Proactively Examining NextGen Human Performance and System Safety

An Application of a Modified STPA in Air Traffic Control

Fort Hill Group

www.FortHillGroup.com

2014 STAMP/STPA User Conference

Katie Berry Ph.D.
Michael Sawyer Ph.D.

March 2014

Human Performance & System Safety

- Many of the most complex, high-consequence domains rely on human operators as the primary decision maker responsible for ensuring safe operations
- Increasing levels of automation and technology may actually make systems more brittle and the job of human operators more difficult in certain situations
- As domains become more complex, the factors leading to adverse events become more difficult to identify

Evolving Views of Human Error

Old View

- Human error is a leading cause of accidents
- Remove or retrain people to reduce errors
- Design the human out of the system

New View

- Human error is a symptom or outcome of systemic issues
  - Inadequate Training
  - Work Schedules
  - Supervisor Practices
  - Organizational Culture

Analysis and mitigations must shift the focus towards understanding the impact of operator and system context on performance

Assessing Human Performance & Safety

Proactive

Identify & Mitigate Risks

Prior to Implementation

- Identifies potential human performance risks associated with new procedures, systems, or capabilities
- Generates functional, design, and training requirements to maximize human performance
- Improves implementation time, cost, and safety

Emergent

Identify & Mitigate Risks

Before an Event

- Assesses risks across current system operations to identify key performance indicators of human performance risks
- Combines operational data, expert input, and near miss reports to assess human performance & system risks
- Improves human performance and system safety

Responsive

Identify & Mitigate Risks

After an Event

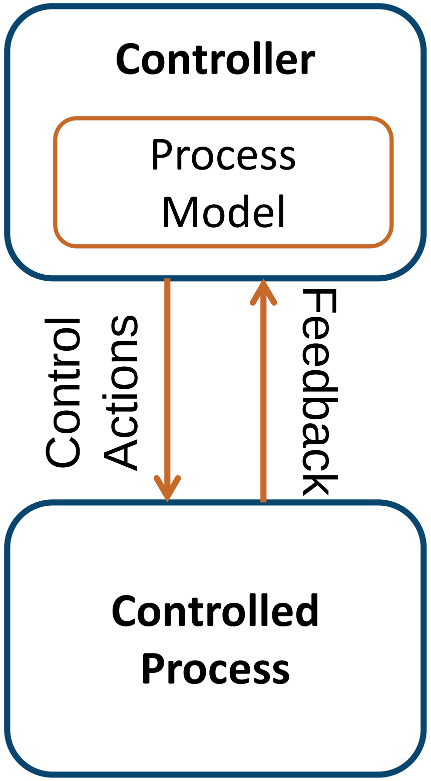
- Identify human performance and systemic causal factors leading to an adverse safety event
- Allows for the development of targeted mitigation strategies to reduce likelihood and severity of adverse events
- Improves human performance and system safety

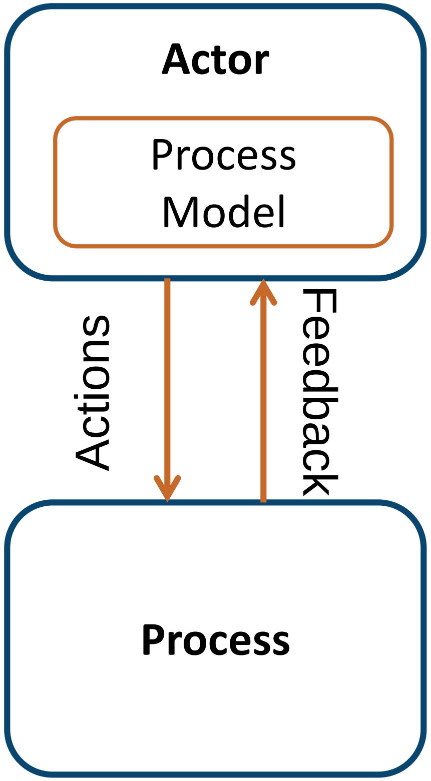
Proactive Human Performance Assessment

Goal: Proactively identify potential human performance & system hazards introduced by new systems or procedures

- Human focused approach to identify the impacts of various hazards to human performance
- Development of targeted mitigation strategies addressing identified hazards
- Development of design and training requirements that maximize human performance
- Applicable when human operator serves a key role as a decision maker or controller

Definition Recalibration





HESRA | Human Error Safety Risk Assessment

- Structured approach for identifying potential human performance hazards
- Developed to integrate into the FAA's Safety Management System process and methodology
- Basis in Failure Modes and Effects Analysis
- Generates a listing of human performance hazards prioritized based on severity, likelihood, and detection / recovery of the hazard's worst credible outcome

HESRA | Process Steps and Output

HESRA Process

1. Define Tasks
2. Identify Hazards
3. Estimate Likelihood, Severity, and Detection/Recovery
4. Determine Risk Priority Number (RPN)
5. Analyze Criticality

HESRA Output

- Hazard Condition
- Human Performance Hazard
- Worst Credible Outcome
- Ratings – Severity, Likelihood, Recovery
- Effect Type
- Risk Priority

HESRA | Human Performance Risk Priority

Category	Definition/Action
Extremely Low Risk	No system or safety implications No further design or evaluation efforts required
Low Risk	No significant system or safety implications Unlikely that significant design, training, or procedural changes will be required
Moderate Risk	Potentially significant system or safety implications Possible that significant design, training, or procedural changes will be required If system is not yet deployed, error mode should be further evaluated and then monitored during usability testing
High Risk	Significant system or safety implication Likely that significant design, training, or procedural element will be required
Extremely High Risk	Critical system or safety implications If an existing system, then immediate remediation should take place If system is not yet deployed, significant design, training, or procedural changes are required before the system is deployed

HESRA | Summary

HESRA

Human Error Safety Risk Assessment

Identifies and prioritizes human performance hazards and potential hazard outcomes

