Extending STPA Hazard Analysis Guidance to Interactions with Human

TOYAMA Keisuke, MIHARA Yukihiro

Software Reliability Enhancement Center
Information-technology Promotion Agency, Japan

KAWANO Takashi

Railway Operation Headquarters,
East Japan Railway Company

KANEMOTO Shigeru

The University of AIZU

Contents

- Background and activities at IPA/SEC
- A motivating accident case
- Approach for an augmented guidance
- Analysis for a safety design
  - in two cases
- Results
- Conclusion

IPA and IPA/SEC

- **Information-technology Promotion Agency, Japan (IPA)**

  Incorporated Administrative Agency

  Working with the Ministry of Economy, Trade and Industry (METI)

- **Established** in 1970, reorganized in 2004

- **Realize a "Reliable IT Society"**

- **Software Reliability Enhancement Center (SEC)**
  - **Founded :** Oct. 1, 2004
  - **Mission :** IPA/SEC contributes to better living with IT in a smart society by implementing safety and security in systems

Background and activities at IPA/SEC

- **Growing expectations to STAMP/STPA for software controlled complex systems**
  - Risks or vulnerabilities in software centric systems can be effectively analyzed using STPA
  - Safety as well as reliability weighs heavily with advances of systems using automatic control

  IPA/SEC is promoting STAMP as a design tool or an evaluation method for advanced safety standard

- **Utilizing STPA more efficiently to software centric systems with human interactions**

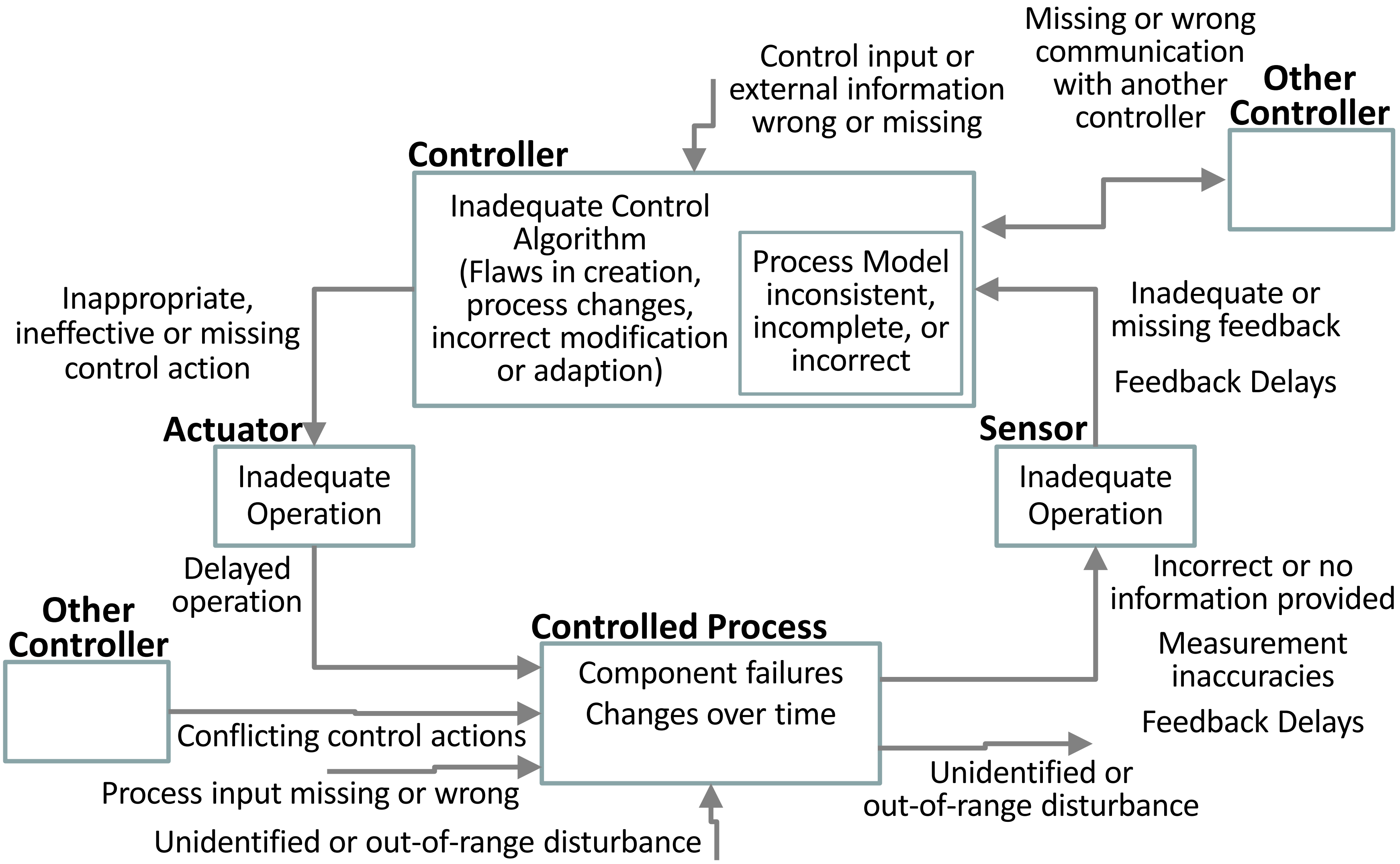
  To get "hint words" that identify HCFs (Hazard Causal Factors)

  - Help find more HCFs that are not foreseen
  - For analysts who are not experts of the target domain
  - Human errors of operators should be analyzed

Characteristics of systems that require safety analysis

- **Human, machine and organization operate cooperatively in critical socio-tech systems**
  - Advanced automated manufacturing site using robots
  - Aircrafts and trains with autopilot systems, Near-autonomous cars
  - Remote controlled or highly automatized construction equipment
- **New, unpredictable risks may occur by mutual interactions between human, machine with software and organization**
- **Existing guidance is rather dedicated to machines and generic**
- **Additional guidance for potential hazard causal factors by human and organization to accidents would be useful**

Classification of Control Flaws to Hazards
- A guidance for identifying HCFs -



Control input or external information wrong or missing

Missing or wrong communication with another controller

Other Controller

Controller

Inadequate Control Algorithm (Flaws in creation, process changes, incorrect modification or adaption)

