



Using STPA trend analysis to determine key system drivers

Katherine Belvin

Product Review Engineer

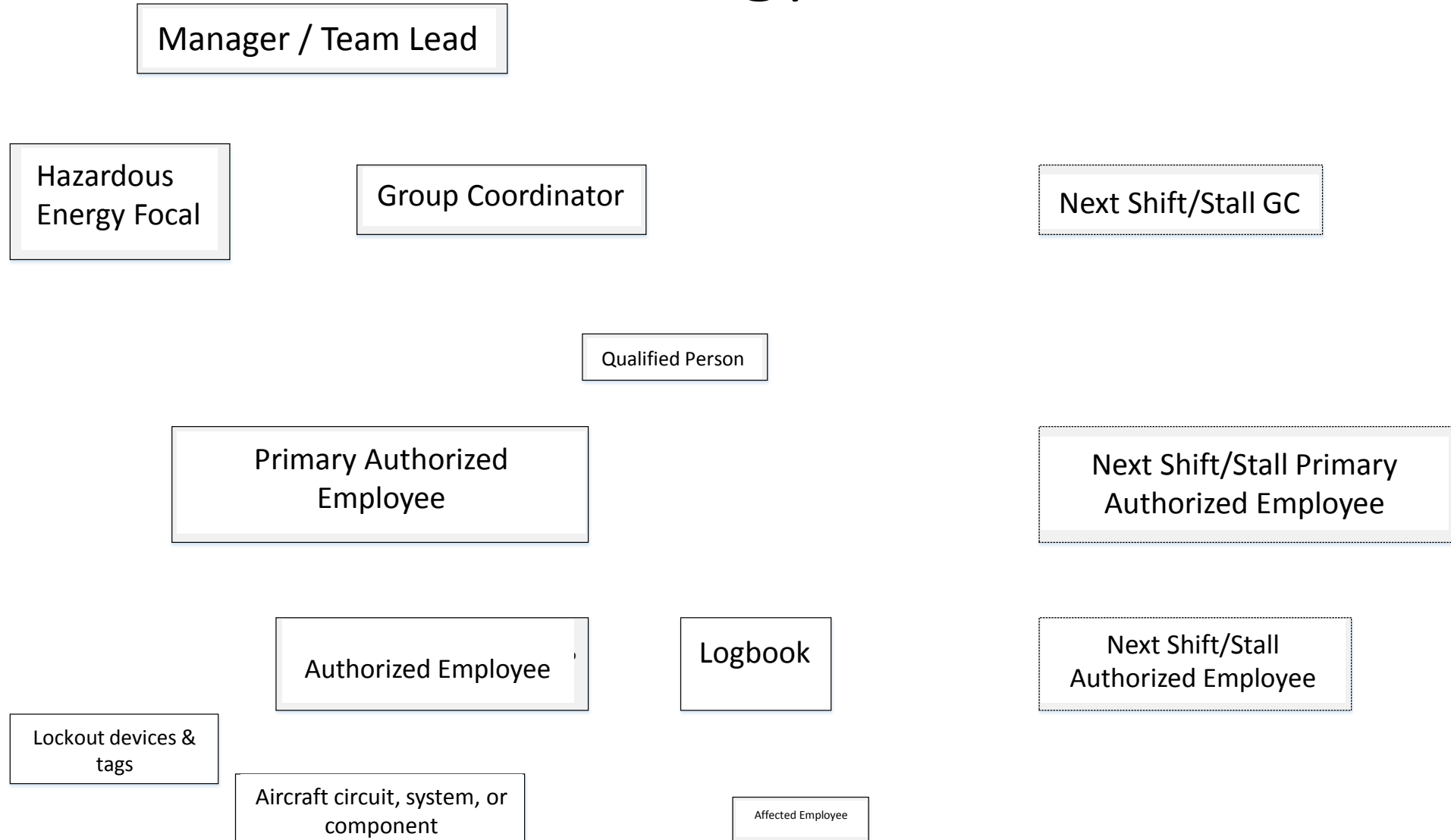
March 27, 2017

Notwithstanding any assignment or transfer to the Publisher, or any other terms of this Agreement, the rights granted by Boeing to Publisher are limited as follows: (i) any rights granted by Boeing to the Publisher are limited to the work-made-for-hire rights Boeing enjoys in the Work; (ii) Boeing makes no representation or warranty of any kind to the Publisher or any other person or entity regarding the Work, the information contained therein, or any related copyright; and (iii) Boeing retains a non-exclusive, perpetual, worldwide, royalty-free right, without restriction or limitation, to use, reproduce, publicly distribute, display, and perform and make derivative works from the Work, and to permit others to do so.