Limited view of system impacts

STPA | Systems Theoretic Process Analysis

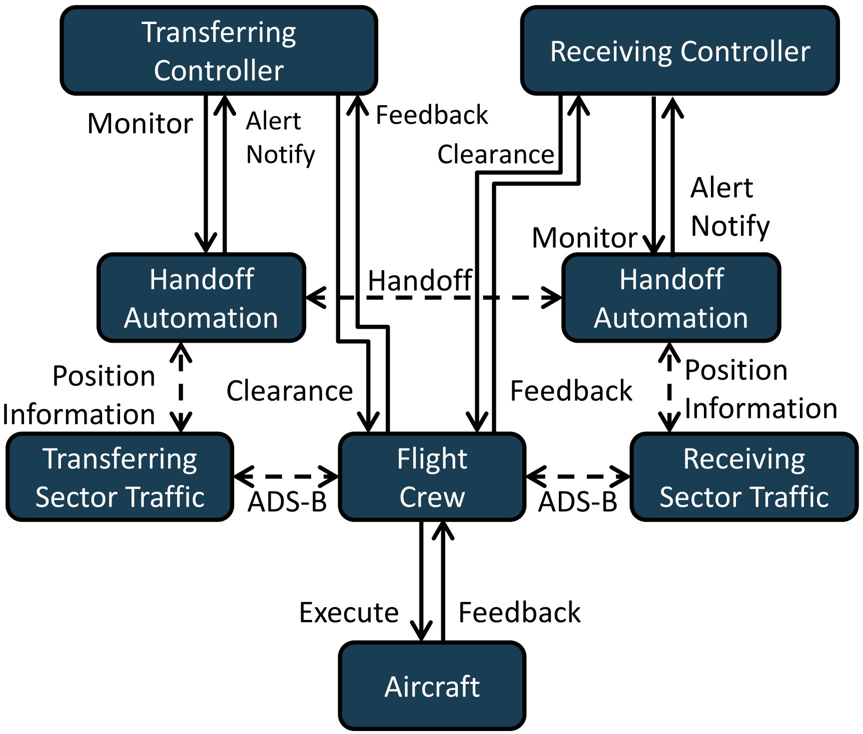
Application of STAMP to hazard identification & analysis

STPA Process

1. Identify accidents and hazards
2. Create control structure
3. Identify unsafe actions
    a. Command not given
    b. Unsafe command given
    c. Command given too early/late
    d. Command stops too soon or applied too long
4. Identify causal factors

Leveson, 2013

Sample ATC Control Structure

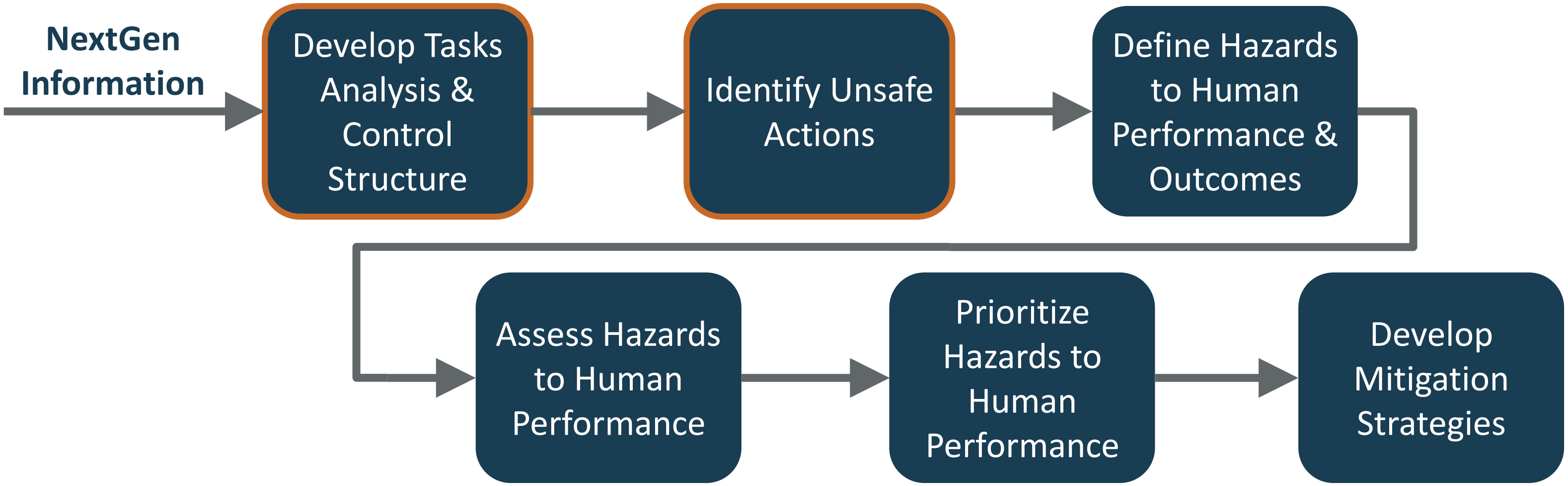


Proactive Human Performance Assessment Methodology Components

HESRA	STPA
Human Error Safety Risk Assessment	System Theoretic Process Analysis
Identifies and prioritizes human performance hazards and potential hazard outcomes	Treats accidents as dynamic control problems using control structures and safety constraints
Limited view of system impacts	Limited view of human performance

HESRA-STPA Methodology

Human Error Safety Risk Assessment – Systems Theoretic Process Analysis



NextGen Information

Develop Tasks Analysis & Control Structure

Identify Unsafe Actions

Define Hazards to Human Performance & Outcomes

Assess Hazards to Human Performance

Prioritize Hazards to Human Performance

Develop Mitigation Strategies

Hazards to Human Performance Components

- Hazard Condition
- Hazard Description
- Worst Credible Outcome
- Affected Controller Tasks
- Risk Priority

Hazards to Human Performance Identification

- Action required but not provided
- Unsafe action provided
- Incorrect timing/order
- Stopped too soon/applied too long
- Other HF component

Benefits of HESRA-STPA Integration

- Identifies system connections/interactions
- Thorough and comprehensive hazards
- Allows for a range of outcomes
- Prioritizes hazards

