Analysis of Human-related Accidents and Assessment of Human Error Based on STAMP

Case study on a Minuteman (MM) III missile accident

Rong Hao, Tian Jin

School of Reliability and Systems Engineering
Beihang University

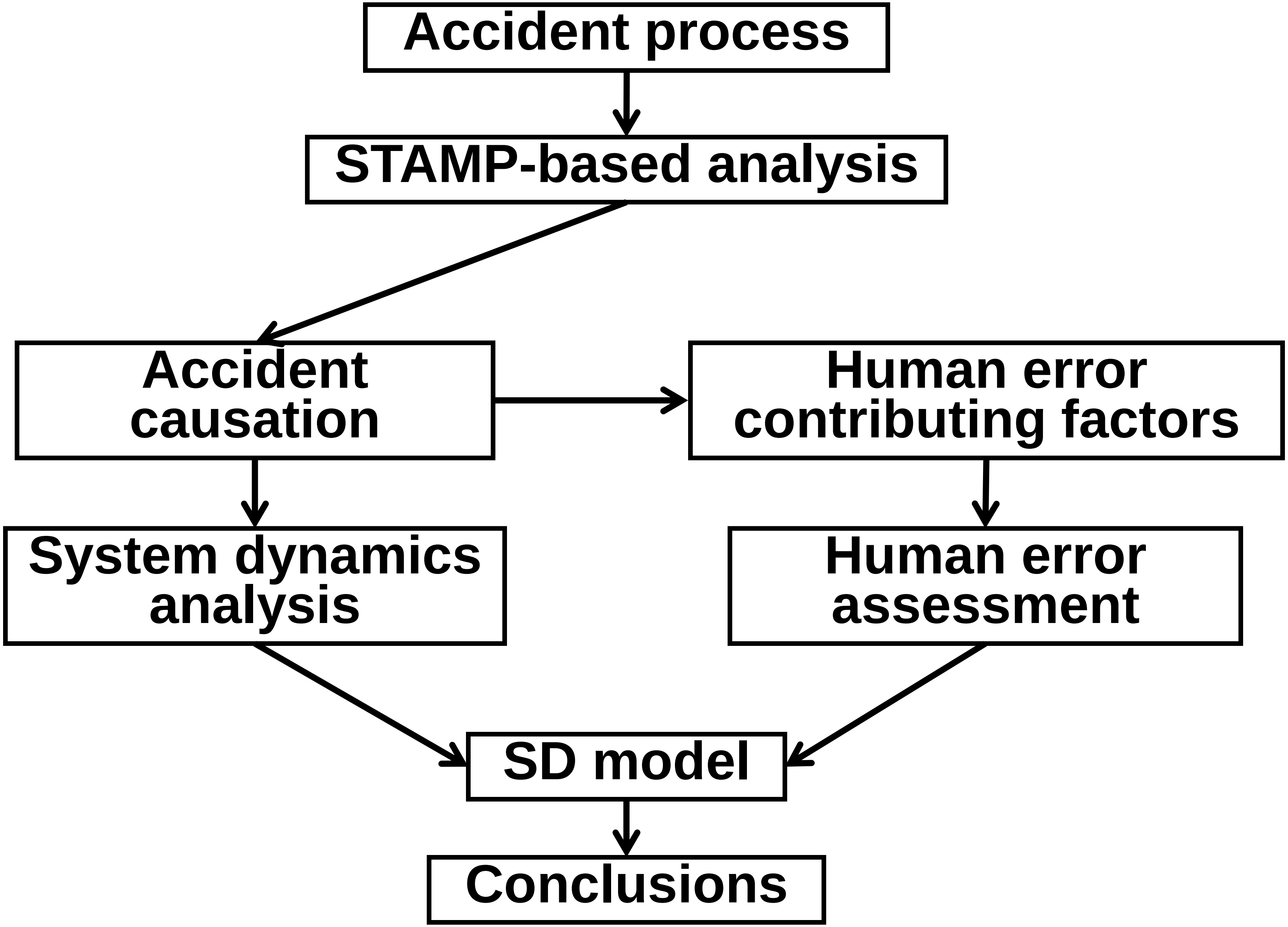
Overview

- Introduction
- Accident process
- STAMP-based analysis
- Human error assessment
- Conclusion

Introduction

- STAMP and STPA were used to analyze a MM III missile accident.
- The accident causation was identified and analyzed, and the dynamics and migration of system was discussed.
- Based on the accident causation, human error contributing factors was further elaborated, and the human error was quantified over time to measure system risk.

Introduction



Overview

- ✓ Introduction
- ➢ Accident process
- ➢ STAMP-based analysis
- ➢ Human error assessment
- ➢ Conclusion

Background

北京航空航天大學 BEIHANG UNIVERSITY

- **MM III missile**
  - Conceived in the late 1950s and deployed in the early 1960s
  - The only land-based Intercontinental Ballistic Missile (ICBM) in service in the United States
  - In state of alert when the accident occurred on May 28, 2008.

- **Human involved in operation (monitoring) process of MM III**
  - Missile Combat Crew (MCC) 【on duty at Launch Control Center (LCC)】
    - Monitor Launch Facility (LF) and missile through Monitoring System and periodic inspections.
  - Missile Maintenance Operations Center (MMOC)
    - Direct the MCC to clear the fault remotely
    - Require MCC to keep monitoring the fault in a specified time period.
    - Or send a maintenance team to the LF