Process Model inconsistent, incomplete, or incorrect

Inappropriate, ineffective or missing control action

Inadequate or missing feedback

Feedback Delays

Actuator

Inadequate Operation

Sensor

Inadequate Operation

Delayed operation

Other Controller

Controlled Process

Component failures

Changes over time

Incorrect or no information provided

Measurement inaccuracies

Feedback Delays

Conflicting control actions

Process input missing or wrong

Unidentified or out-of-range disturbance

Unidentified or out-of-range disturbance

A motivating accident case

- **Conflicts in rules and improper actions in organizations caused an aviation accident**

  Überlingen mid-air collision

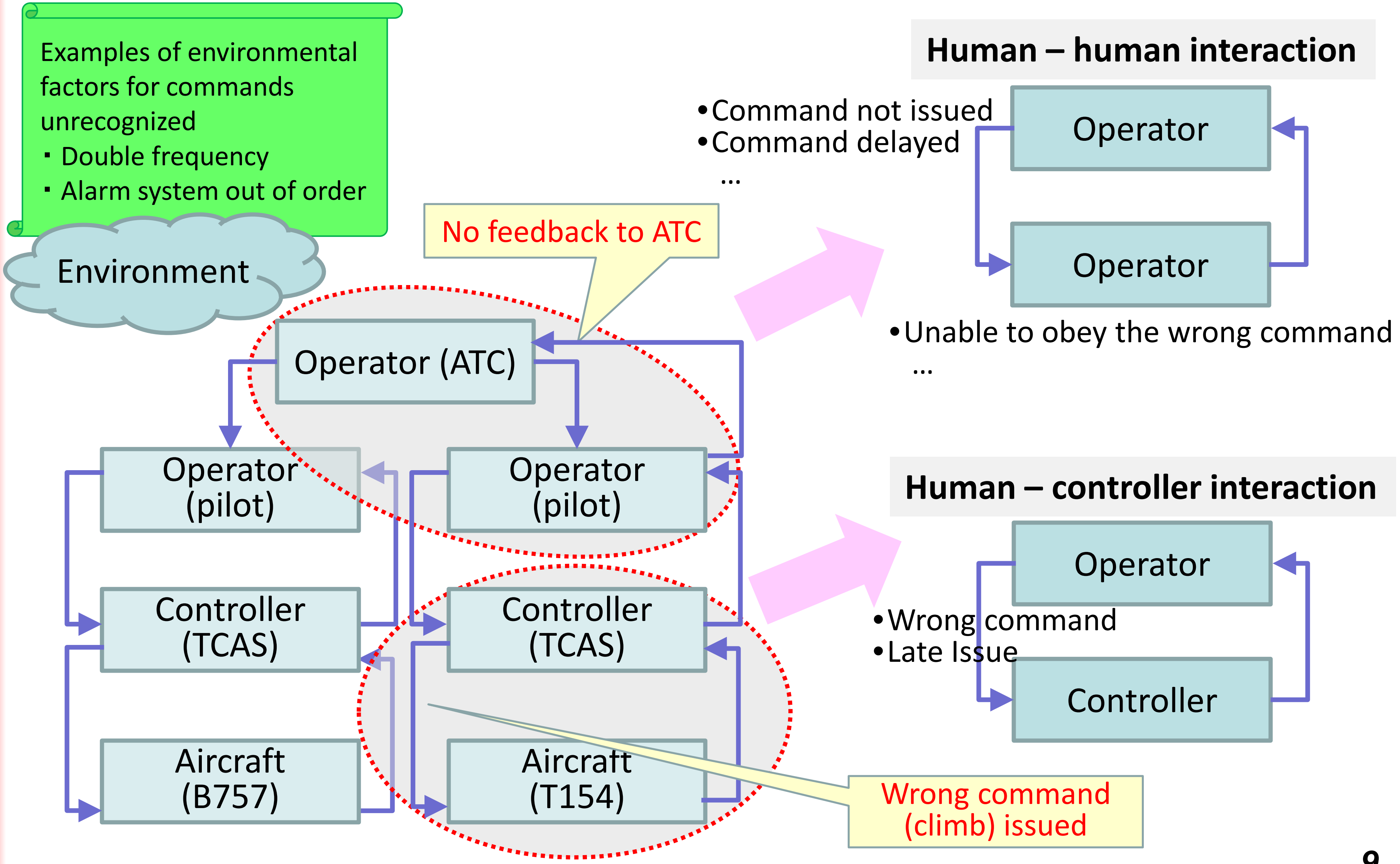
  - On 1 July 2002, a passenger jet (T154) and a cargo jet (B757) collided in mid-air over the southern German town.
    All 71 passengers and crew members aboard were killed
  - The main cause of the collision :
    - A number of shortcomings on the part of the Swiss air traffic control service in charge of the sector involved, and
    - Ambiguities in the procedures regarding the use of TCAS, the on-board aircraft collision avoidance system

Analysis for the accident case

Causes of the accident

- Single man operation, Downgraded Radar/ Phone System, Dual Frequency Responsibility, Alarm system out of operation
  - Unaware of the near-miss, which delayed prompt recovery
- After the pilots were alerted to the collision, TCAS instructed B757 pilot to descend and T154 pilot to climb.
  However, T154 had already been instructed by the ATC (air traffic controller) to descend
- ATC had no information about TCASs' instructions and T154 failed to notice ATC of its behavior because of a frequency trouble
  - ATC was not aware that the two aircrafts were both descending

Control structure and HCFs



Examples of environmental factors for commands unrecognized
- Double frequency
- Alarm system out of order