HESRA-STPA Methodology

Human Error Safety Risk Assessment – Systems Theoretic Process Analysis

- Basis in human factors and system engineering theories

Human Factors Theories

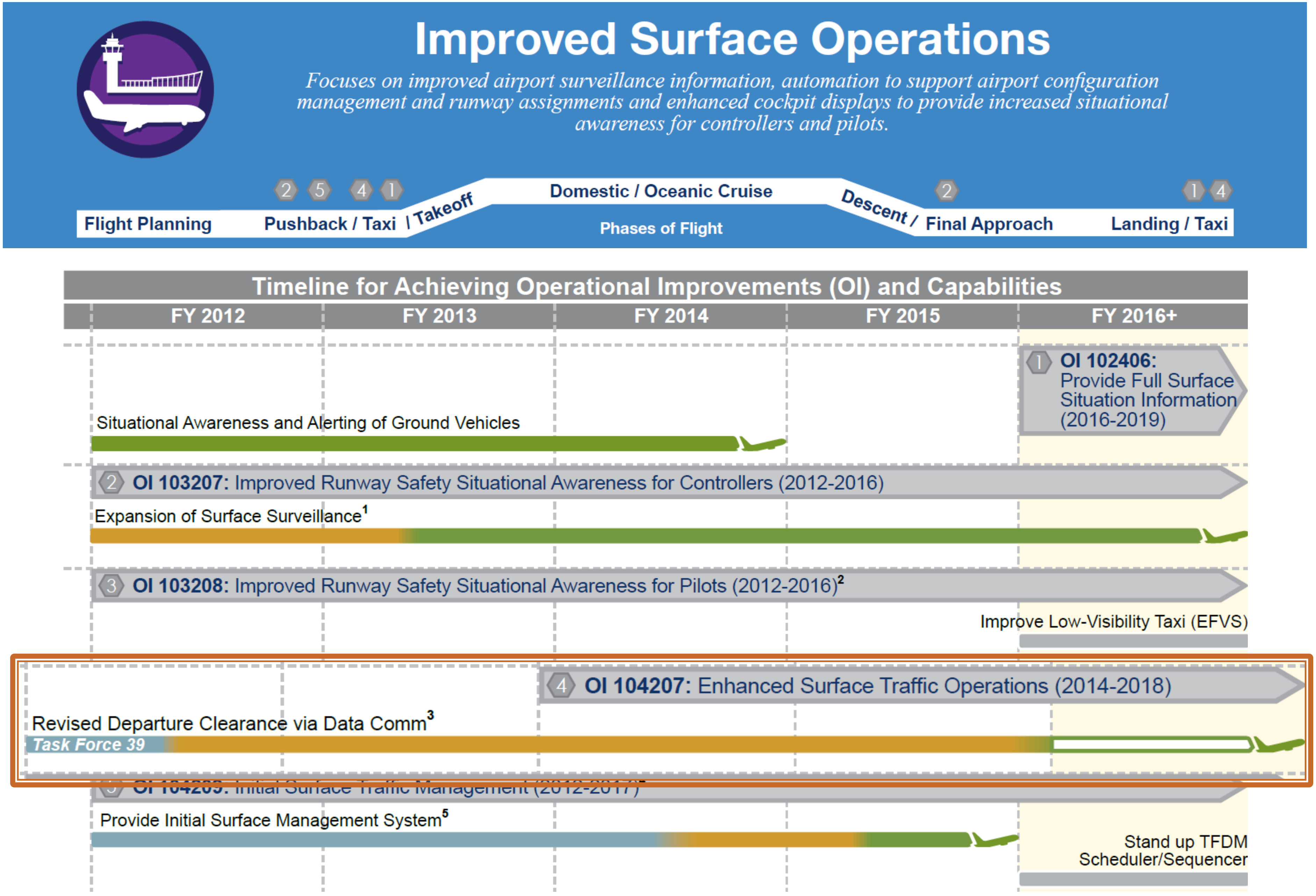
  - AirTracs
  - HESRA

Systems Engineering Theories

  - STAMP
  - STPA

- Provides a comprehensive view of potential risks
  - Human performance impacts
  - System-level contributing factors
- Control structure outlines the interactions among actors and systems
- Conforms to FAA and ICAO Safety Management System (SMS)
- Produces a prioritized listing of potential human performance and system hazards

Application | Improved Surface Operations



Improved Surface Operations

Focuses on improved airport surveillance information, automation to support airport configuration management and runway assignments and enhanced cockpit displays to provide increased situational awareness for controllers and pilots.

Timeline for Achieving Operational Improvements (OI) and Capabilities

1 **OI 102406:** Provide Full Surface Situation Information (2016-2019)

Situational Awareness and Alerting of Ground Vehicles

2 **OI 103207:** Improved Runway Safety Situational Awareness for Controllers (2012-2016)

Expansion of Surface Surveillance[1]

3 **OI 103208:** Improved Runway Safety Situational Awareness for Pilots (2012-2016)[2]

Improve Low-Visibility Taxi (EFVS)

4 **OI 104207:** Enhanced Surface Traffic Operations (2014-2018)

Revised Departure Clearance via Data Comm[3]

Task Force 39

5 **OI 104209:** Initial Surface Traffic Management (2012-2017)[4]

Provide Initial Surface Management System[5]

Stand up TFDM Scheduler/Sequencer

(FAA, 2013)