Accident process

Accident introduction

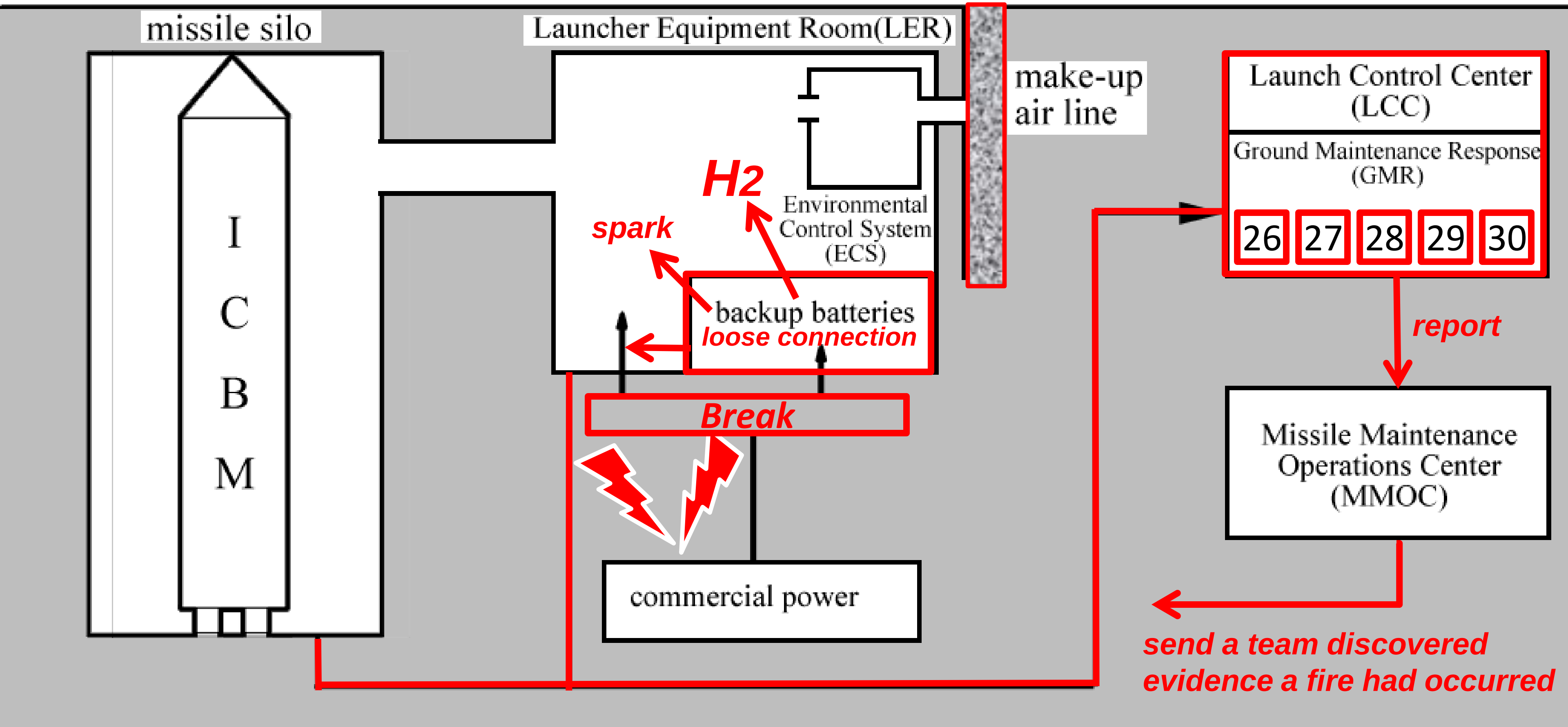
- On May 23, 2008, a fire broke out in Minuteman (MM) III Launch Facility (LF) A06, located near F.E. Warren AFB, WY. Fortunately, the fire did not influence missile, but the most probable total damage estimate is $1,029,855.77

- A loose connection on capacitor C101A of the battery charger inside A06's launcher equipment room (According to Accident Investigation Board Report)

Minuteman (MM) III Launch Facility A06

Dec 3, 2007 — Dec 12, 2007 — Mar 4, 2008 — Apr 24, 2008 — May 23, 2008 1100 MST — 1600 MST — 1634 MST — 1634-1638 MST — 1638 MST — 2241 MST — May 28, 2008

May 23, 2008 1634 MST



Overview

- ✓ Introduction
- ✓ Accident process
- ➢ STAMP-based analysis
- ➢ Human error assessment
- ➢ Conclusion

STAMP-based analysis

北京航空航天大學 BEIHANG UNIVERSITY

- STEP1： Identify the system safety constraints and system requirements
- STEP2： Document the safety control structure controlling the hazard and enforcing the safety constraints
- STEP3: Analyze the hazards at the operation process level based on STPA
- STEP4： Moving up the levels of the safety control structure, determine how and why each successive higher level allow or contribute to the inadequate control at the current level

STAMP-based analysis

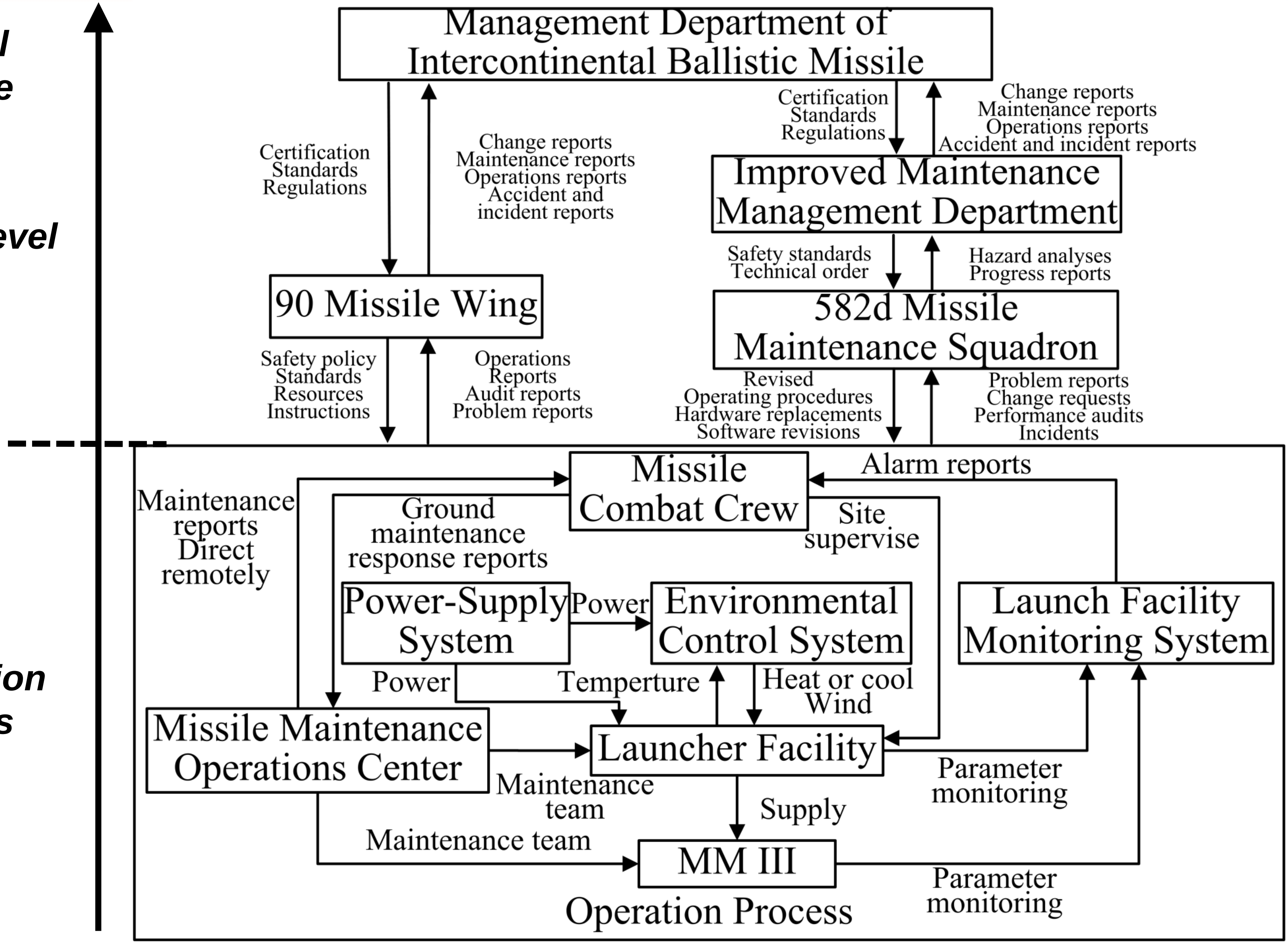
- STEP1： Identify the system safety constraints and system requirements.
  - Fire accident.
  - Safety constraints:
  - 1) Avoiding the concurrence of flammable substances, oxidizer and ignition source.
  - 2) Avoiding the interaction of flammable substances, oxidizer and ignition source.
- STEP2： Document the safety control structure to control the hazard and enforce the safety constraints.