No feedback to ATC

Wrong command (climb) issued

Human – human interaction

- Command not issued
- Command delayed

…

- Unable to obey the wrong command

…

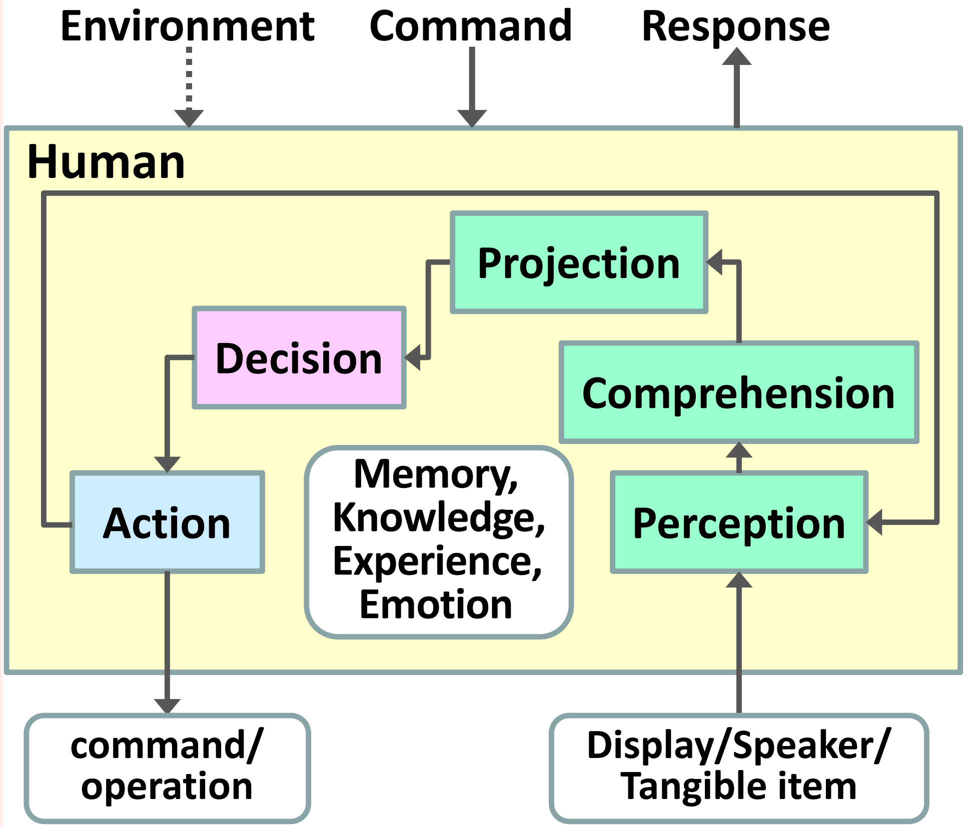
Human – controller interaction

- Wrong command
- Late Issue

Approach for an augmented guidance

- **Human information model and error type classification**
  - **Exhaustivity**
    Like the four types for UCAs
    (Not providing / providing / too early … / too long …)
  - **Systems view for human**
    - Biological characteristic
    - Physiological characteristic
    - Situation awareness
- **Establish "Hint words" for human-controller from small cases**
- **Expand them to human and organization’s interaction**

Adding Human Factors to Hazard Analysis
- Human Controller model -



- **Existing human information processing model and human error classification**
  - **Kuroda's human information processing model,**
    Endsley's situation awareness model, ...

    "Perception", "Comprehension", "Decision", "Action"

    "Memory", "Knowledge", "Experience", "Emotion"
  - **m-SHEL model**

    "Software", "Hardware", "Environment", "Liveware", "Management"

Error classification for human HCFs

Classification of human errors

	Omission	Commission
Perception	Overlook, Fail to hear	Misseeing, Mishearing
Comprehension	Lack of confirmation/ awareness	Underestimation
Projection	Forget remembering Lack of prediction/consideration	Misunderstanding Wrong/under estimation
Decision	Wrong decision, Sabotage	**Lapse**, Deviation
Action	Forget to do	**Slip**, **Mistake**, Violation

Contributing Factors

- For individual
- From background

Contributing Factors
- to conceive human error causes -

Individual factor	
Pathological **Pharmaceutical**	
Physiological	Fatigue, Circadian rhythm, …
Physical	User interface, …
Psychological	Impatience, Carelessness, …
Psychosocial	Psychological stress, …

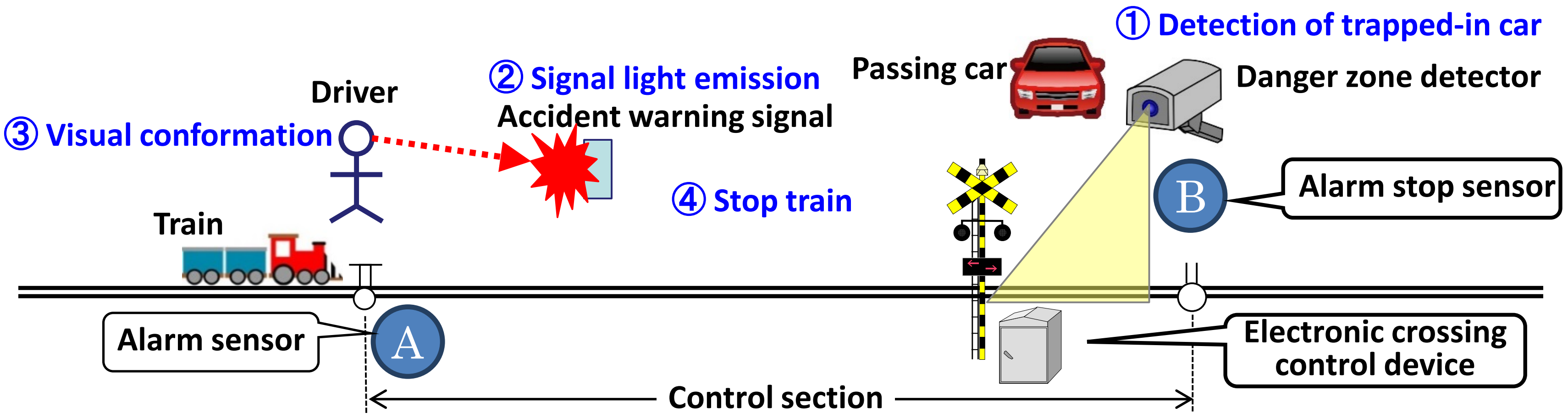
Background factor	
Software	Defects in requirements
Hardware	Defects in equipment
Environment	Noise, habit, …
Liveware	Mis/inadequate communication, …
Management	Problems in organization, Commitment, …

Analysis for a safety design (1)

Detection of obstacles trapped in a railroad crossing

- A system or function that notifies train driver of obstacles (cars) trapped in a railroad crossing in order that the driver stops the train to ensure safety of the crossing

		Behavior of equipment	Human process or operation	notes
1	occurrence	Detection of a car passing	—	
2	action	The accident warning signal emits light	The driver recognizes the signal	Visual observation
3	action	— 〃 —	The driver makes a break	Manual break