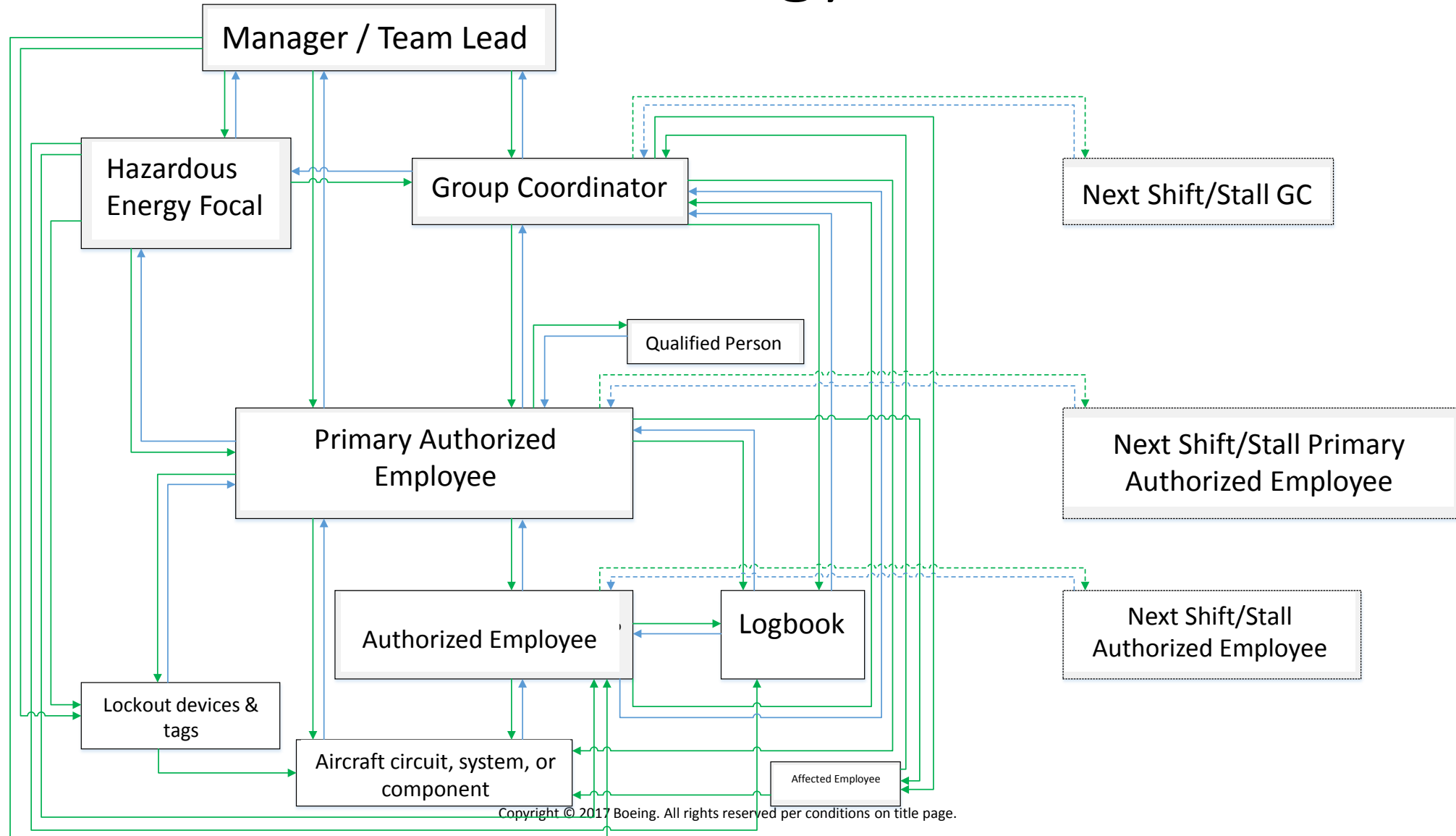
Introduction

- Aircraft production is complex and can be hazardous
- Hazardous energy managed via Lockout-Tagout (LOTO)
 - Group Coordinator
 - Primary Authorized Employee
 - Authorized Employee
- Why do LOTO-related incidents and injuries occur?
- STPA method applied to LOTO
- Goal: Implement the most effective solutions

