Disclaimer: The information in this presentation is not intended as direction or recommendations, but simply sharing how the Boeing Company is using STAMP to make our workplace safer.

STAMP in Workplace Safety

Emily Howard
Senior Technical Fellow
March 27, 2017

The Team

Boeing

Dr. Emily Howard, Senior Technical Fellow, Human Factors, Defense, Space & Security
Katherine Belvin, Liaison Engineer, Defense, Space & Security
Paul Staszak, Systems Engineer, Defense, Space & Security
Shawna Murray, Health & Safety Specialist, Environment, Health & Safety
Liz Juhnke, User Experience Designer, Information Technology & Data Analytics

Liberty Mutual Research Institute for Safety

Dr. Larry Hettinger, Principal Research Scientist, Human Factors Engineering

MIT

Megan France, Master's Candidate, Aeronautics and Astronautics (Human Factors)

Outline

- Project Overview
- Role of Human Factors
- Overview of Workplace Safety
- Exercise: Application of STPA
  - Control Structure
  - Unsafe Control Actions
  - Causal Scenarios
- Summary and Conclusions

How We Got Involved with STAMP

Recent challenge from our CEO: ***"Achieve step function improvement in workplace safety"***

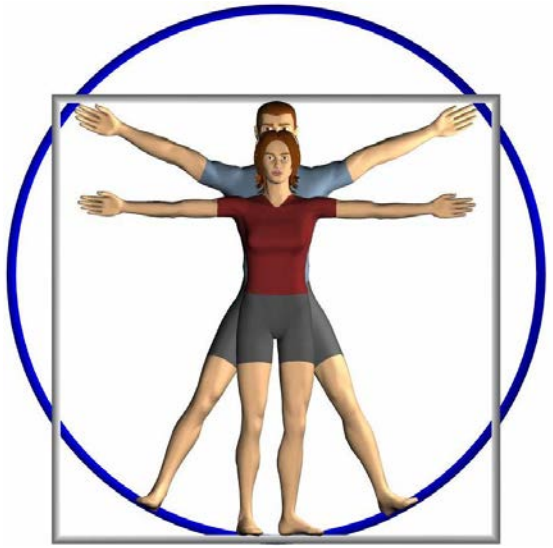
The engineering vice-president for Boeing Defense, Space and Security retained the services of Dr. Nancy Leveson in May 2015.

Guided by Dr. Leveson, a limited engineering study team has embarked on a 3 year journey to explore STAMP methodology and determine its feasibility for application to workplace safety.

Dr. Leveson recommended reaching out to Liberty Mutual Research Institute for Safety who have partnered with us.