STAMP-based analysis

- ***Control Structure***

High level

Operation process



STAMP-based analysis

- STEP3: Analyze the hazards at the operation process level based on STPA.

STAMP-based analysis

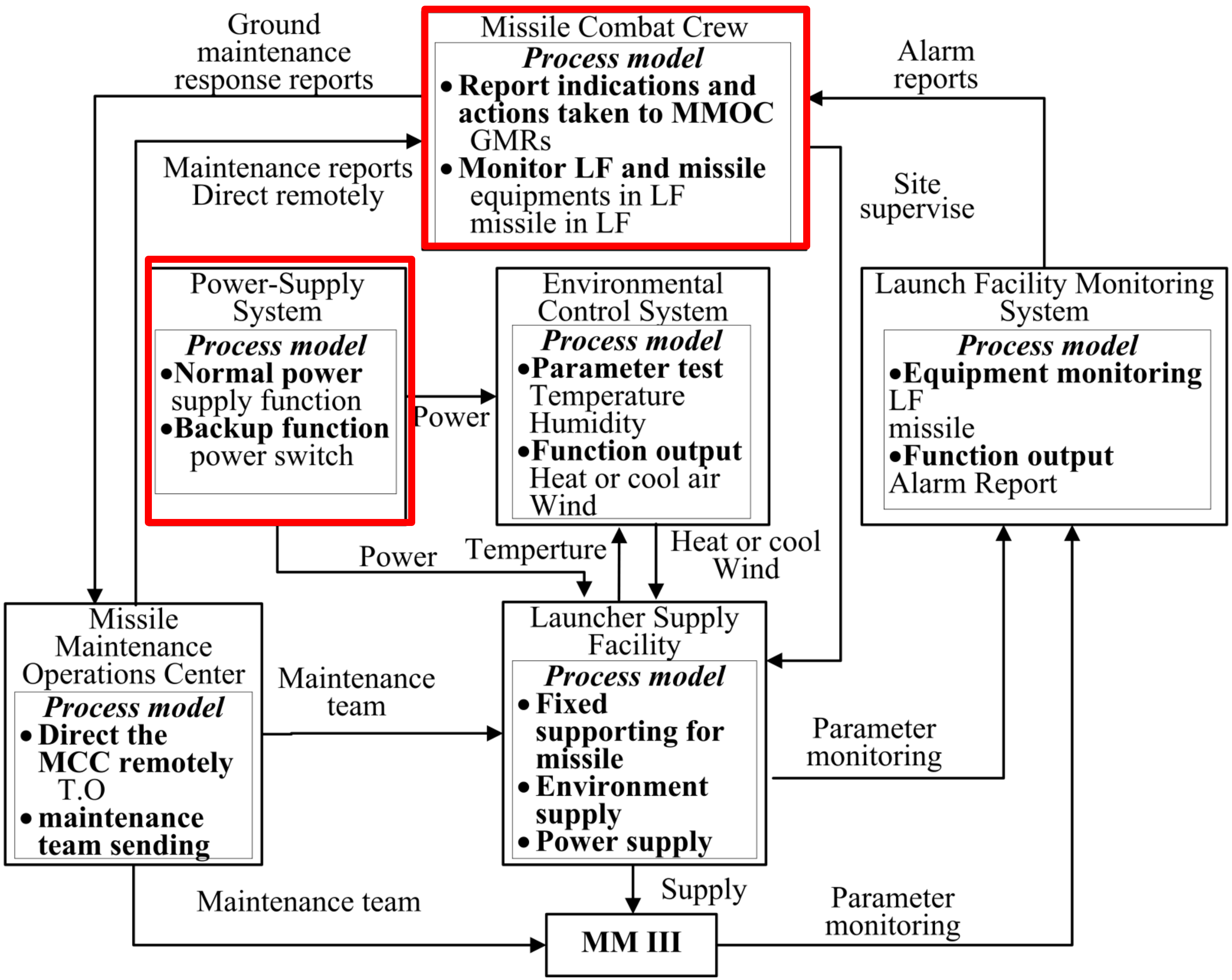
- Unsafe control actions for all controllers in operation process

Controller	Control action	a.Not Providing	b.Providing	c.Wrong Time or Order	d.Stopped Too Soon or Applied Too Long
MCC	Report indications and actions taken to MMOC	No reports	Inappropriate or missing reports	Delayed report	
	Monitor LF and missile	Missing Monitor	Ignore the monitoring information and GMRs.	Delayed respond to emergency situations	
MMOC	Direct the MCC to clear the fault remotely	No response in the time	Inappropriate or wrong direction	Delayed direct	
	Send maintenance team to the LF	No response in the time		Delayed send	
Launch Facility Monitoring System	Monitor physical system operation	No alarm when failures occur	False alarm	Delayed alarm	
Power-Supply System	Power supply	No automatically switched to backup power when emergency situations occur	Unstable electrical frequency; Leakage of electricity		Unexpected power outages
Environmental Control System	Control the temperature and humidity in LF	invalid temperature and humidity control; Inappropriate parameter test			Too high or too low control sensitivity