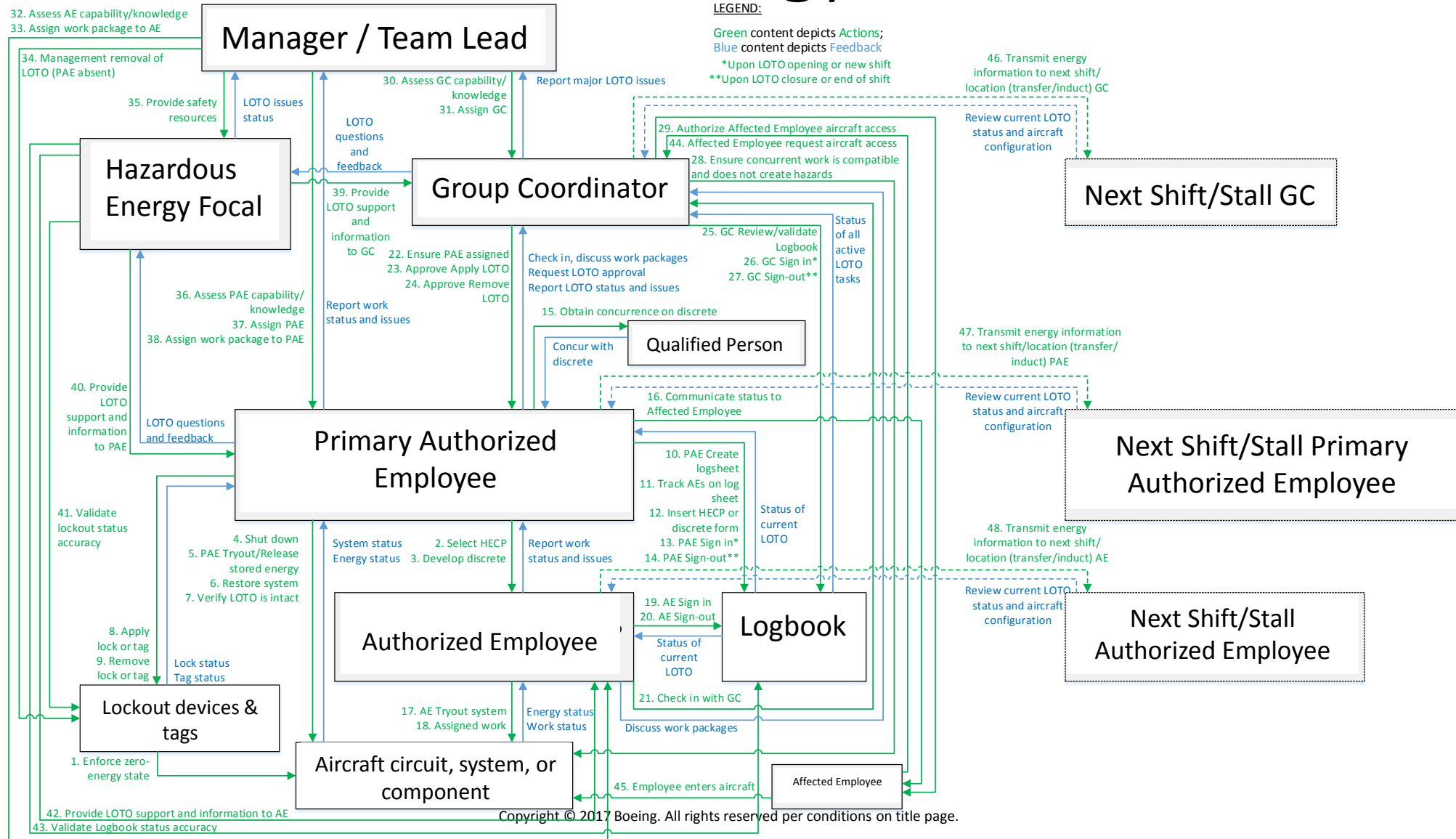
STPA for Hazardous Energy Control



STPA for Hazardous Energy Control

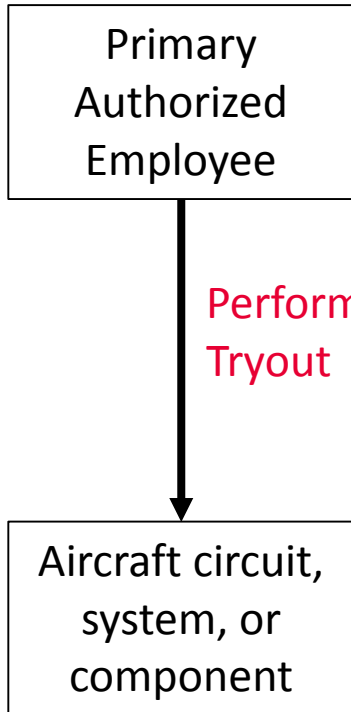


STPA for Hazardous Energy Control



STPA Example

Controller & Control Action



Unsafe Control Actions

Performing Tryout is Made Unsafe By:

- Performing Tryout on the wrong component
- Performing Tryout procedure incorrectly
- **Performing the wrong Tryout procedure**
- Not performing Tryout
- Performing Tryout too late
- Performing Tryout too soon (before energy is released)

Causal Scenarios

Wrong Tryout Procedure Used Because:

- Employee doesn't know it's the wrong procedure
- Employee could not find the right procedure
- Employee was rushed and did not want to find the right procedure
- Higher authority employee suggested the procedure
- Etc....

STPA Limitations

- Analysis results in too much data for easy comprehension
 - Controllers: 13
 - Control actions: 48
 - Unsafe control actions: **200**
 - Causal scenarios that could result in incidents or injury: **958**

Challenges

- How to put all of this data into context of the “bigger picture”?
- How to translate that knowledge into business decisions?

Applying Trend Grouping

Three categories of system drivers:

- Mental models
- Inadequate information or resources
- Process deficiency

Which of these causes the greatest systemic impact?

How are they related?

How to prioritize and estimate improvement?