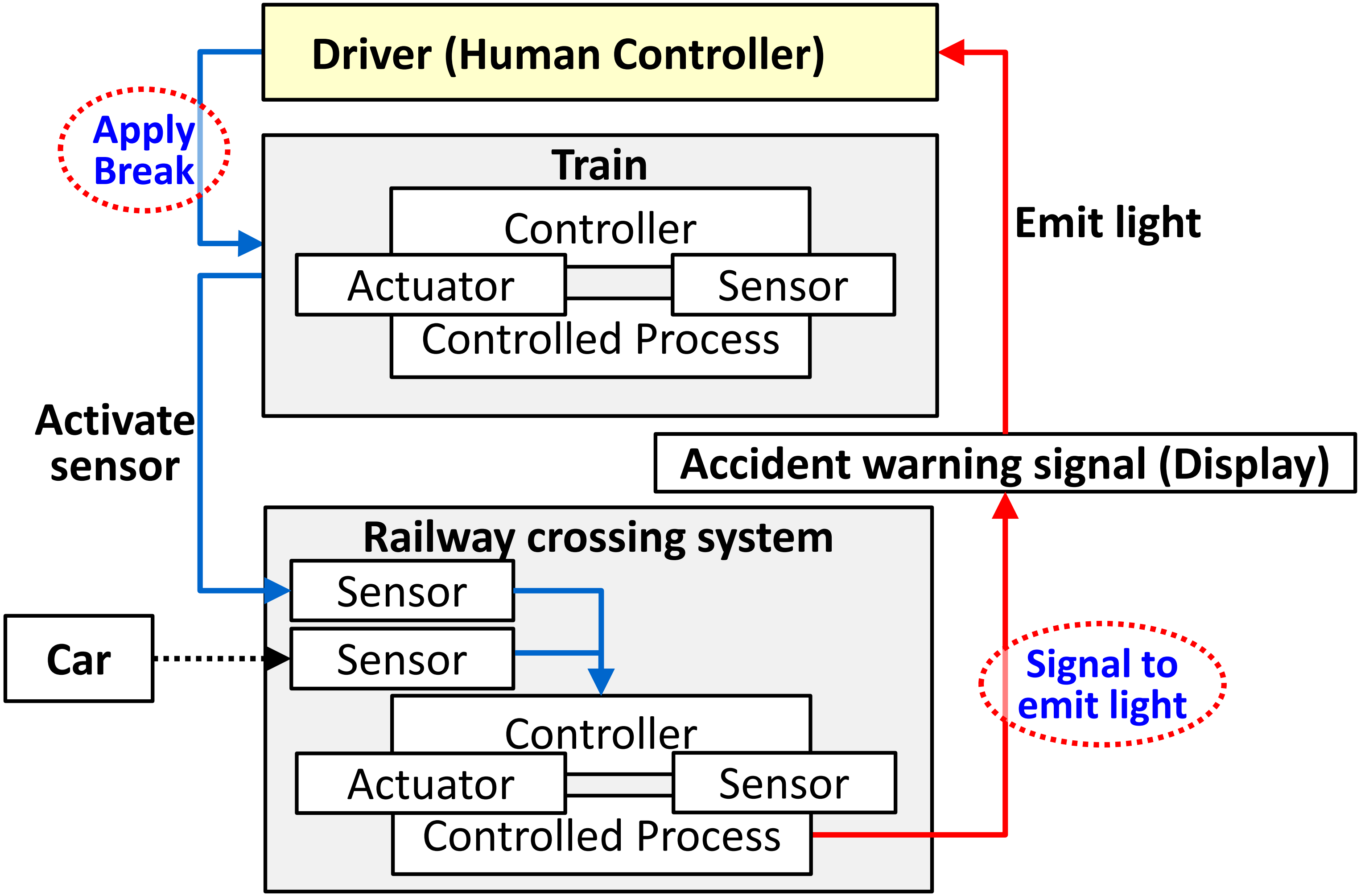
Preparation 1

Identifying Safety Constraints

Loss	Hazard	Safety Constraints
(A1) A train collides with a "trapped-in" car • The driver of the collided car is killed or wounded • Crews and passengers of the train are killed or wounded	(H1) The accident warning signal does not emit light when "trapped-in" has occurred	（SC1) The accident warning signal emits light when "trapped-in" has occurred
	(H2) The accident warning signal stops emitting light when "trapped-in" has occurred	(SC2) The accident warning signal does not stop emitting light when "trapped-in" has occurred
	(H3) The driver does not visually confirm the light emission of the accident warning signal	(SC3) A crew is able to confirm visually the light emission of the accident warning signal