Aviation Communication

Current System

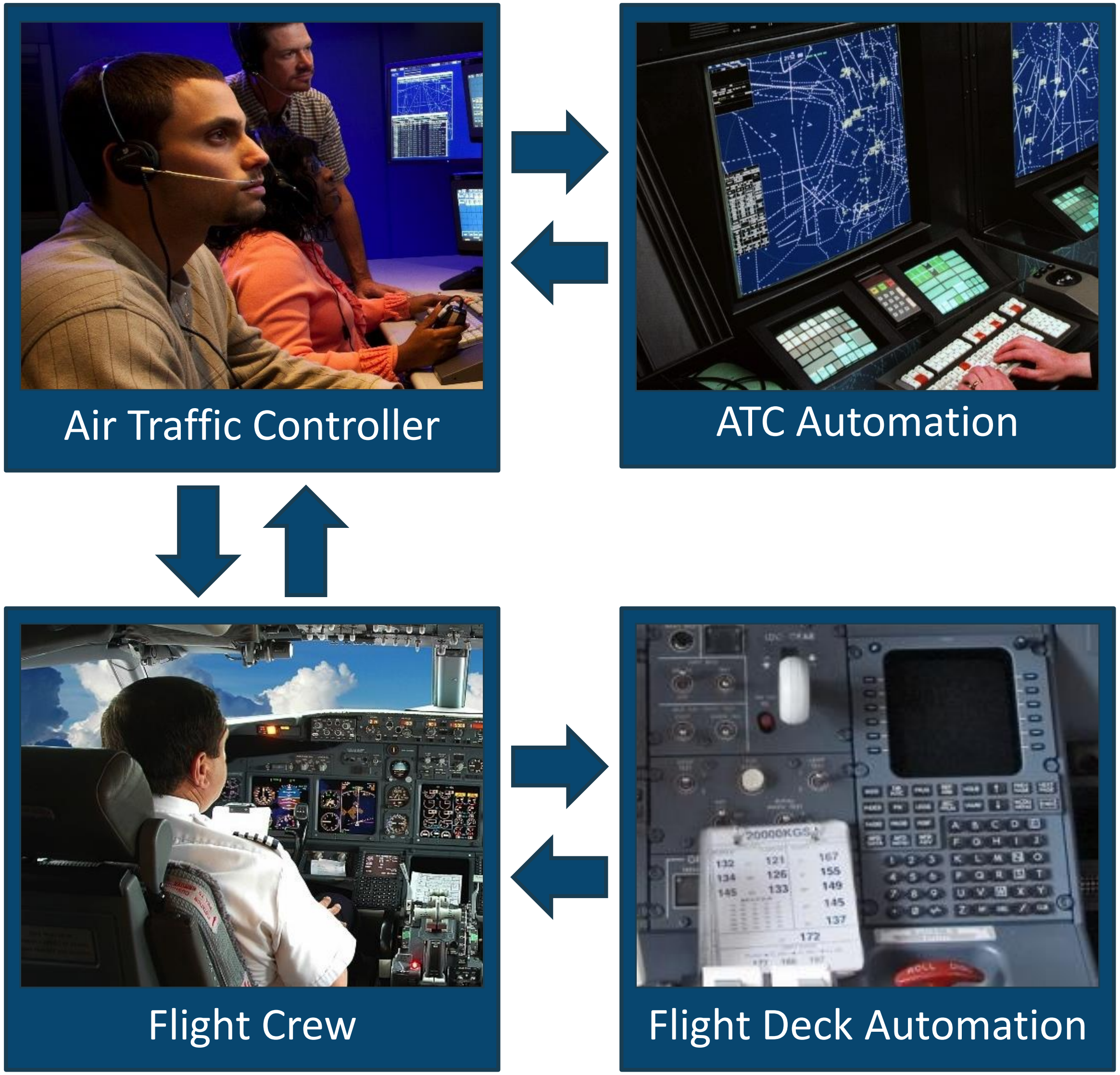
Voice Communications

All in-flight clearances and reroutes are issued via voice

All aircraft in one sector communicate with controller on the same frequency

Current Risks

- Frequency congestion
- Stuck mic – blocked frequency
- Controller workload



Air Traffic Controller

ATC Automation

Flight Crew

Flight Deck Automation

Aviation Communication

Proposed System

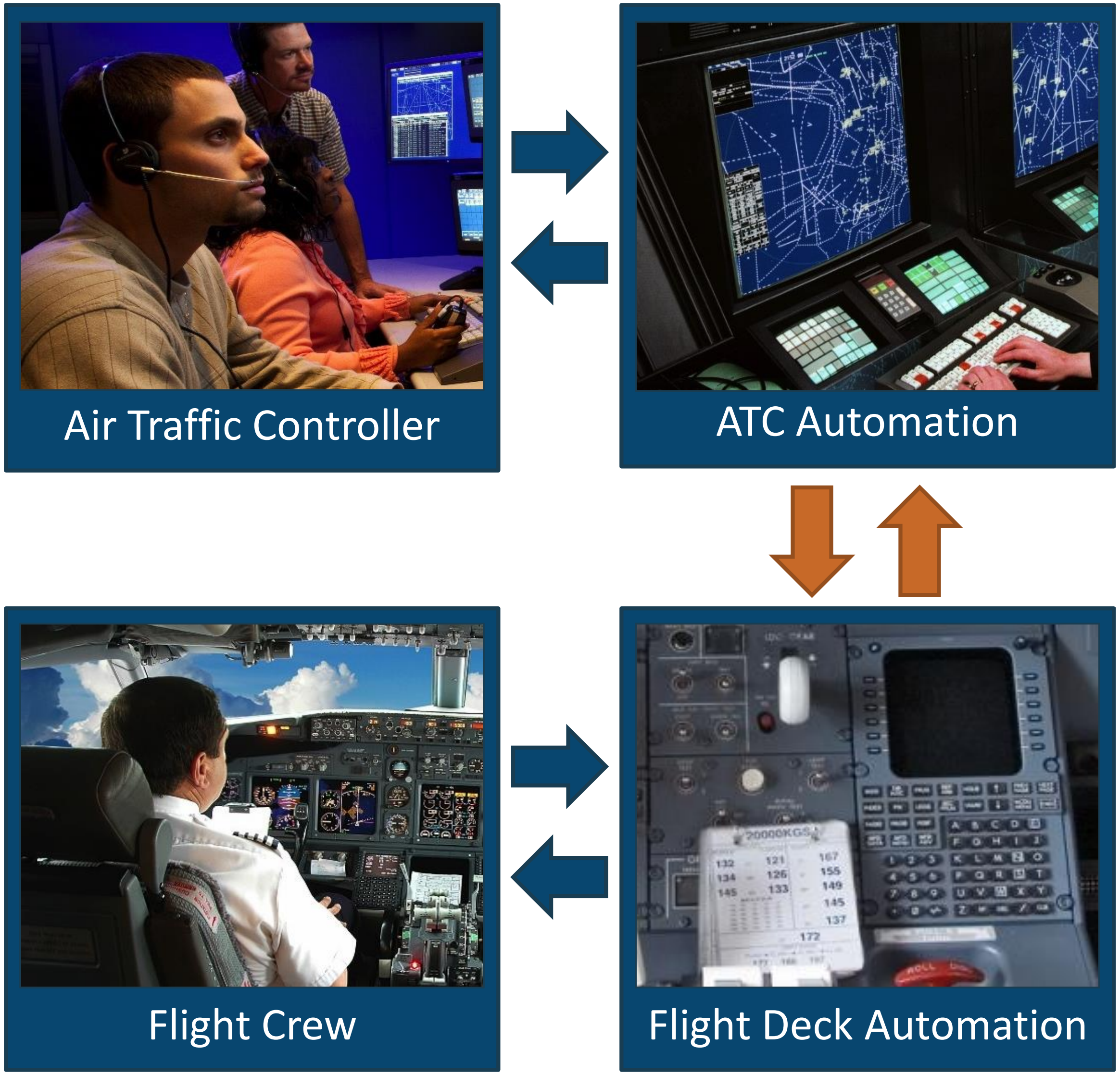
Data Communications

Pre- and in-flight clearances and reroutes are issued via text messages to aircraft

Potential Benefits

- Reduced frequency congestion
