Proactively Examining NextGen Human Performance and System Safety

An Application of a Modified STPA in Air Traffic Control

Fort Hill Group

www.FortHillGroup.com
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.
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
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

Controller

Process Model

Controlled Process

Actor

Process Model

Actions

Feedback

Control Actions

Feedback
• 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
<table>
<thead>
<tr>
<th>Category</th>
<th>Definition/Action</th>
</tr>
</thead>
</table>
| 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
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*
# Proactive Human Performance Assessment Methodology Components

<table>
<thead>
<tr>
<th>HESRA</th>
<th>STPA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Human Error Safety Risk Assessment</td>
<td>System Theoretic Process Analysis</td>
</tr>
<tr>
<td>Identifies and prioritizes human performance hazards and potential hazard outcomes</td>
<td>Treats accidents as dynamic control problems using control structures and safety constraints</td>
</tr>
<tr>
<td>Limited view of system impacts</td>
<td>Limited view of human performance</td>
</tr>
</tbody>
</table>
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
• 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

<table>
<thead>
<tr>
<th>Fiscal Year</th>
<th>FY 2012</th>
<th>FY 2013</th>
<th>FY 2014</th>
<th>FY 2015</th>
<th>FY 2016+</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OI 102406:</td>
<td>Situational Awareness and Alerting of Ground Vehicles</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>2</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OI 103207:</td>
<td>Improved Runway Safety Situational Awareness for Controllers (2012-2016)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OI 103208:</td>
<td>Expansion of Surface Surveillance¹</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>3</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OI 103208:</td>
<td>Improved Runway Safety Situational Awareness for Pilots (2012-2016)²</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>4</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OI 104205:</td>
<td>Revised Departure Clearance via Data Comm³</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OI 104205:</td>
<td>Task Force 39</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Provide Initial Surface Management System⁵</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Stand up TFDM Scheduler/Sequencer</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(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?
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

Revised Departure Clearance Via Data Comm

- Tower Controller
  - 1a. Edit Reroute
    - Send Revised DC
  - 1b. Accept / Reject
    - Revised DC

- Tower Automation
  - 3a. Revised DC
    - 3b. Accept / Reject
      - Revised DC

- Flight Crew
  - 2a. Accept/Reject
    - Revised DC

- Aircraft Automation
  - 2b. Revised DC
    - Feedback

- Aircraft
  - 5a. Surveillance
  - 6a. Control Instructions

- Flight Information
  - 4a. Flight Plans
  - 6b. Feedback

Fort Hill Group
## Step 2: Identify Unsafe Actions

<table>
<thead>
<tr>
<th>Action</th>
<th>Required Action Not Provided</th>
<th>Unsafe Action Provided</th>
<th>Incorrect Timing / Order</th>
<th>Stopped Too Soon / Late</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automation sends DCL to controller</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Controller reviews and edits DCL</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ATC/automation sends data comm DCL to aircraft</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Aircraft FMS displays DCL to pilot</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pilot reviews the DCL clearance</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pilots accept or reject DCL via data comm and updates FMS</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Step 2: Identify Unsafe Actions

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

- 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.
### DCL Data Comm Hazard 05

<table>
<thead>
<tr>
<th>Hazard Condition</th>
<th>Controller send revised DCL to aircraft via data comm.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Human Performance Hazard</strong></td>
<td>Controller fails to send revised DCL to aircraft via data comm</td>
</tr>
<tr>
<td><strong>Worst Credible Outcome</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Hazard Actor</strong></td>
<td>Tower Controller</td>
</tr>
<tr>
<td><strong>Severity</strong></td>
<td>Major (3)</td>
</tr>
<tr>
<td><strong>Risk Priority Category</strong></td>
<td>Moderate</td>
</tr>
</tbody>
</table>
### DCL Data Comm Hazard 15

<table>
<thead>
<tr>
<th>Hazard Condition</th>
<th>Controller send DCL to aircraft via data comm.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Human Performance Hazard</td>
<td>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.</td>
</tr>
<tr>
<td>Worst Credible Outcome</td>
<td>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.</td>
</tr>
<tr>
<td>Hazard Actor</td>
<td>Tower Controller</td>
</tr>
<tr>
<td>Outcome Actor</td>
<td>TRACON Controller and Pilot</td>
</tr>
<tr>
<td>Severity</td>
<td>Major (3)</td>
</tr>
<tr>
<td>Likelihood</td>
<td>Remote (3)</td>
</tr>
<tr>
<td>Detection / Recovery</td>
<td>Moderate (3)</td>
</tr>
<tr>
<td>Risk Priority Category</td>
<td>High</td>
</tr>
</tbody>
</table>
### Step 5: Prioritize Hazards to Human Performance

<table>
<thead>
<tr>
<th>Risk Priority Category</th>
<th>DCL Data Comm Hazards</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extremely High</td>
<td>0</td>
</tr>
<tr>
<td>High</td>
<td>4</td>
</tr>
<tr>
<td>Moderate</td>
<td>5</td>
</tr>
<tr>
<td>Low</td>
<td>5</td>
</tr>
<tr>
<td>Extremely Low</td>
<td>2</td>
</tr>
</tbody>
</table>

- 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

<table>
<thead>
<tr>
<th>Hazard Condition</th>
<th>Pilot reviews the DCL message.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Human Performance Hazard</td>
<td>Pilot delays reviewing the DCL.</td>
</tr>
<tr>
<td>Worst Credible Outcome</td>
<td>Original clearance is no longer valid for situation. Potential for conflict with weather or other adverse situation.</td>
</tr>
</tbody>
</table>

Sample Mitigation Strategies

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