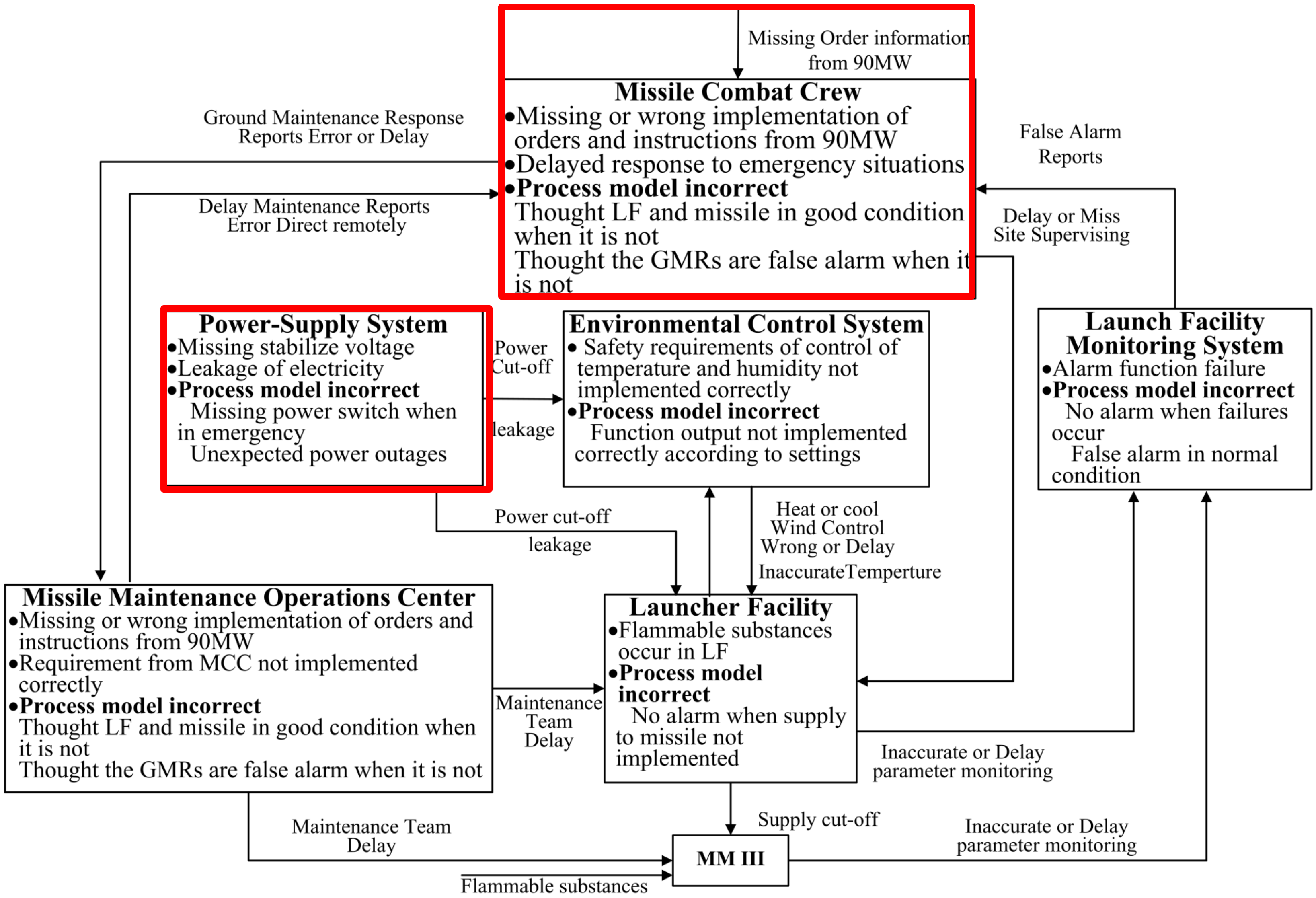
STAMP-based analysis

北京航空航天大學 BEIHANG UNIVERSITY

- Process model for operation process.