- Reduced controller workload

Potential Risks?



Air Traffic Controller

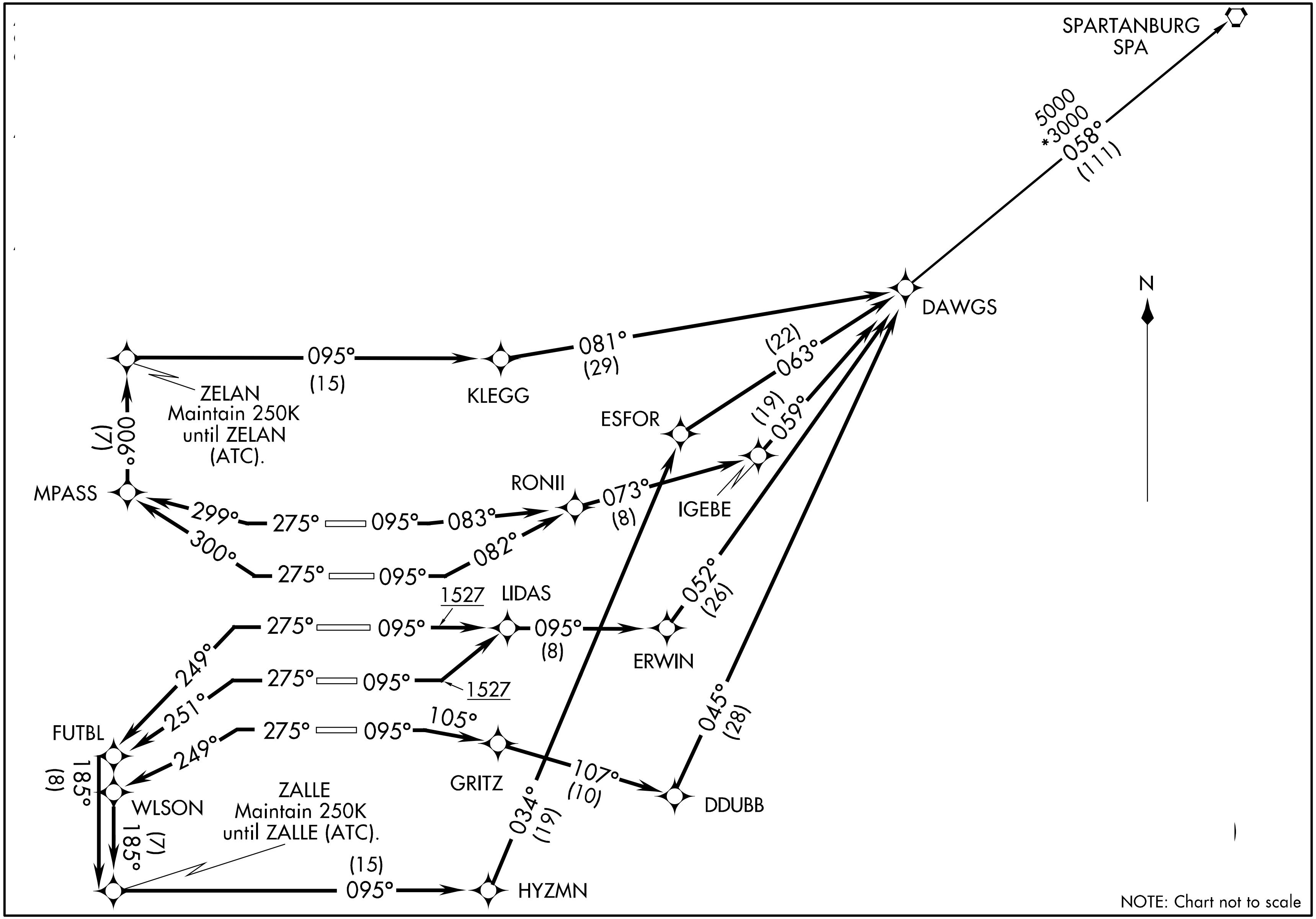
ATC Automation

Flight Crew

Flight Deck Automation

DAWGS SIX DEPARTURE (RNAV)
(DAWGS6.DAWGS) 13010

ATLANTA/ HARTSFIELD-JACKSON ATLANTA INTL (ATL)
ATLANTA, GEORGIA



(DAWGS6.DAWGS) 13010
DAWGS SIX DEPARTURE (RNAV)

ATLANTA/ HARTSFIELD-JACKSON ATLANTA INTL (ATL)
SL-26 (FAA)
ATLANTA, GEORGIA

Step 1: Process Analysis

Concept Description

A Departure Clearance (DCL) Data Comm capability will allow controllers to rapidly issue departure clearance revisions, due to weather or other airspace issues, to one or more aircraft equipped with Data Comm.