Category Drivers by Group

Mental Models

Reacting to time pressure

Believed to be inconsequential

Belief that another employee did / will perform task

Attention was diverted

Situational misperception

Resources / Information

Required people cannot be located

Production complexity

Unavailable information

Required resources cannot be located

Device failure

Process

Inadequate training / experience

Unclear role assignments

Unclear requirements

Process unenforced

Unclear authority

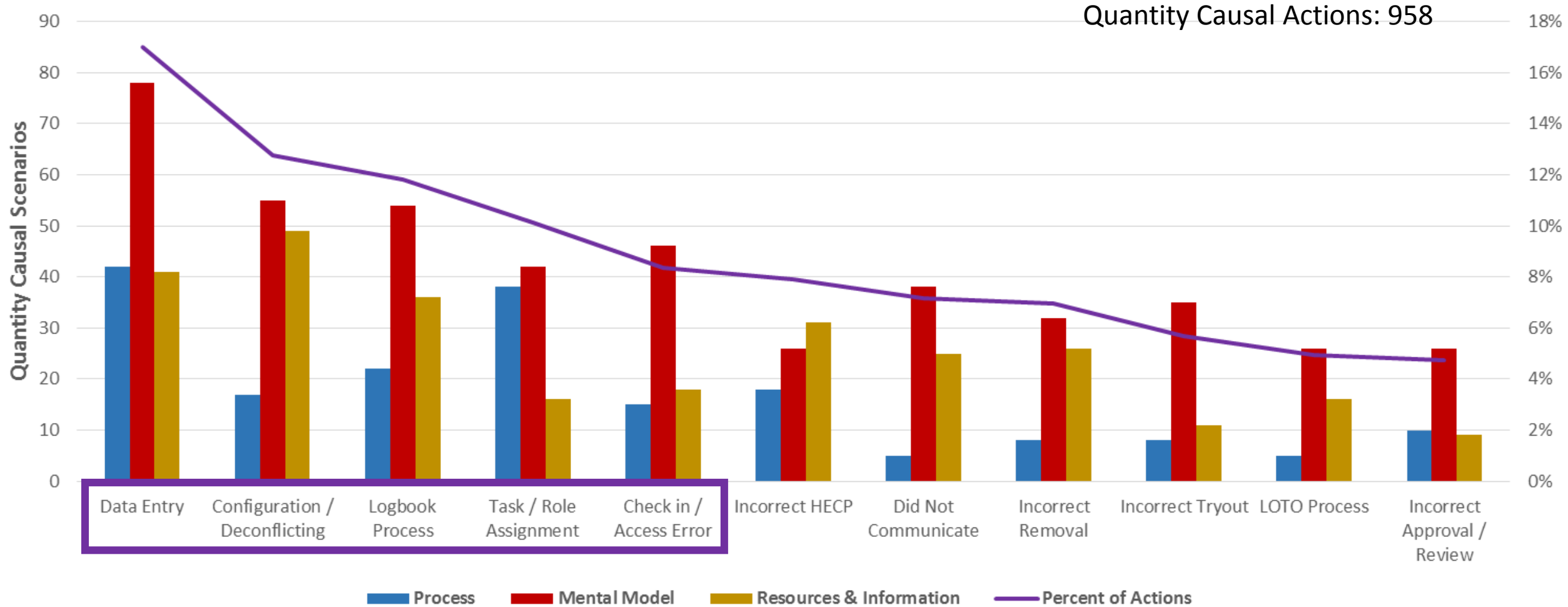
Trend Grouping Example

- Controller: Primary Authorized Employee (PAE)
 - **Unsafe Control Action:** Performs incorrect Tryout procedure because...
 - **Causal Scenario:** ... PAE was given an incorrect procedure, does not know where to find procedures and believes that taking the time to find a correct one would result in unacceptable production delay.
 - **Trend Grouping: Assigning Key Drivers**
 - **Causal Action: Incorrect Tryout**
 - **Mental Model: Reacting to Time Pressure**
 - **Resource / Information Deficiency: Required resources cannot be located**
 - **(no process driver)**