Preparation 2

- Control structure



Step 1

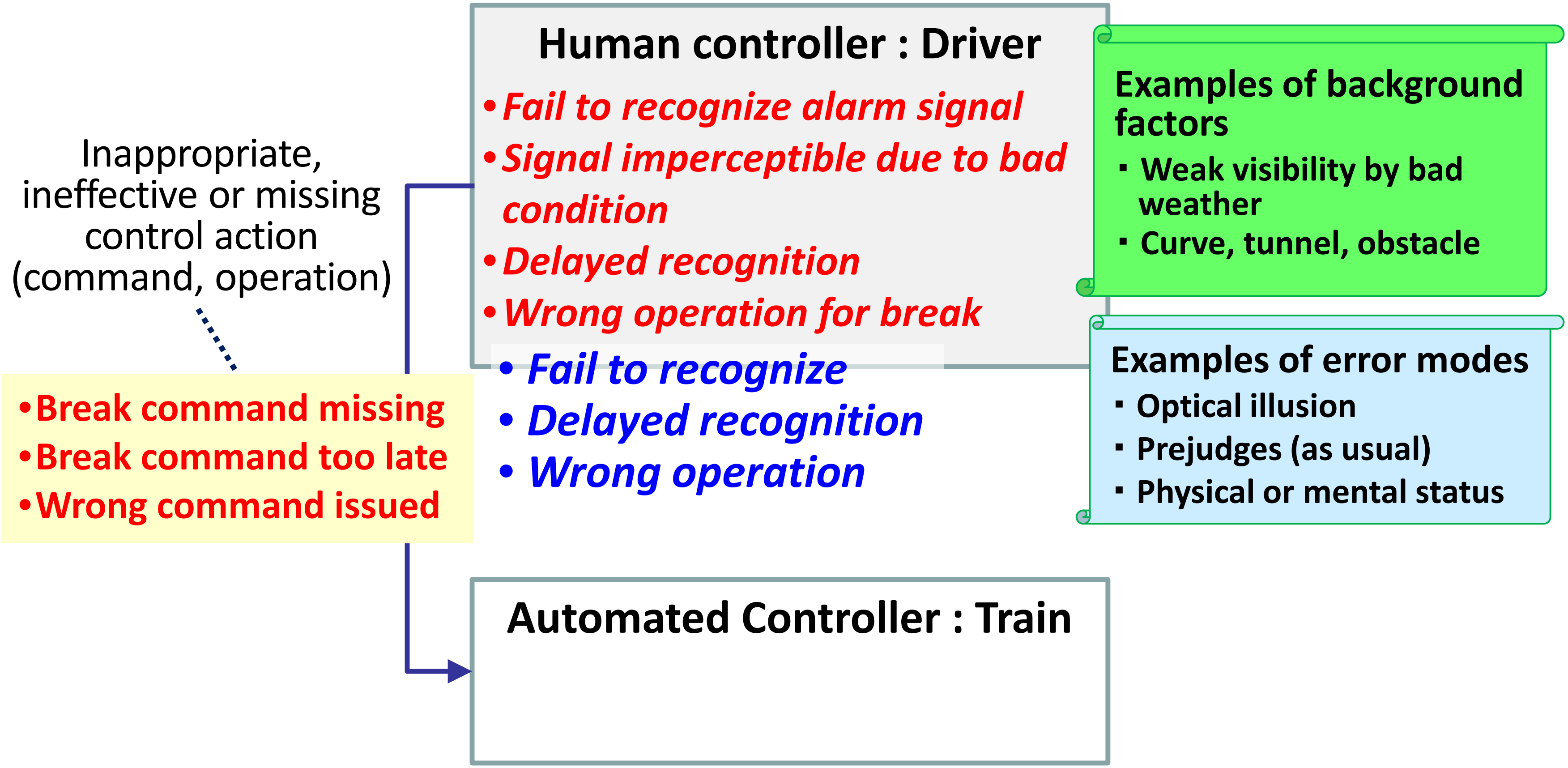
Identifying UCAs

Control action	Not providing	Providing causes Hazard	Too early / late	Stop too soon
(Detector → Warning signal) Emit light	(UCA1) The accident warning signal does not emit light when "trapped-in" occurred	Stop train by emitting light when "trapped-in" does not occur	（UCA2) The accident warning signal emits light too late when "trapped-in" occurred	
		・・・		
(Driver → Train) Operation to make break	(UCA3) The train does not apply break	Stop train by emitting light when "trapped-in" does not occur	(UCA4) The train does not come to rest in time	(UCA4) ←
		・・・		

UCA with human

Step 2 Identifying HCFs

■ Obtained hazardous scenarios leading to the UCA for human



Inappropriate, ineffective or missing control action (command, operation)

- Break command missing
- Break command too late
- Wrong command issued

Human controller : Driver

- *Fail to recognize alarm signal*
- *Signal imperceptible due to bad condition*
- *Delayed recognition*
- *Wrong operation for break*

- ***Fail to recognize***
- ***Delayed recognition***
- ***Wrong operation***

Examples of background factors

- ▪ Weak visibility by bad weather
- ▪ Curve, tunnel, obstacle

Examples of error modes

- ▪ Optical illusion
- ▪ Prejudges (as usual)
- ▪ Physical or mental status

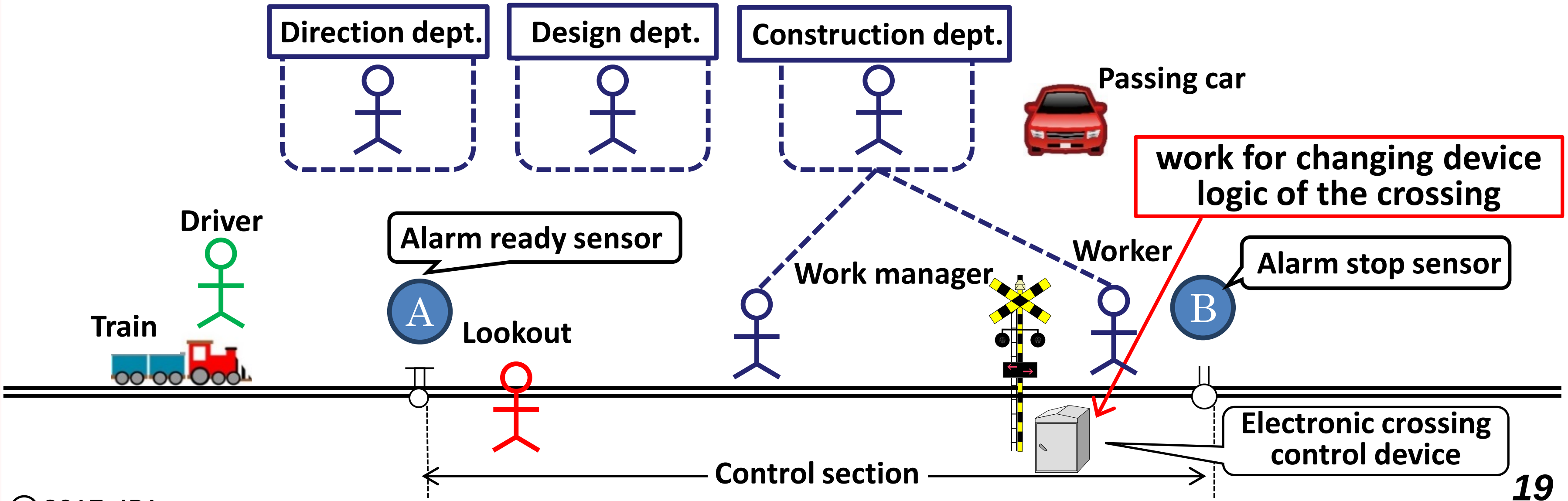
Automated Controller : Train

Application to another case

- Analysis for a safety design (2) -

Maintenance work of railway crossing system

	Step	Operation of the crossing	human	check
1	Design	–	• Logic development • Preparation of charts, procedures	Checked by human (double check, screening, approval, …)
2	Construction	Temporary suspend	• Cable wiring	Checked by human (visual observation, repetition, …)
3	Test	Temporary suspend	• Simulation	
4	Operation	Operation with the new logic	• (observation)	