The use of Data Comm this type of capability has both safety and efficiency benefits over the current voice-based method of communications between controllers and pilots.

(FAA, 2013)

Human Factors Task Analysis

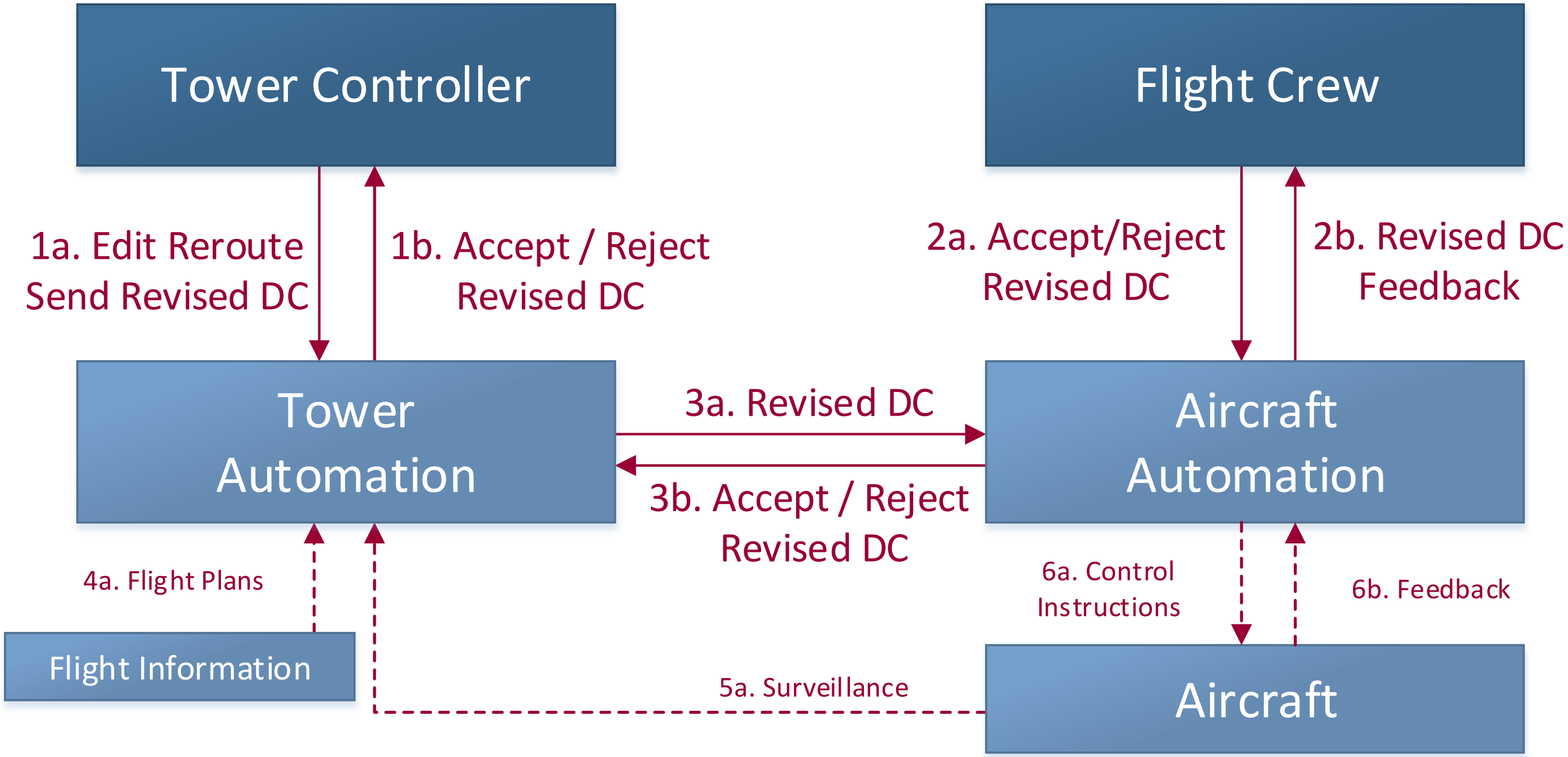
- DCL automation sends controller revised DCL
- Controller reviews and edits DCL
- Controller sends DCL to aircraft via data comm automation
- Aircraft FMS receives and displays DCL to pilots
- Pilots reviews DCL
- Pilots accept or reject DCL
- Pilot updates FMS with revised DCL