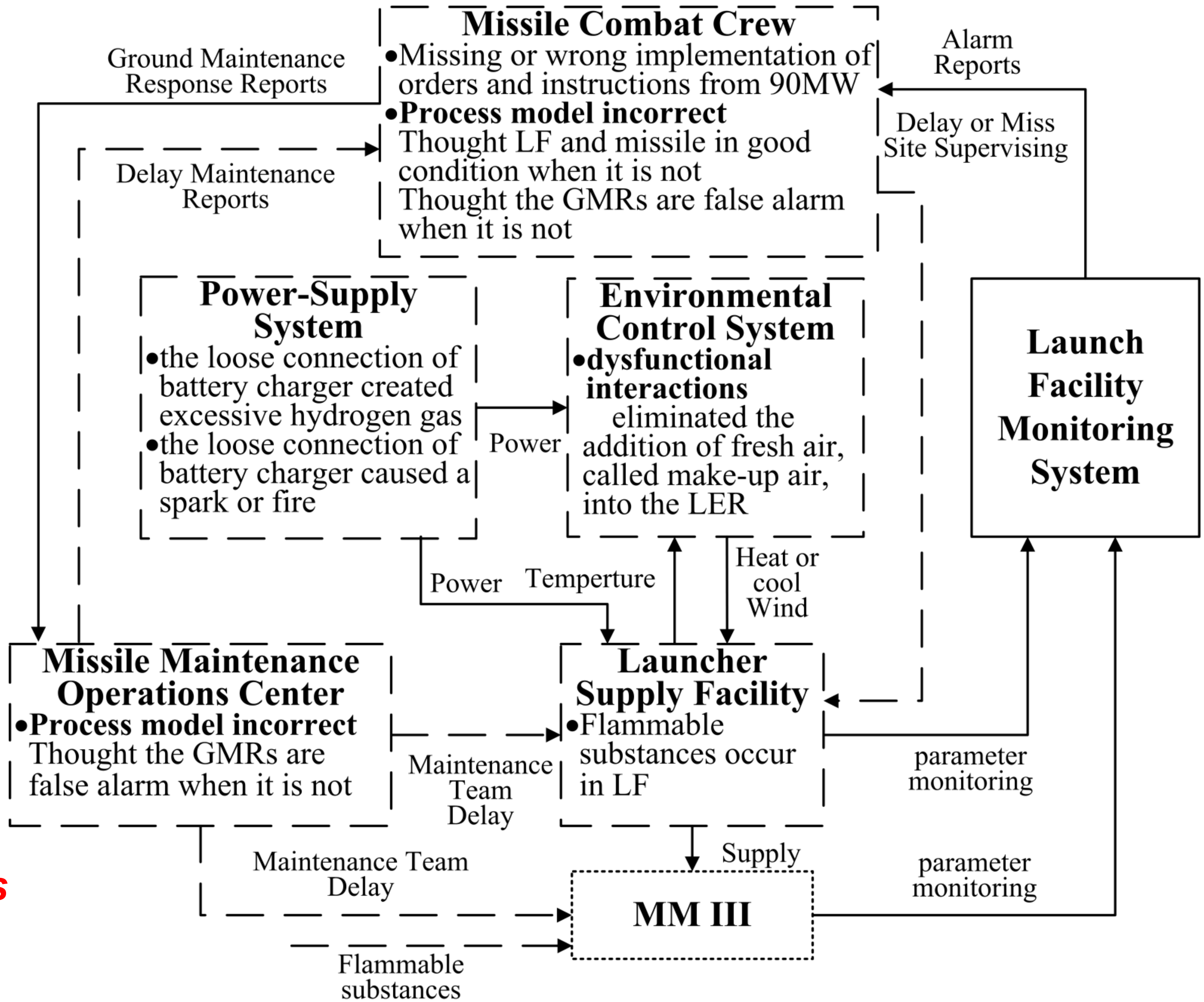


- Causal factor analysis



STAMP-based analysis

- The structure at the time of the accident



half of structure is ineffective

STAMP-based analysis

- Loose connection on capacitor of the battery charger caused the emergence of flammable substances(H_2) and ignition source (electrical arcing caused a fire or spark)
- MCC, MMOC and other controllers were neither in the right place, nor inspected periodically when accident happened, which triggered the interaction of flammable substances, oxidizer and ignition source
- Inadequate human-related control in operation process is exacerbated with the degraded quality of physical system (e.g. the false alarm)
- Dysfunctional interaction:

  New ECS eliminated the addition of fresh air into the LER, exacerbated the accumulation of H_2

STAMP-based analysis

北京航空航天大學 BEIHANG UNIVERSITY

- STEP4：Moving up the levels of the safety control structure, determine how and why each successive higher level allowed or contributed to the inadequate control at the current level

STAMP-based analysis

北京航空航天大學 BEIHANG UNIVERSITY

- Analysis of controllers in high level

Management Department of Intercontinental Ballistic Missile

Improved Maintenance Management Department

90 Missile Wing

Safety Requirements and Constraints:

- Propose specific plans of training and task according to orders from 90MW
- Control and management of MCC and MMOC in operation process, keep communication and coordination between them
- Supervision of MCC and MMOC to ensure safe operation process

The controller operation:

- Orders, Standards and Regulations from Management Department of Intercontinental Ballistic Missile missing or wrong, such as flammable substance management rule
- Incomplete safety culture construction
- Thought MCC and MMOC receive order or task plan information when it is not
- Thought MCC and MMOC implement task plan correctly when it is not

Actuators and controlled processes:

- Task plan conveying flaw

Context and environment in which the human is working:

- Pressure of resources or finance on supervision and management of MCC and MMOC
- Implement management according to the old experience
- Lack of communication to MCC and MMOC

582d Missile Maintenance Squadron

Safety Requirements and Constraints:

- Implement equipment improved maintenance plan according to orders from Improved Maintenance Management Department
- Provide logistics support for operation process
- Responsible for maintenance, repair, overhaul, and modification in operation process
- Report problems and maintenance related information to Improved Maintenance Management Department

The controller operation:

- Equipment improved maintenance plan and technical documentation from Improved Maintenance Management Department missing or wrong
- Inappropriate technical documentation including T.O.
- Thought LF and missile in good condition when it is not
- Delayed update equipment improved maintenance plan and technical documentation
- Problem report and safety report missing

Actuators and controlled processes:

- Maintenance error caused equipment failure

Context and environment in which the human is working:

- Insufficient training for solider

Coordination and Communication among contorllers and Decision makers:

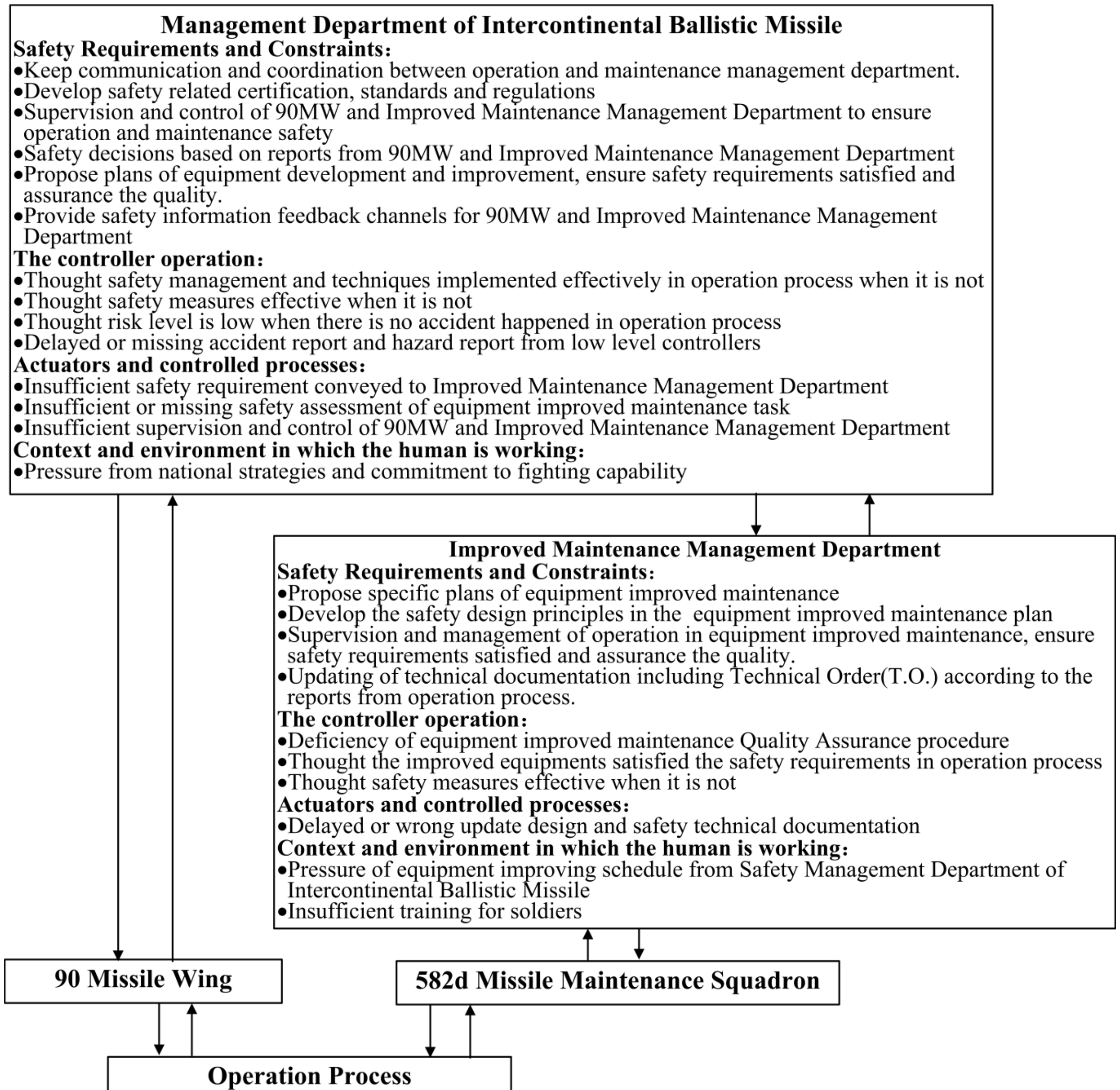
- resources pressure and financial pressure on human error