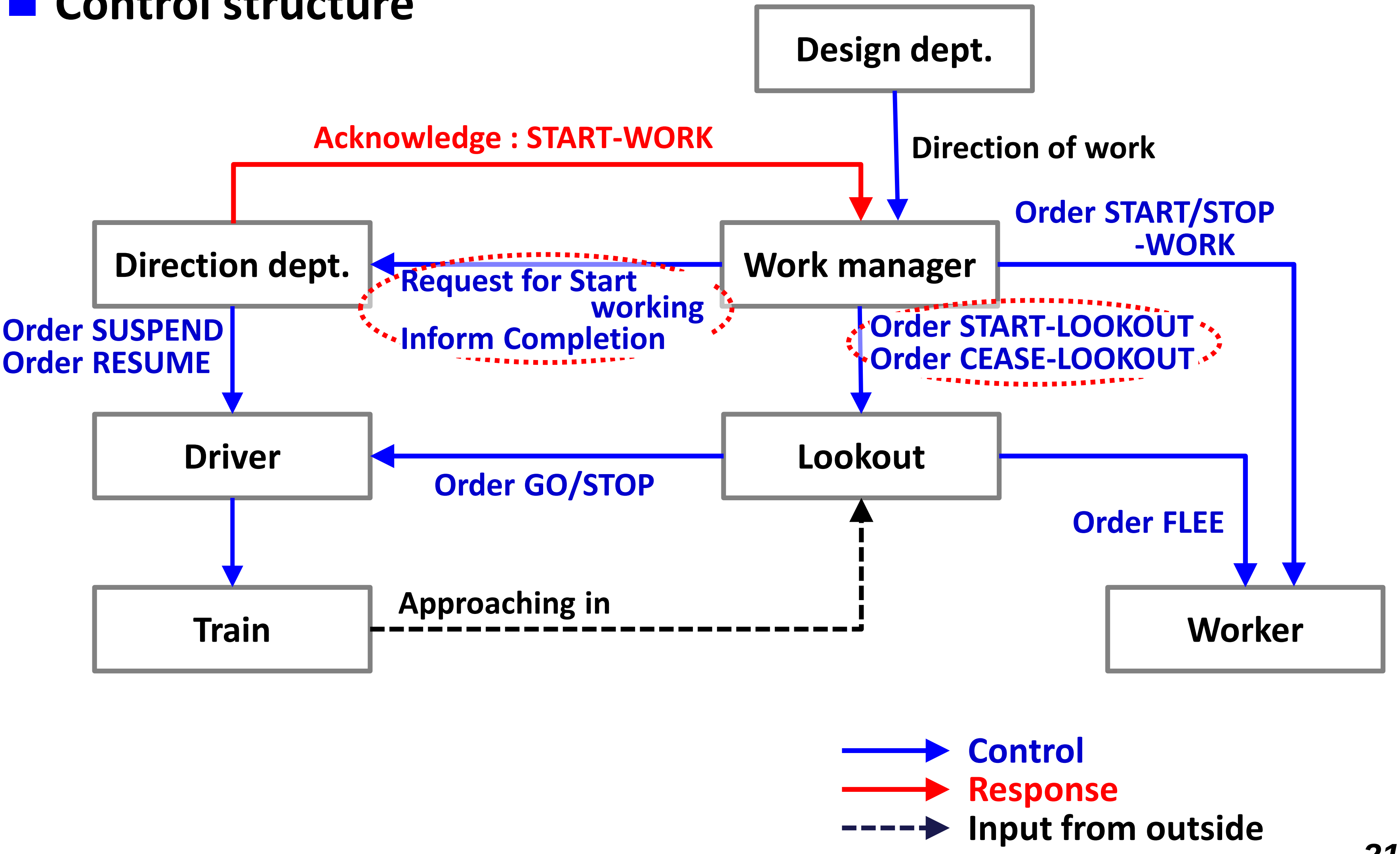
Preparation 1

Identifying Safety Constraints

Loss	Hazard	Safety Constraints
(A1) A worker, vehicle and materials collide with a train	(H1) The train proceeds when maintenance in progress	（SC1) The train shall not proceed into the control section under work
	(H2) The work is not suspended when train proceeds into the control section under work	(SC2) The work shall be suspended when train proceeds into the control section under work
	・・・	

