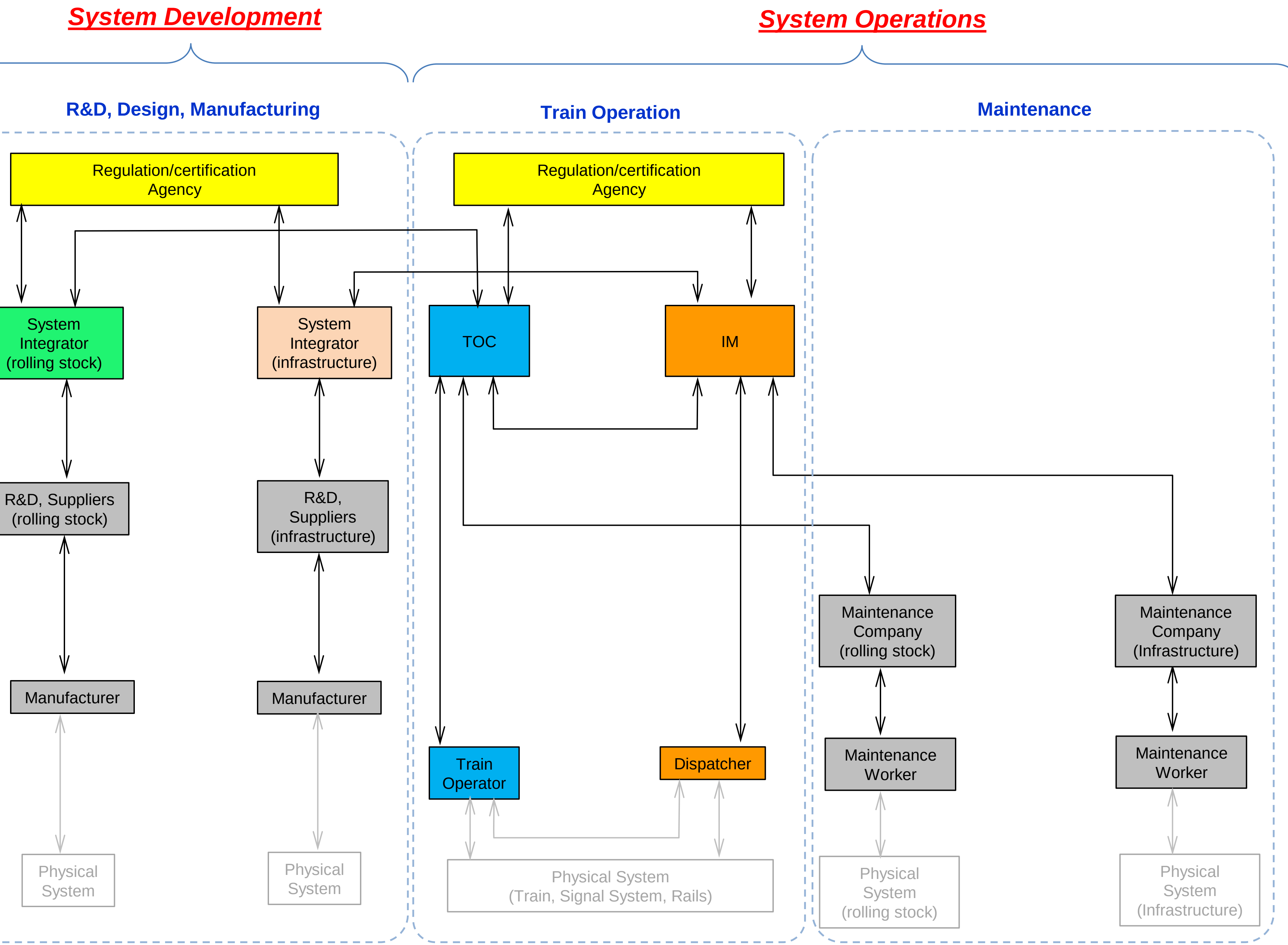
Model development : processes focused on