Operation Process

STAMP-based analysis

北京航空航天大學 BEIHANG UNIVERSITY

Analysis of controllers in high level



STAMP-based analysis

- Management department thought that the missile itself is more important than other supporting equipments in LF, and techniques more significant than management, which risked a huge misallocation of resources. Thus the improving plan of supporting equipments was ignored (unlike MM III), technical documents was updated with delay, and discussion work of new ECS was insufficient.
- Ignorance of safety management broke the human-related control in operation process, due to laxer implementations of periodical inspections, which is exacerbated with the degraded quality of physical system (e.g. the false alarm)
- Missing or delayed reports from lower levels to higher levels, because management department thought safety management and techniques implemented effectively and safety measures effective in operation process when they are not

Overview

北京航空航天大學 BEIHANG UNIVERSITY

- ✓ Introduction
- ✓ Accident process
- ✓ STAMP-based analysis
- ➢ Human error assessment
- ➢ Conclusion

Human error assessment

- Most of major accidents result from a migration of the system toward decreasing safety margins over time.
- Changing (human-related) factors cause the variation of system state:
- Operation process:
  - the quality degradation of equipments (e.g. the false alarm)
  - personal safety awareness (task pressure, personal commitment, training experience)
- The management controllers:
  - a contradiction between management commitment to system goal (e.g. fighting capability, profit) and that to safety
  - lax supervision and control due to a long term non-accident state and a bounce after an accident.

Human error assessment

Measurement for system risk

- Widely used:

  accident/incident rate

- Human-related accident:

  Human Error Probability (HEP) was used

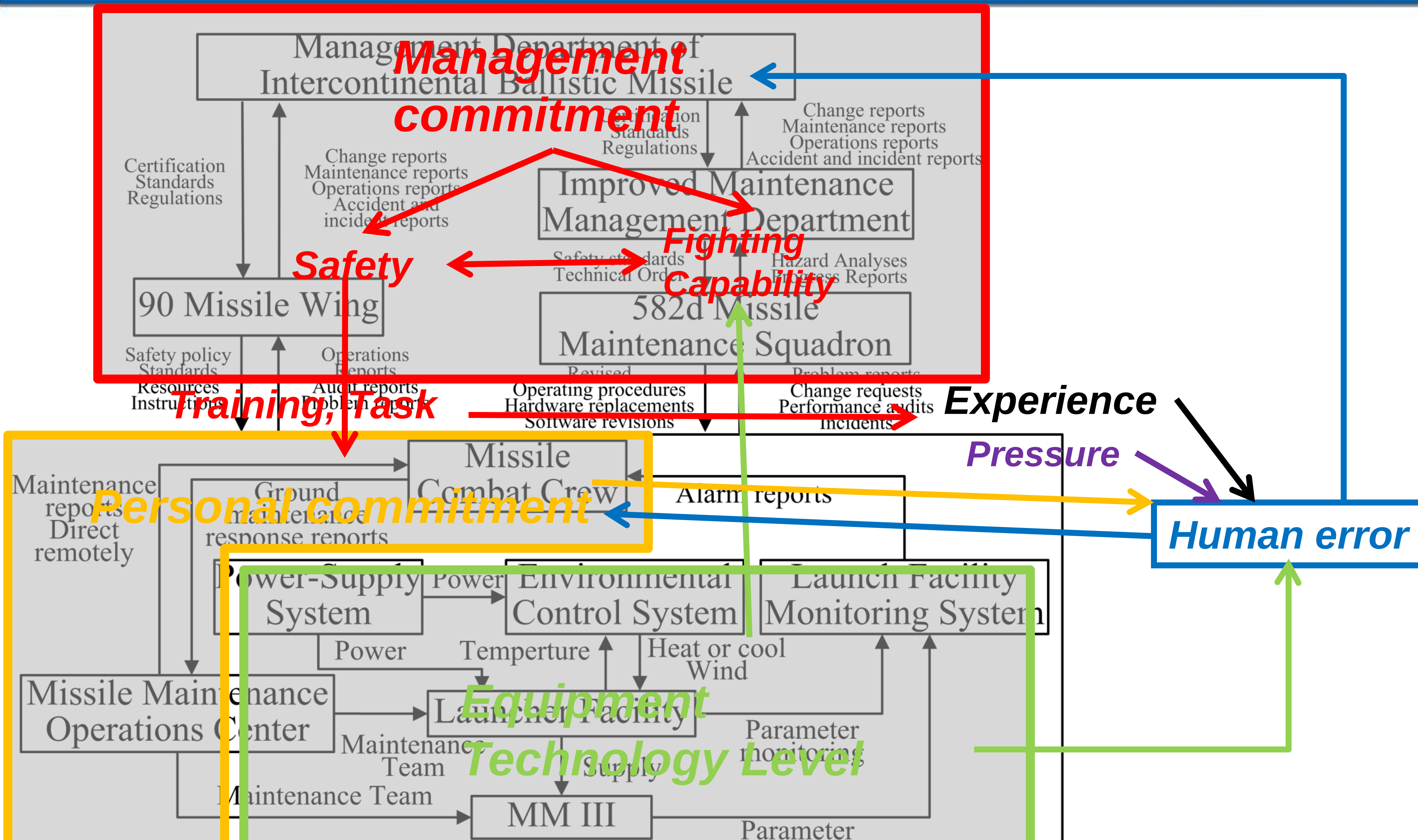
- Advantage:
  - based on Human Reliability Analysis (HRA) that has been relatively developed.
  - a more specific measurement than general accident/incident rate

Human error assessment

- **Human error contributing factors:**
  - management
  - task pressure
  - experience
  - safety awareness
  - equipment quality degradation

- All the factors change over time, so the HEP is probably a changing variable from a view of long term
- System Dynamics was used to analyze the complex relationship among these factors