Preparation 2

- Control structure



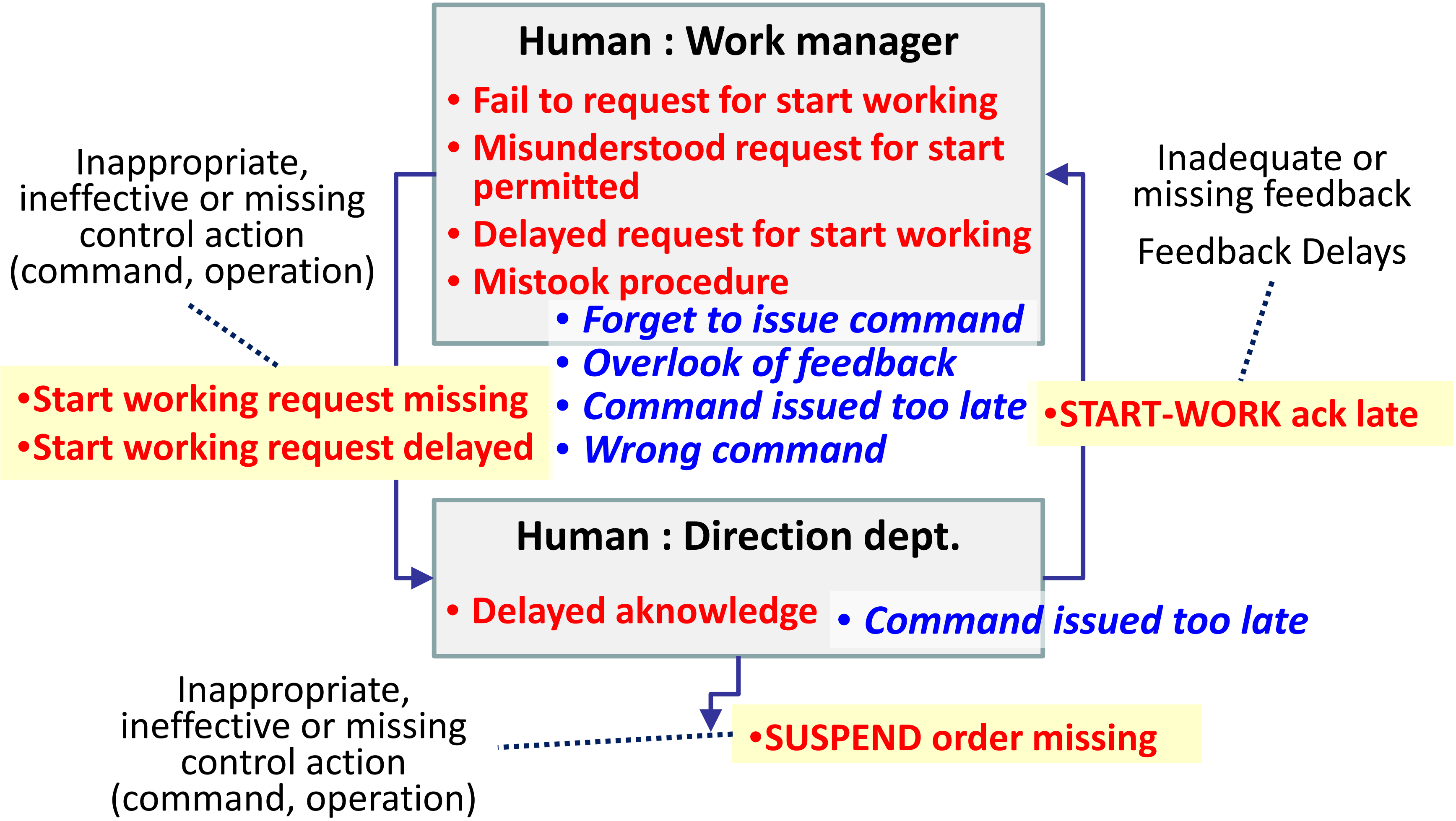
Step 1

Identifying UCAs

Control action	Not providing	Providing causes Hazard	Too early / late	Stop too soon
(Work manager → Direction dept.) Request for Start working	(UCA1) Train proceeds because SUSPEND order has not been issued, assuming the work has not started	-	（UCA2) Train proceeds because SUSPEND order is issued too late	-
・・・				
(Work manager → Lookout) Order START-LOOKOUT	(UCA3) Train proceeds into when Lookout does not watch	-	(UCA4) Train proceeds into when Lookout goes effective is too late	-
・・・				

Step 2 Identifying HCFs

■ Obtained hazardous scenarios leading to the UCA for human



Human : Work manager

- Fail to request for start working
- Misunderstood request for start permitted
- Delayed request for start working
- Mistook procedure

- *Forget to issue command*
- *Overlook of feedback*
- *Command issued too late*
- *Wrong command*

Inappropriate, ineffective or missing control action (command, operation)

•Start working request missing

•Start working request delayed

Inadequate or missing feedback

Feedback Delays

•START-WORK ack late

Human : Direction dept.

- Delayed aknowledge

- *Command issued too late*

Inappropriate, ineffective or missing control action (command, operation)

•SUSPEND order missing

ⓒ2017, IPA

Identified hazard scenarios

HCF/ Scenario	
UCA1: Train proceeds because SUSPEND order not issued due to absence of application for start working	
Scenario1	Forget to submit application for start working
Scenario2	START-WORK order is issued without permission Not to wait permission or make a wrong guess of permission obtained
UCA2: Application for start working is too late, thus order SUSPEND too late	
Scenario3	Wrong order of work procedure steps is taken
UCA3: WORK-COMPLETE is noticed despite work in progress, and order RESUME is issued	
Scenario4	Presumed completed (finish time has come, etc.) and inform before actual finish
Scenario5	Forget/ignore the cleanup time and notice before actual finish
• • •	

Verification: effectiveness in case study

- **The two cases are practical applications at JREast** ("trapped-in detection" and "maintenance at railway crossing")
  - Identified causes of unsafe control

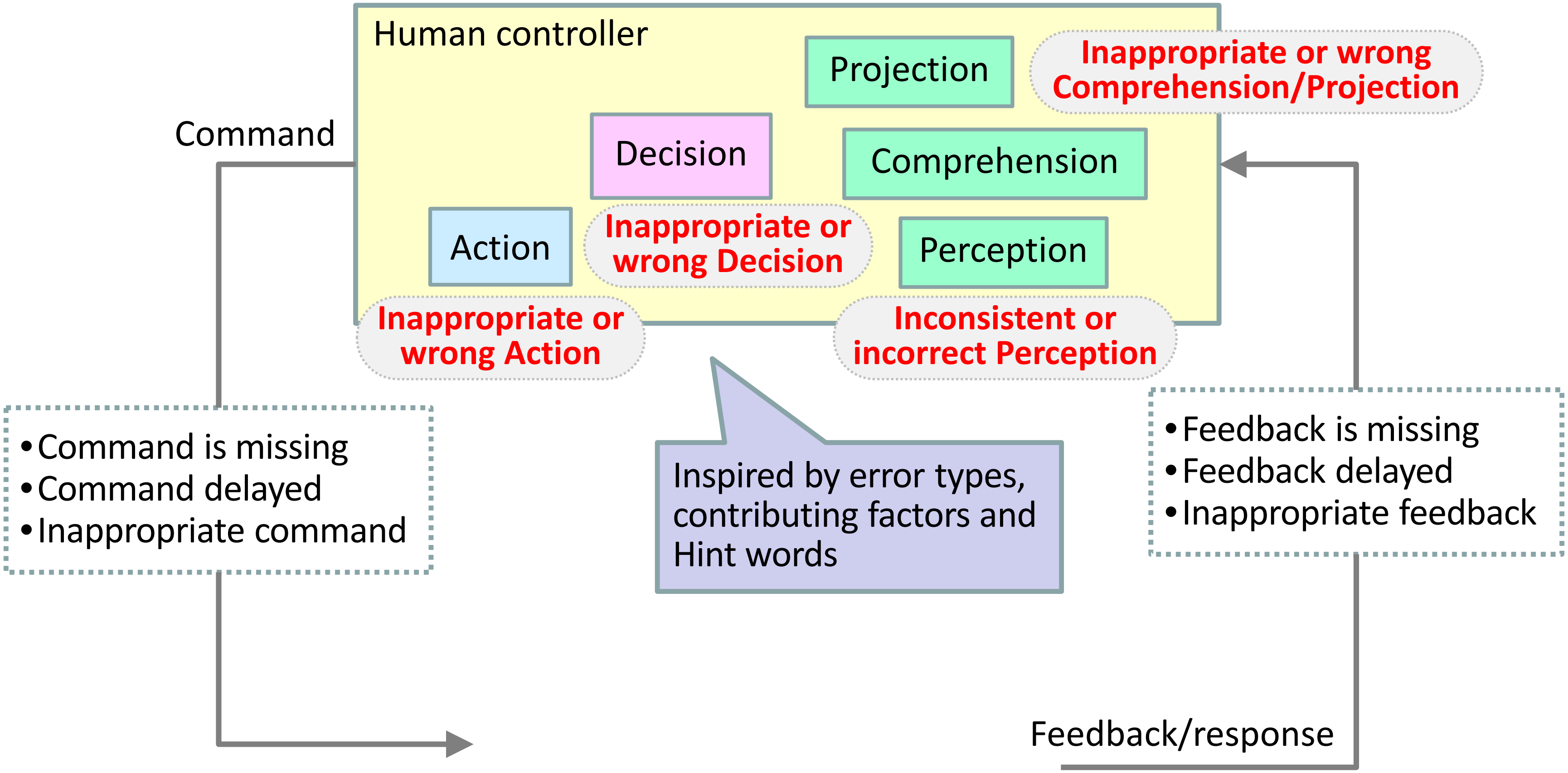
	All HCFs	Failures/ Sensing errors	Design flaws	Human	
				Director	Directee
CASE 1 (Trapped-in)	23	15	4	4	0
CASE 2 (maintenance)	40	1	0	29	10