Results

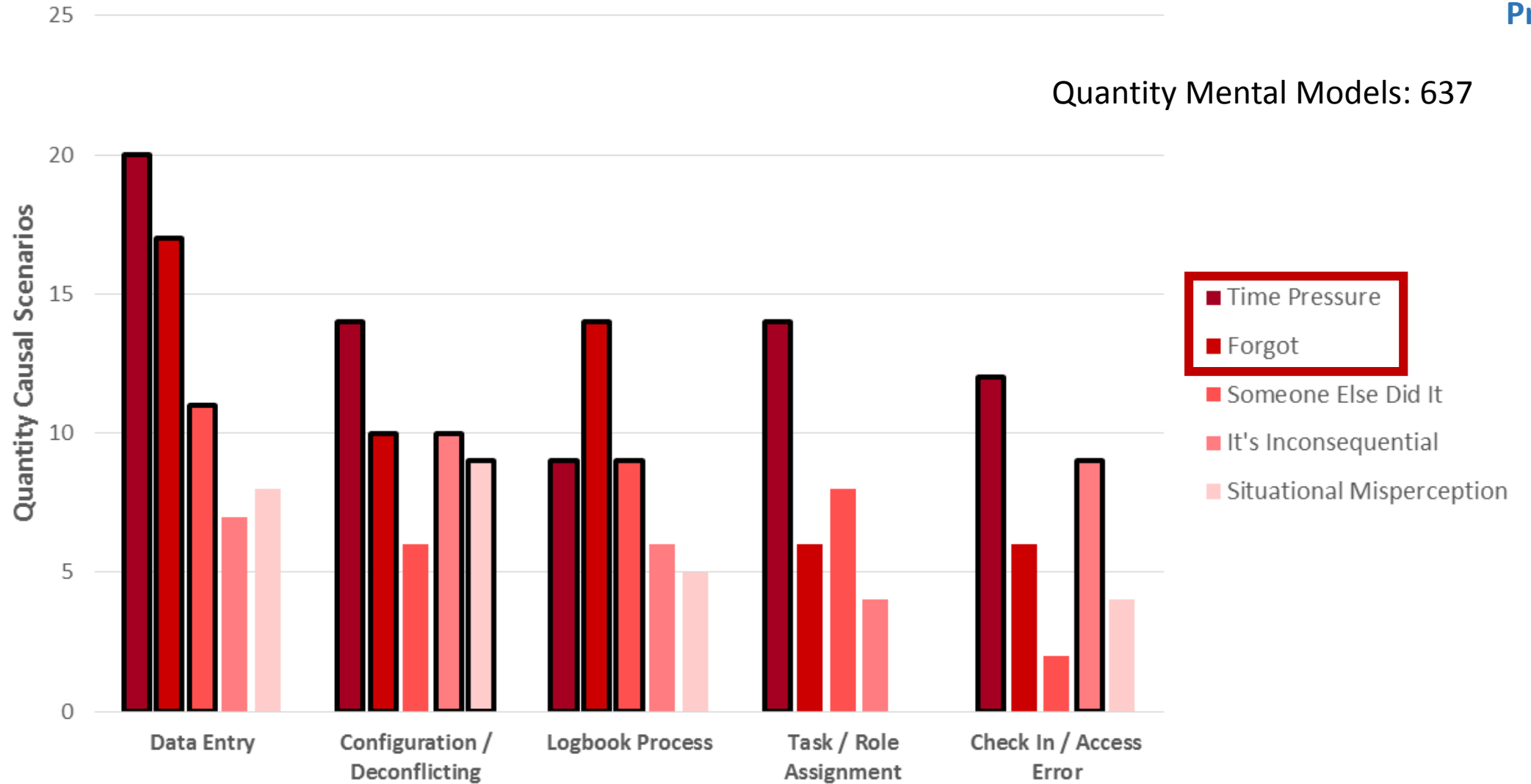
Actions Breakdown

Actions
Mental Model
Resources & Information
Process