Human error assessment

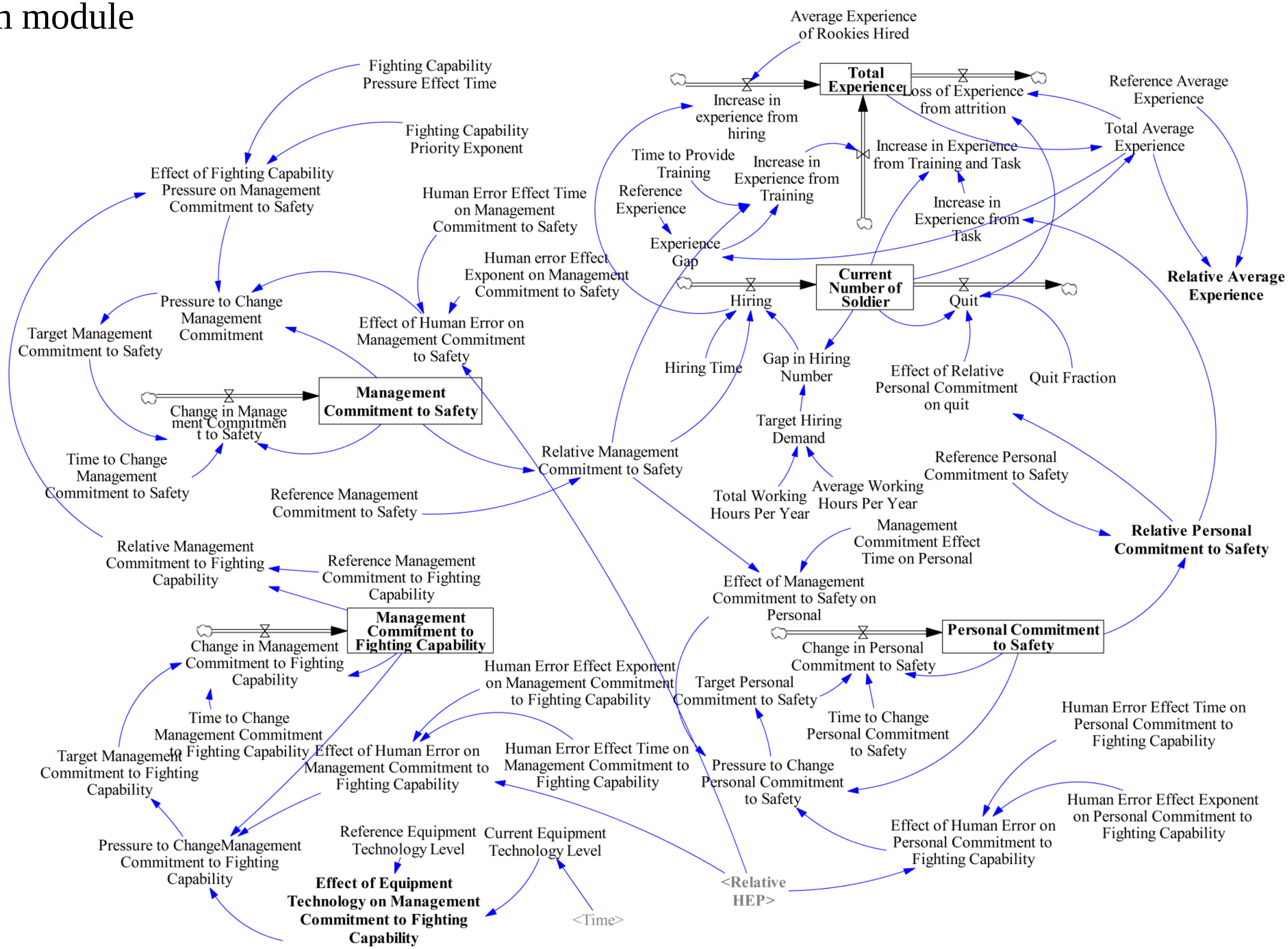


The figure describing causal relation

Human error assessment

北京航空航天大學 BEIHANG UNIVERSITY

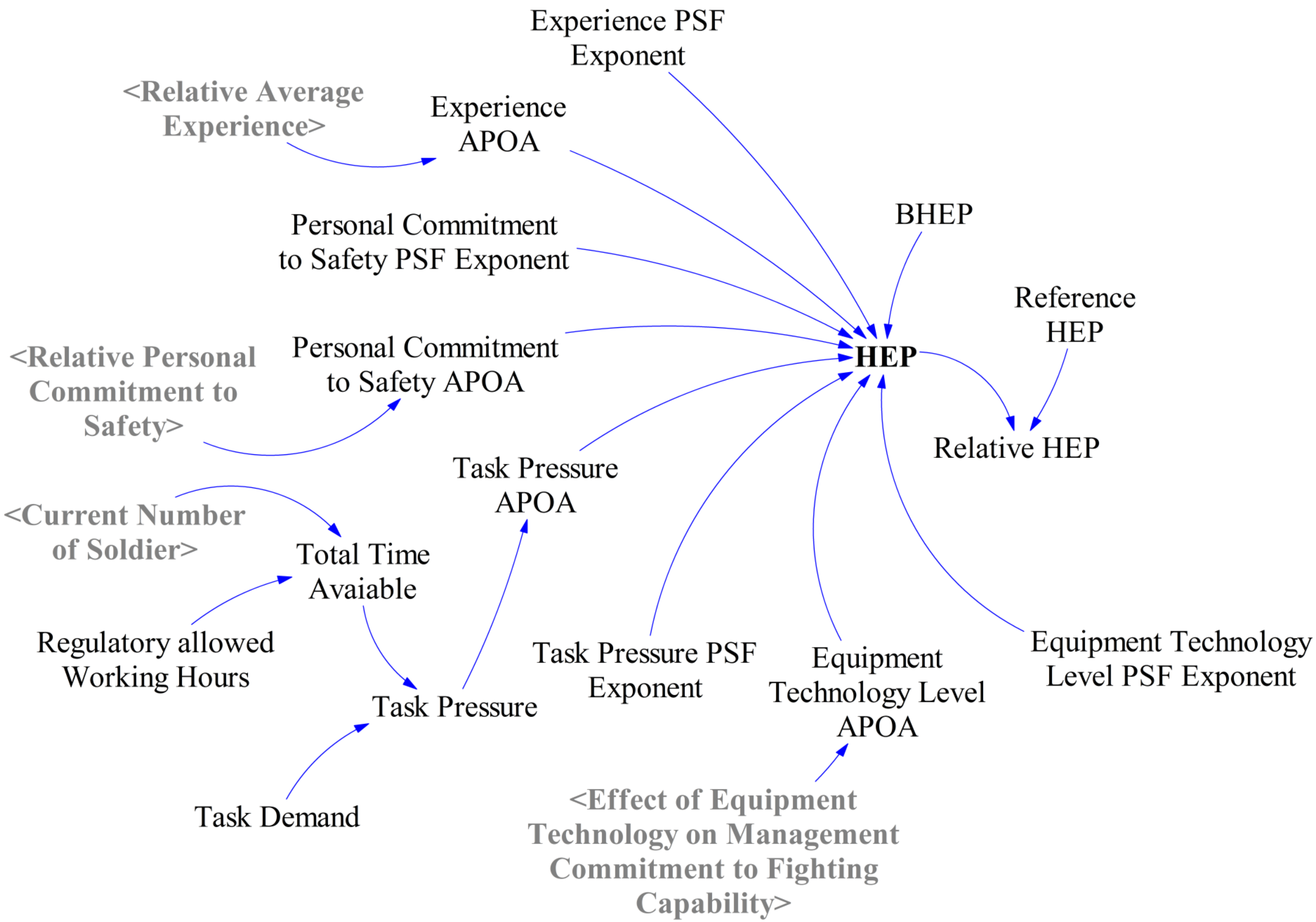
- System module



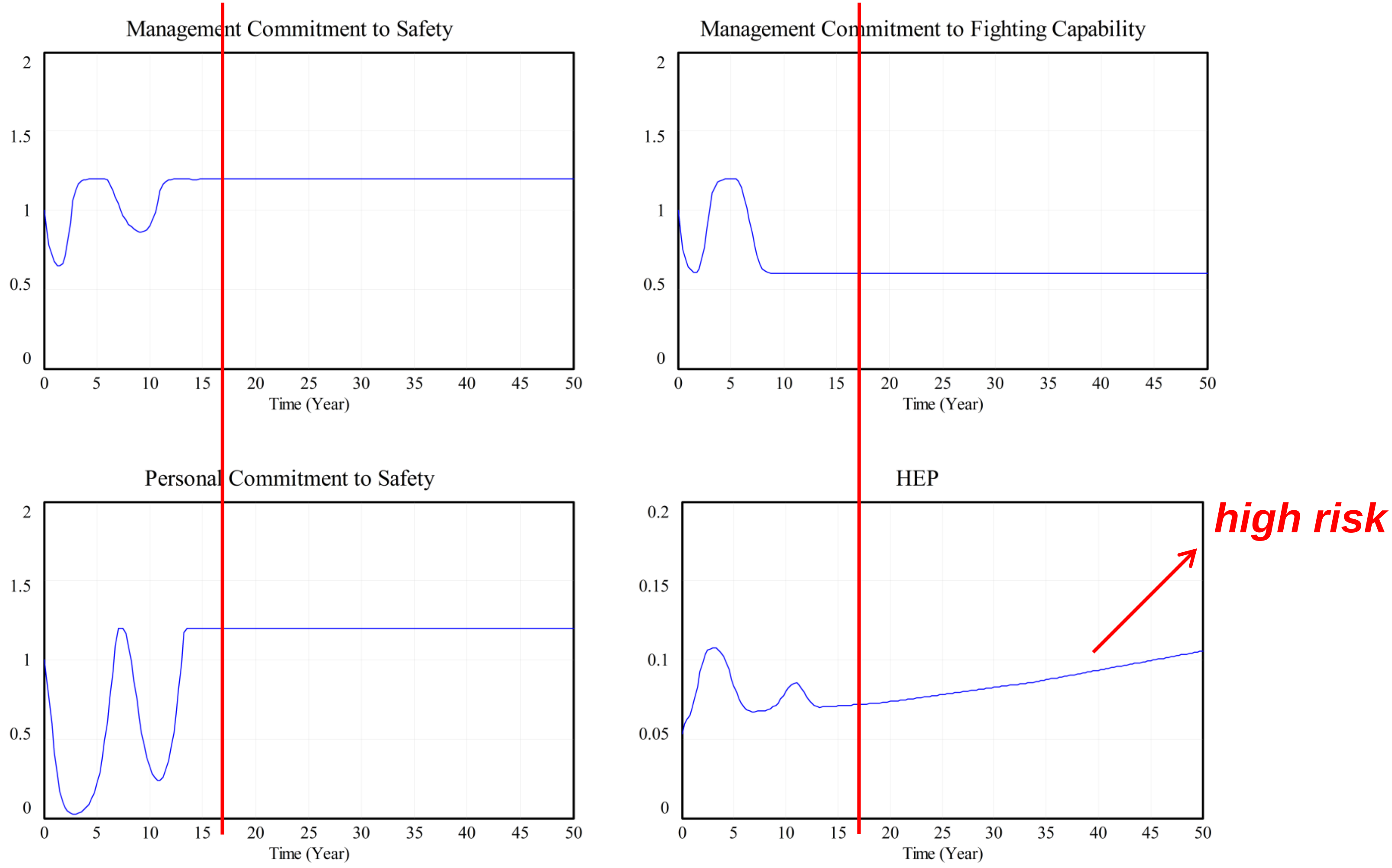
Human error assessment

北京航空航天大學 BEIHANG UNIVERSITY

- Human error module



Results and discussion



Human error assessment

- Human error contributing factors should be focused on
  - experience, personal commitment (safety awareness), pressure, equipment technology level (e.g. man-machine interface)
- The human-related variables fluctuate in the early time period, with the amplitude getting less
  - Because management has effect on personal commitment, but the effect is decreasing due to degenerate physical system.
  - some measurements should be adopted to keep HEP as low as possible.:
    - better equipment technology level
    - management pay enough attention on human error
- HEP keeps increasing during the mid-late period
  - degenerate physical system is dominant in contributing factors
  - the critical increasing/decreasing factors (e.g. equipment technology level)should be focused more on

Overview

- ✓ Introduction
- ✓ Accident process
- ✓ STAMP-based analysis
- ✓ Human error assessment
- ➢ Conclusion

Conclusion

- In operation process, prevent the failures of all controllers to missile in the same time.
  - (MCC, MMOC, Monitoring system)
- Management department should pay balanced attention to each aspect in the system, by changing its “process model”
  - safety & fighting capability, management & technology
- Better control and feedback channel to ensure the real system state informed to all controllers
- Analyze accident causes from a view of system
  - not just replace the battery charger

北京航空航天大學
BEIHANG UNIVERSITY

Thanks!

email：Rong Hao ronghao2010@sina.com
Tian Jin rabbit-tian@163.com