Our Safety Analyses Start with a Specific View of Human Factors

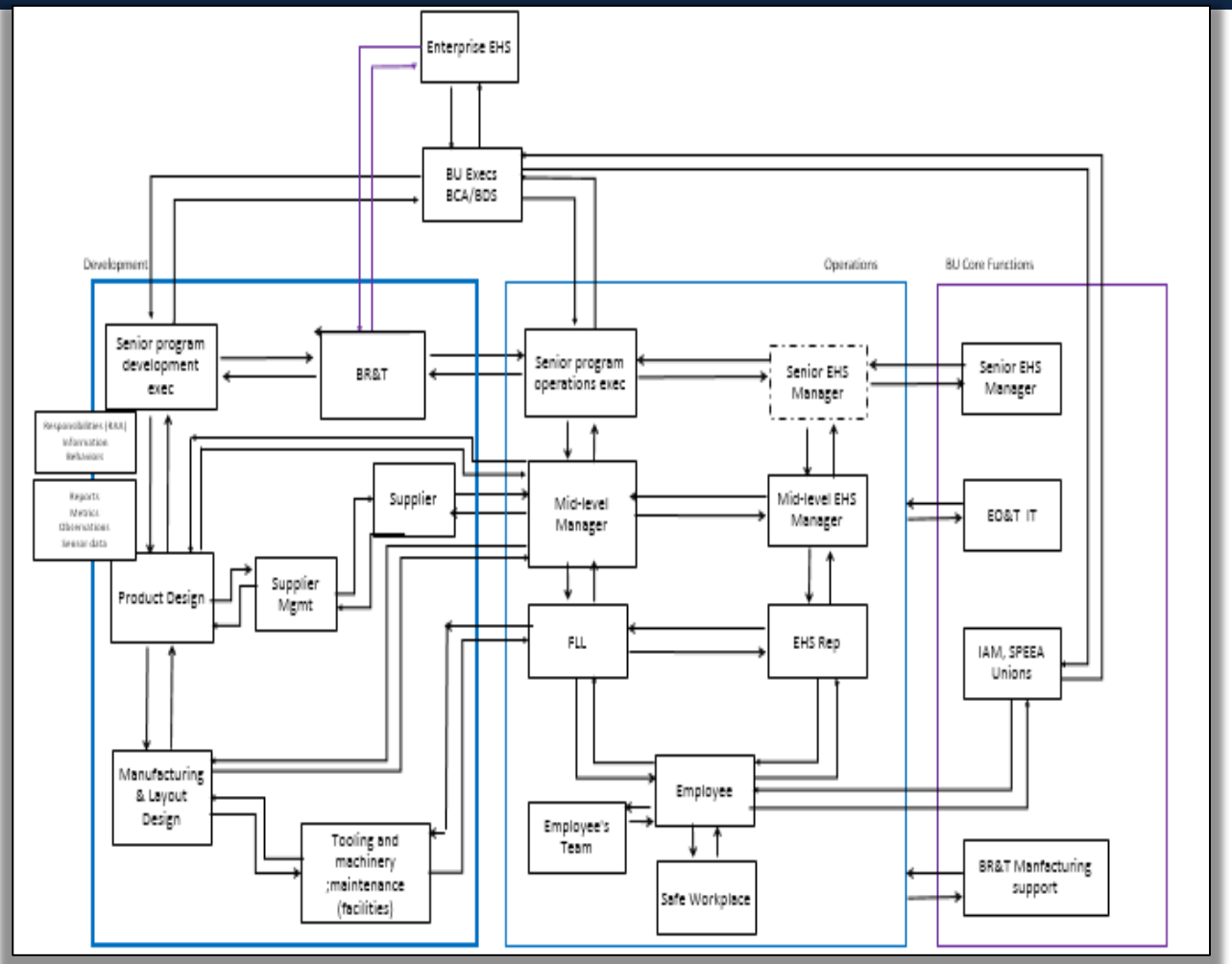
- Boeing's human factors' expertise derives from decades of commercial and military aviation research.
  - Our mission success can only be assured through successful human performance.
- Our goal is to identify systemic influences on human judgment and behavior.
- Don't stop with what people did wrong, but try to understand why it made sense to them to do what they did.
- Determine how to change the environment in order to change the human behavior.



Focus on changing the environment, process and/or tools rather than trying to change the person!