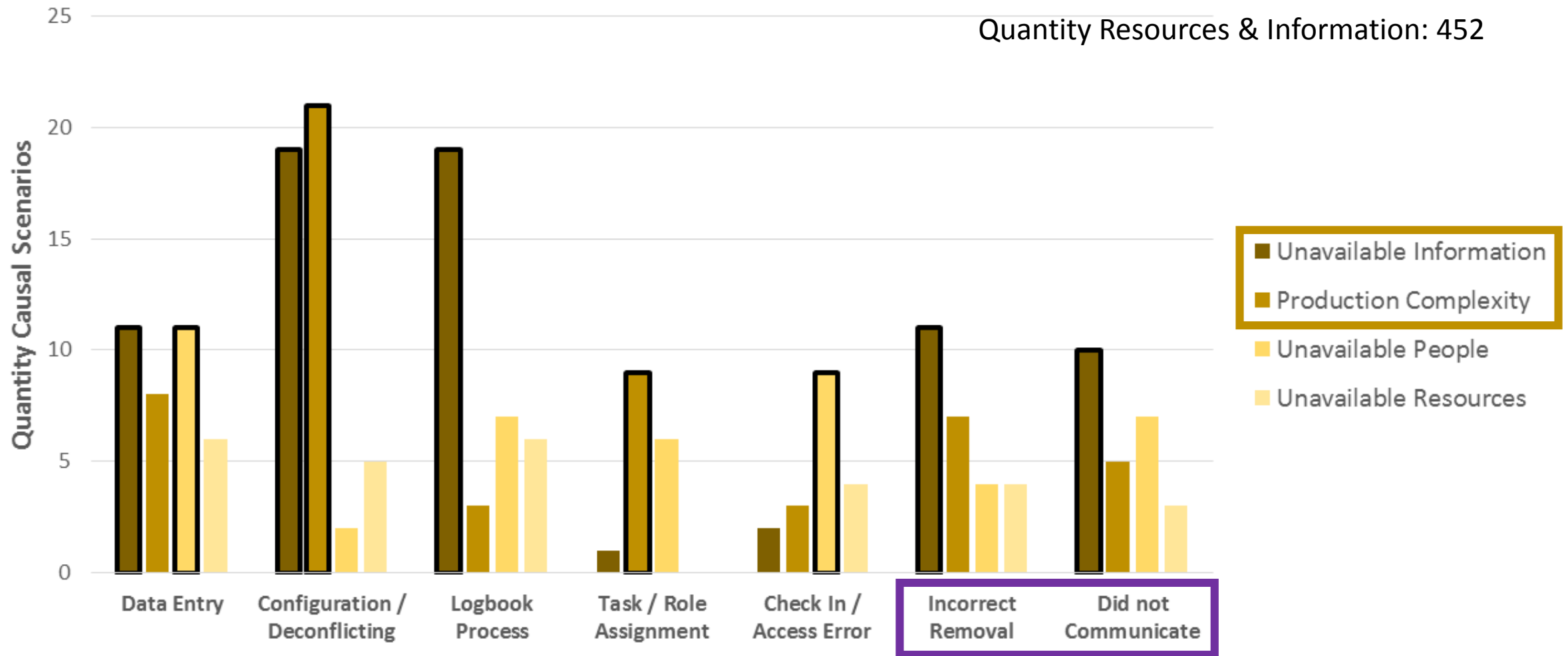
Top Mental Models by Action

Actions
Mental Model
Resources & Information
Process