- **The identified HCFs relating to human are derived with "Hint words" proposed**
- **Experts from the train system company evaluated this result as "These HCFs are practically exhaustive"**

Obtained “Hint words”

		Hint words	
Director	Omission	Presume the command unnecessary	
		Forget to issue the command	*Maintenance*
		Suppose the command has been issued	
		Operation is skipped due to an overlook of feedback	*Trapped-in*
	Commission	Issue a wrong command	*Trapped-in*
		Command is issued too late (Forget and remember the command)	*Trapped-in*
		The meaning of command mistaken	
		Issue command to a wrong directee	
		Issue command inappropriately (fail to confirm)	*Maintenance*
Directee	Omission	Unable to receive the command	
		Unable to execute the command	
		Forget to feedback the result	*Collision*
	Commission	Executed behavior is not what was ordered	
		Execution is delayed (Forget and remember the command)	
		Unable to act because the command is wrong	*Collision*

Proposed human entity for HCF guidance

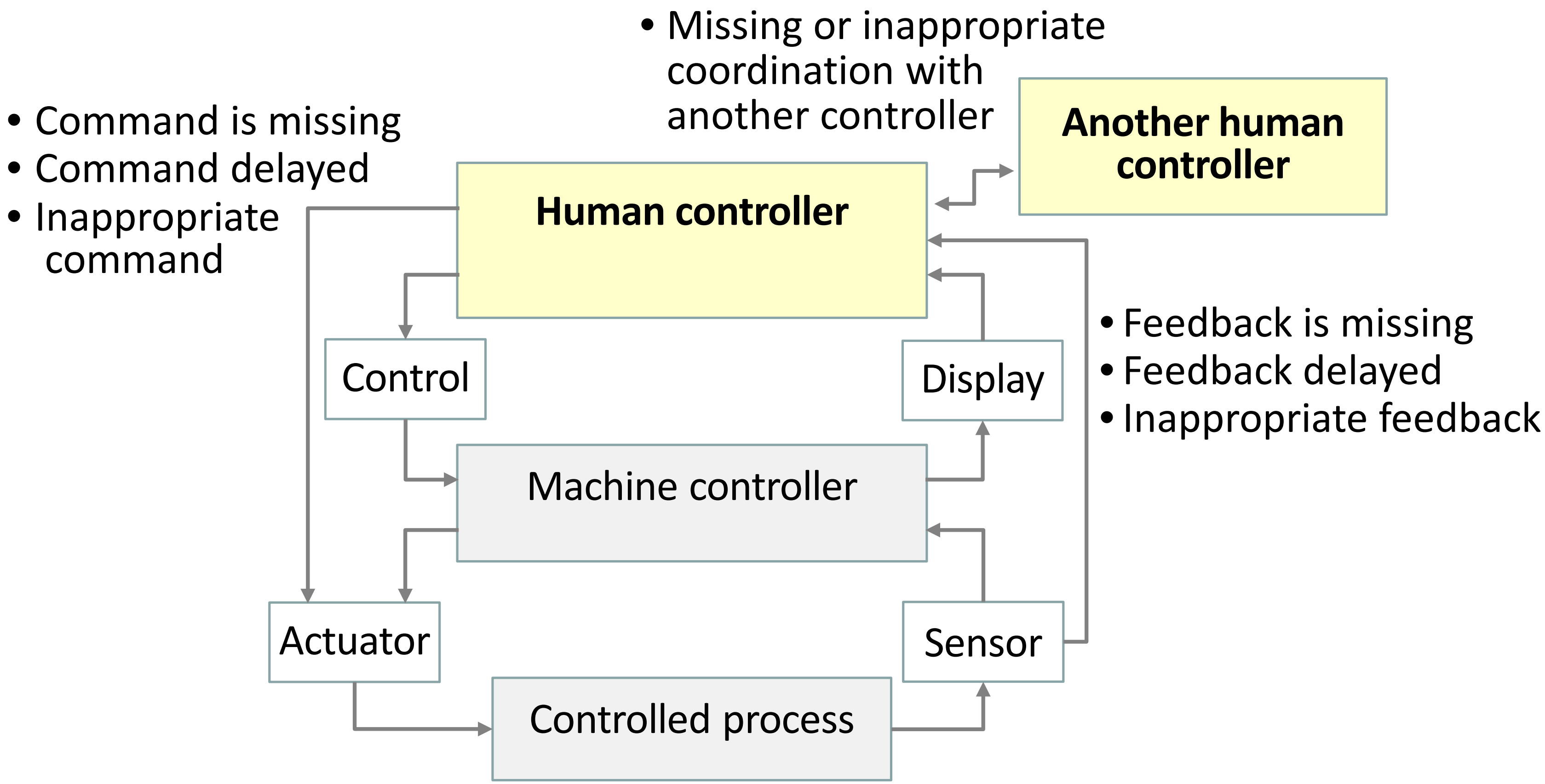

Human controller
Projection
Inappropriate or wrong Comprehension/Projection
Command
Decision
Comprehension
Action
Inappropriate or wrong Decision
Perception
Inappropriate or wrong Action
Inconsistent or incorrect Perception
Feedback/response

- Command is missing
- Command delayed
- Inappropriate command

Inspired by error types, contributing factors and Hint words

- Feedback is missing
- Feedback delayed
- Inappropriate feedback

Augmented HCF guidance



- Missing or inappropriate coordination with another controller

- Command is missing
- Command delayed
- Inappropriate command

Another human controller

Human controller

Control

Display

Machine controller

Actuator

Sensor

Controlled process

- Feedback is missing
- Feedback delayed
- Inappropriate feedback

Conclusion and Future work

- **Augmentation for control flaw guidance**
  - Human Controller entity in control loop model
  - Classification of human error types and Contributing factors
  - "Hint words" to identify as many HCFs originated by human
- **Analysis for organizations**

Thank you for your attention