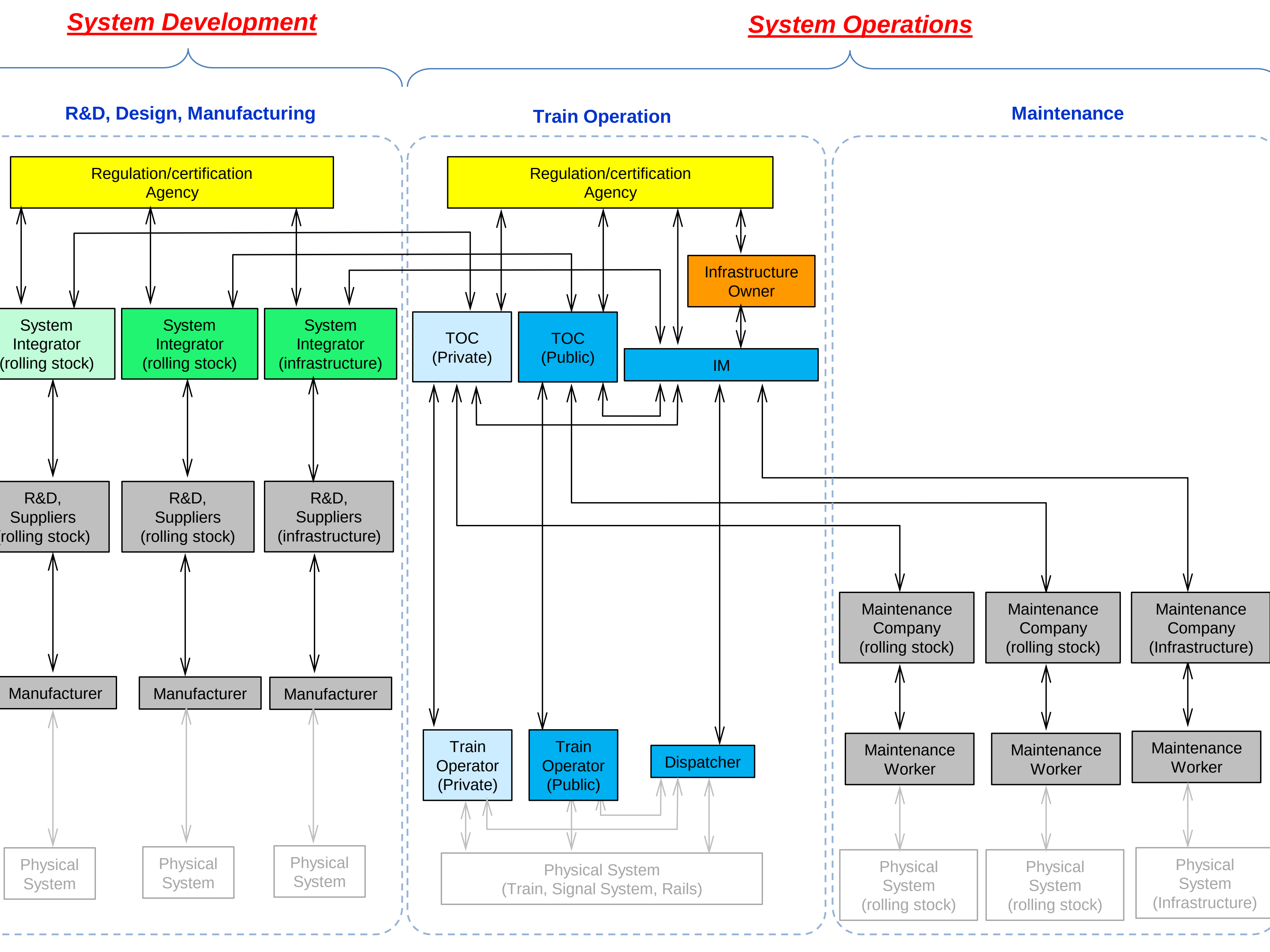


Key Processes of Railway Projects



System Development
System Operations
R&D, Design, Manufacturing
Train Operation
Maintenance
Regulation/certification Agency
Regulation/certification Agency
System Integrator (rolling stock)
System Integrator (infrastructure)
System Integrator (infrastructure)
TOC
IM
IM
R&D, Suppliers (rolling stock)
R&D, Suppliers (infrastructure)
R&D, Suppliers (infrastructure)
Maintenance Company (rolling stock)
Maintenance Company (Infrastructure)
Maintenance Company (Infrastructure)
Manufacturer
Manufacturer
Manufacturer
Train Operator
Dispatcher
Dispatcher
Maintenance Worker
Maintenance Worker
Maintenance Worker
Physical System
Physical System
Physical System
Physical System (Train, Signal System, Rails)
Physical System (rolling stock)
Physical System (Infrastructure)
Physical System (Infrastructure)


System Development
System Operations
R&D, Design, Manufacturing
Train Operation
Maintenance
Regulation/certification Agency
Regulation/certification Agency
System Integrator (rolling stock)
System Integrator (infrastructure)
TOC
IM
R&D, Suppliers (rolling stock)
R&D, Suppliers (infrastructure)
Manufacturer
Manufacturer
Maintenance Company (rolling stock)
Maintenance Company (Infrastructure)
Train Operator
Dispatcher
Maintenance Worker
Maintenance Worker
Physical System
Physical System
Physical System (Train, Signal System, Rails)
Physical System (rolling stock)
Physical System (Infrastructure)



System Development
System Operations
R&D, Design, Manufacturing
Train Operation
Maintenance
Regulation/certification Agency
Regulation/certification Agency
Infrastructure Owner
System Integrator (rolling stock)
System Integrator (rolling stock)
System Integrator (infrastructure)
TOC (Private)
TOC (Public)
IM
R&D, Suppliers (rolling stock)
R&D, Suppliers (rolling stock)
R&D, Suppliers (infrastructure)
Maintenance Company (rolling stock)
Maintenance Company (rolling stock)
Maintenance Company (Infrastructure)
Manufacturer
Manufacturer
Manufacturer
Train Operator (Private)
Train Operator (Public)
Dispatcher
Maintenance Worker
Maintenance Worker
Maintenance Worker
Physical System
Physical System
Physical System
Physical System (Train, Signal System, Rails)
Physical System (rolling stock)
Physical System (rolling stock)
Physical System (Infrastructure)