Top Resources & Information by Action

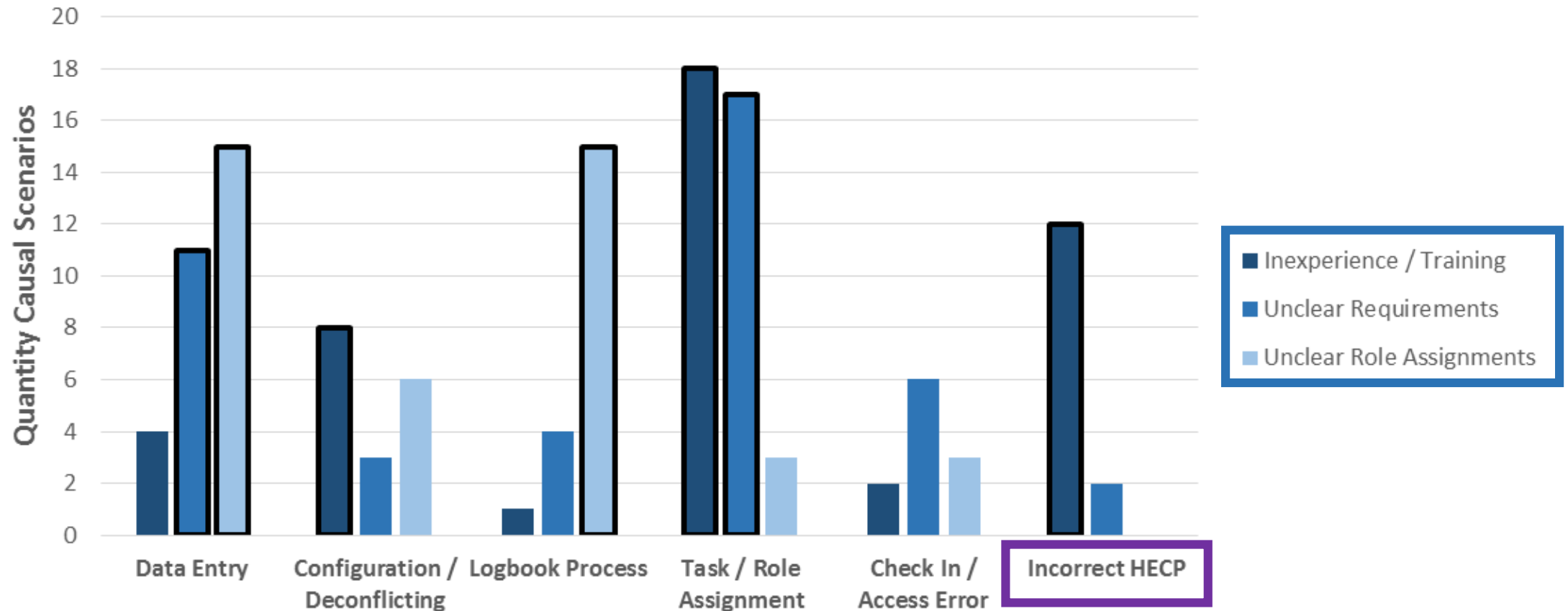
Actions
Mental Model
Resources & Information
Process