Step 1: Process Analysis

HESRA-STPA

Step One
Develop Tasks Analysis & Control Structure

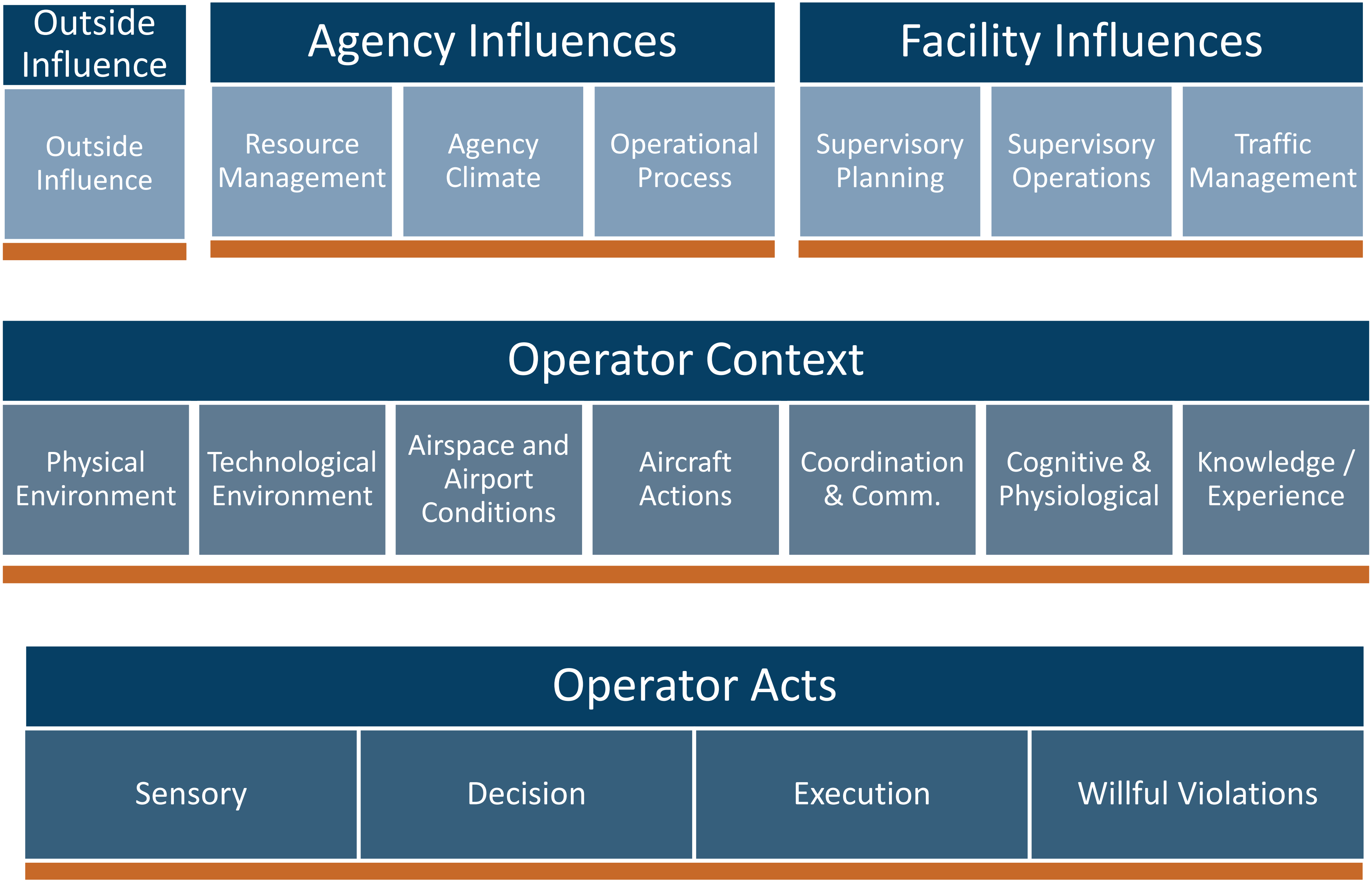
Revised Departure Clearance Via Data Comm



Fort Hill Group

Step 2: Identify Unsafe Actions

Action	Required Action Not Provided	Unsafe Action Provided	Incorrect Timing / Order	Stopped Too Soon / Late
Automation sends DCL to controller				
Controller reviews and edits DCL				
ATC/automation sends data comm DCL to aircraft				
Aircraft FMS displays DCL to pilot				
Pilot reviews the DCL clearance				
Pilots accept or reject DCL via data comm and updates FMS				