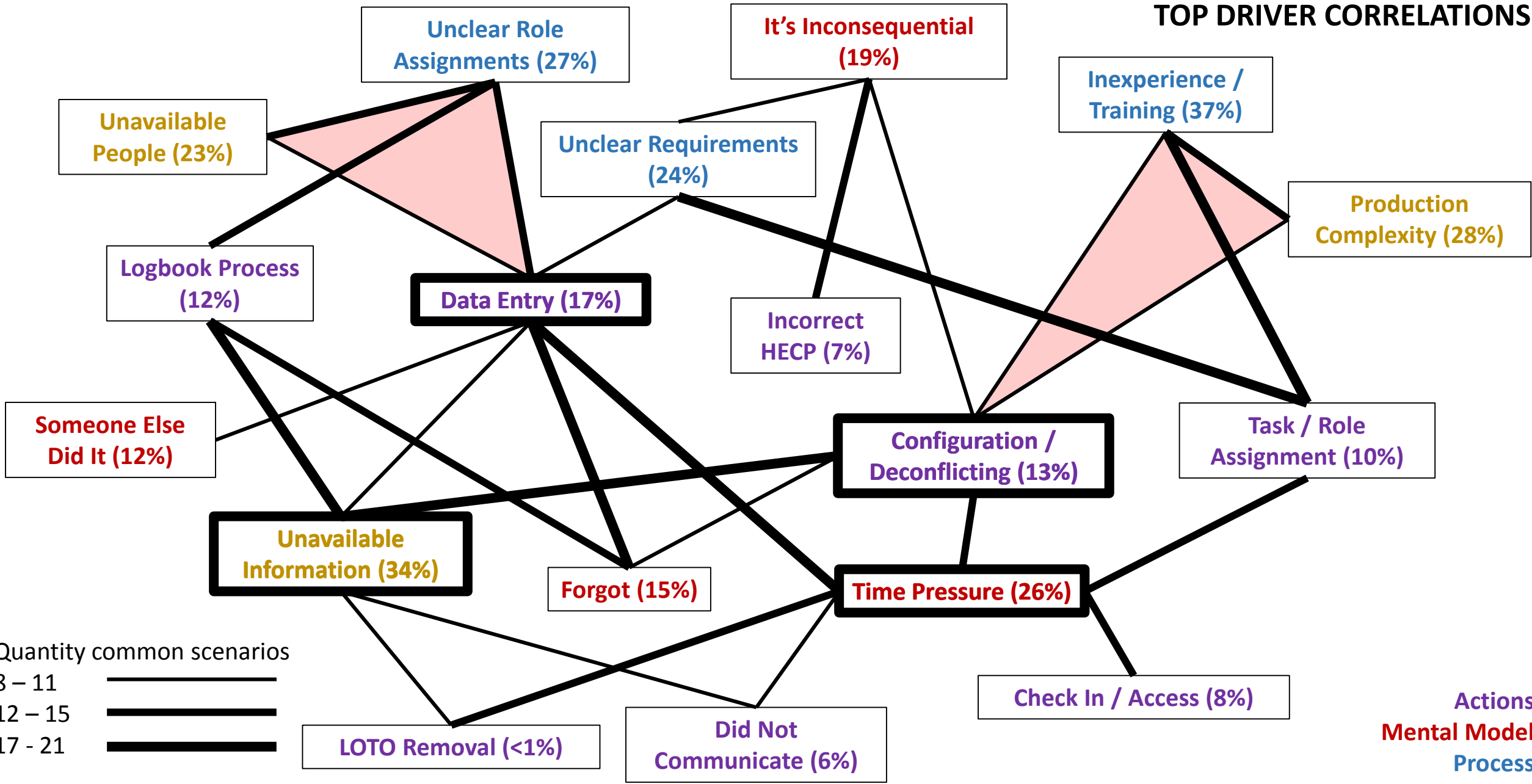
Top Processes by Action

Actions
Mental Model
Resources & Information
Process

Quantity Process: 295



TOP DRIVER CORRELATIONS



How STPA Results Translate to Business Priorities

Main Message: Focus on Areas with Greatest Systemic Impact

Highest Priority Actions

- Focus on Reduction in Data Entry
 - Correlated with over half each of **Mental Model** and **Resource & Information** drivers
- Improve Accessibility to Information
 - Strong relationship with **Configuration / Deconflicting** errors
- Simplify Administrative Tasks
 - A third of causal actions are correlated with **Time Pressure** driver

Lowest Priority Actions

- Revamp LOTO **process**: Smallest group of assigned drivers
- Heavier emphasis on “compliance”

Summary

- STPA provides detailed insight to incident and injury causality mechanisms
- Large quantities of data are generated
- Cut through complexity with trend grouping
- Enables prioritization of improvements based on estimated impact