Outside Influence

- Outside Influence

Agency Influences

- Resource Management
- Agency Climate
- Operational Process

Facility Influences

- Supervisory Planning
- Supervisory Operations
- Traffic Management

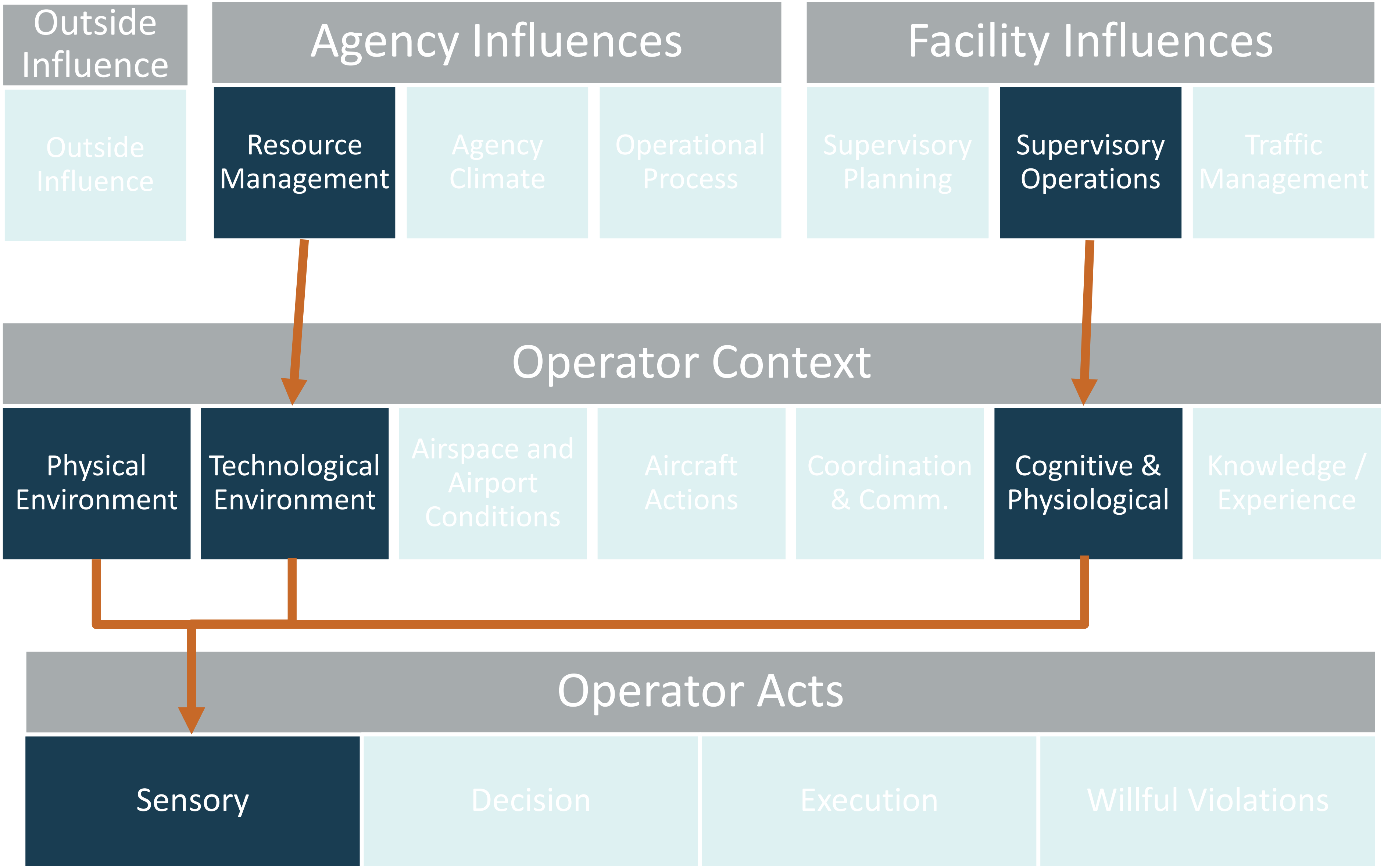
Operator Context

- Physical Environment
- Technological Environment
- Airspace and Airport Conditions
- Aircraft Actions
- Coordination & Comm.
- Cognitive & Physiological
- Knowledge / Experience

Operator Acts

- Sensory
- Decision
- Execution
- Willful Violations

Fort Hill Group



Outside Influence

Agency Influences

Facility Influences

Outside Influence

Resource Management

Agency Climate

Operational Process

Supervisory Planning

Supervisory Operations

Traffic Management

Operator Context

Physical Environment

Technological Environment

Airspace and Airport Conditions

Aircraft Actions

Coordination & Comm.

Cognitive & Physiological

Knowledge / Experience

Operator Acts

Sensory

Decision

Execution

Willful Violations

Step 2: Identify Unsafe Actions

Action	Required Action Not Provided	Unsafe Action Provided	Incorrect Timing / Order	Stopped Too Soon / Late
Automation sends DCL to controller	Fails to send DCL	DCL inadequate for constraint	Delays sending DCL	
Controller reviews and edits DCL		Edited DCL inadequately for constraint		
ATC/automation sends data comm DCL to aircraft	Fails to send DCL	Sends DCL to incorrect aircraft Truncates DCL	Delays sending DCL	
Aircraft FMS displays DCL to pilot	FMS does not display clearance			
Pilot reviews the DCL clearance	Does not notice new data comm DCL message	Does not fully review the DCL	Delays reviewing the DCL clearance	
Pilots accept or reject DCL via data comm and updates FMS	Complies with DCL but fails to update FMS	Mis-keys and accepts DCL when should have been rejected		

- Event requires controller to issue time-sensitive DCL via voice communications. Due to skill degradation, controllers do not properly issue DCL and update automation.
- Controller issues inadequate DCL to aircraft causing conflicting paths between aircraft. Due to lack of party line information, pilots are unaware of conflicting paths.

Step 3 – 4: Define & Assess Hazards to Human Performance

DCL Data Comm Hazard 05					
Hazard Condition	Controller send revised DCL to aircraft via data comm.				
Human Performance Hazard	Controller fails to send revised DCL to aircraft via data comm				
Worst Credible Outcome	Aircraft departs on un-amended route. Aircraft encounters weather or other airspace issue. TRACON controller tactically manages traffic. Potential for conflict or loss of separation minima.				
Hazard Actor	Tower Controller	**Outcome Actor**	TRACON Controller and Pilot		
Severity	Major (3)	**Likelihood**	Remote (3)	**Detection / Recovery**	Moderate (3)
Risk Priority Category	Moderate				

Step 3 – 4: Define & Assess Hazards to Human Performance

DCL Data Comm Hazard 15

Hazard Condition	Controller send DCL to aircraft via data comm.				
Human Performance Hazard	Event requires controller to issue time-sensitive DCL via voice communications. Controller issues DCL via voice but fails to update automation with revised DCL issuance.				
Worst Credible Outcome	Aircraft departs on revised departure clearance. TRACON controller is unaware of revised DCL. TRACON controller issues conflicting instruction to other aircraft. Potential for loss of separation minima. TRACON controller identifies aircraft deviating from flight plan in system and tactically manages traffic flow.				
Hazard Actor	Tower Controller	**Outcome Actor**	TRACON Controller and Pilot		
Severity	Major (3)	**Likelihood**	Remote (3)	**Detection / Recovery**	Moderate (3)
Risk Priority Category	High				

Step 5: Prioritize Hazards to Human Performance

Risk Priority Category	DCL Data Comm Hazards
Extremely High	0
High	4
Moderate	5
Low	5
Extremely Low	2

- Controller issues data comm clearance that is in response to a time-sensitive, emergency event
- Controller delays sending DCL data comm message
- Pilots delay reviewing the CDL data comm message
- Data comm automation truncates DCL message

Step 6: Develop Mitigation Strategies

Data Comm Hazard 09	
Hazard Condition	Pilot reviews the DCL message.
Human Performance Hazard	Pilot delays reviewing the DCL.
Worst Credible Outcome	Original clearance is no longer valid for situation. Potential for conflict with weather or other adverse situation.

Sample Mitigation Strategies

UAL123
Depart Runway 27L with 240 Heading

Clearance valid for
05:00.00

- Functional Design Requirements
  - The FMS shall incorporate a validity timer for time-sensitive clearances.
- Research Requirements
  - How much time should be included for clearance delivery to aircraft and for pilot decision-making?
- Training Requirements
  - Develop training for pilots on how to understand and respond to validity timer.

Questions

Michael Sawyer

Michael.Sawyer@FortHillGroup.com

Katie Berry

Katie.Berry@FortHillGroup.com

www.FortHillGroup.com

Fort Hill Group

We would like to acknowledge the FAA Human Factors Division (ANG-C1) for funding and supporting this work