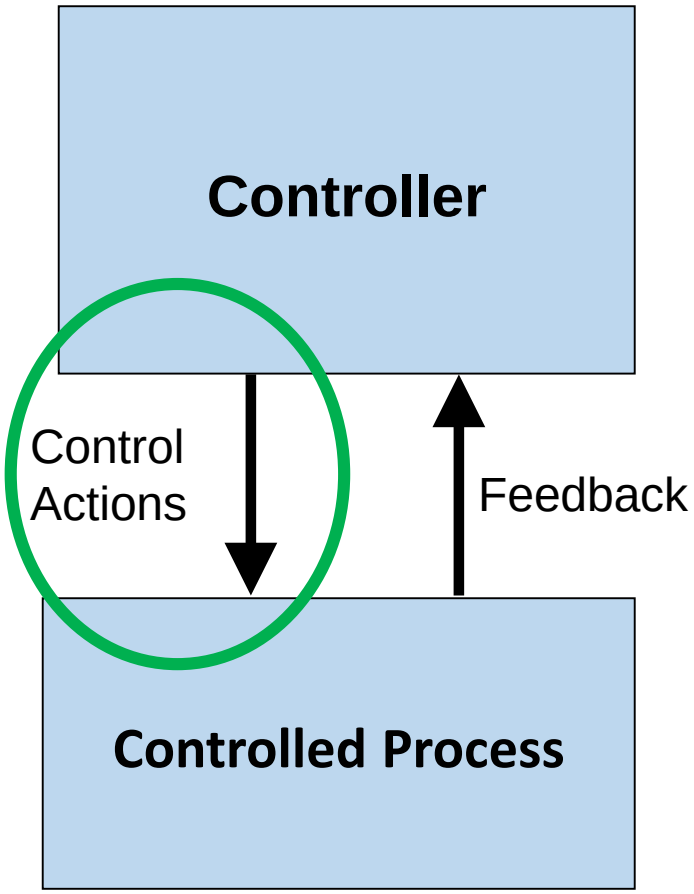
Building a Control Structure at Boeing

- Includes assigned role, action (decisions/behaviors) and feedback (information/metrics) loop
- Utilizes product safety practices applied to the workplace
  - Addresses hazards in both development and operations
- Used for engineering analysis to reveals systemic causal conditions of incidents (safety and quality)



Action and Feedback Loops for All Controlled Processes

STPA: Hazard Analysis Based Upon Safety Control Structure



- Systems Theoretic Process Analysis (STPA) provides a systematic way to identify or anticipate hazards, due to unsafe control actions
- STPA utilizes a control structure diagram, which represents system behavior as the interaction between a controller and a controlled process
- Four types of unsafe control actions:
  - Control actions are not executed when they are required for safety
  - Control actions are executed when they should not have been
  - Potentially safe actions are executed too early, too late
  - An extended control action stops too soon or is applied too long

Generic Exercise:
Lock Out Tag Out Try Out (LOTO)

OSHA 29 CFR 1910.147: *requires employers to establish a program and utilize procedures for affixing appropriate lockout devices or tagout devices to energy isolating devices, and to otherwise disable machines or equipment to prevent unexpected energization, start up or release of stored energy in order to prevent injury to employees.*

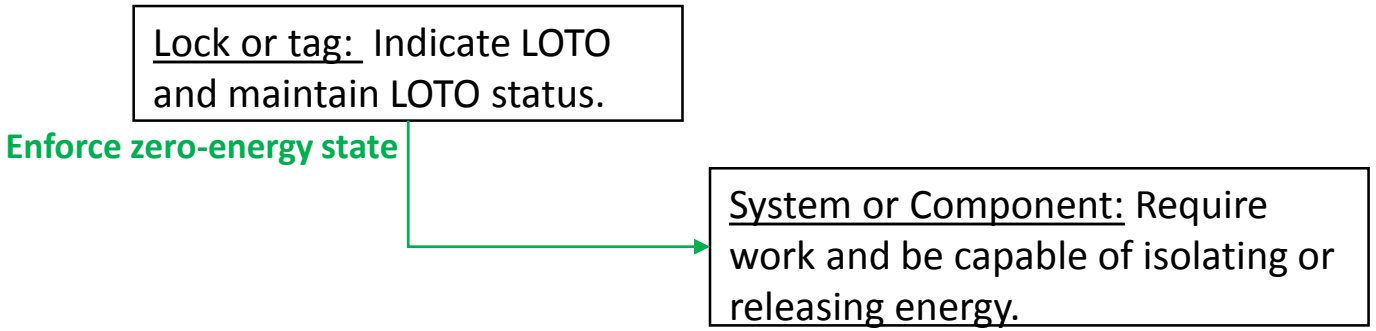
1. What is the undesired accident or loss?
2. What is the associated hazard?
3. What is the primary safety constraint for the system?
4. What are the controllers and process(es) that make up this system?

Generic Exercise:
Lock Out Tag Out Try Out (LOTO)

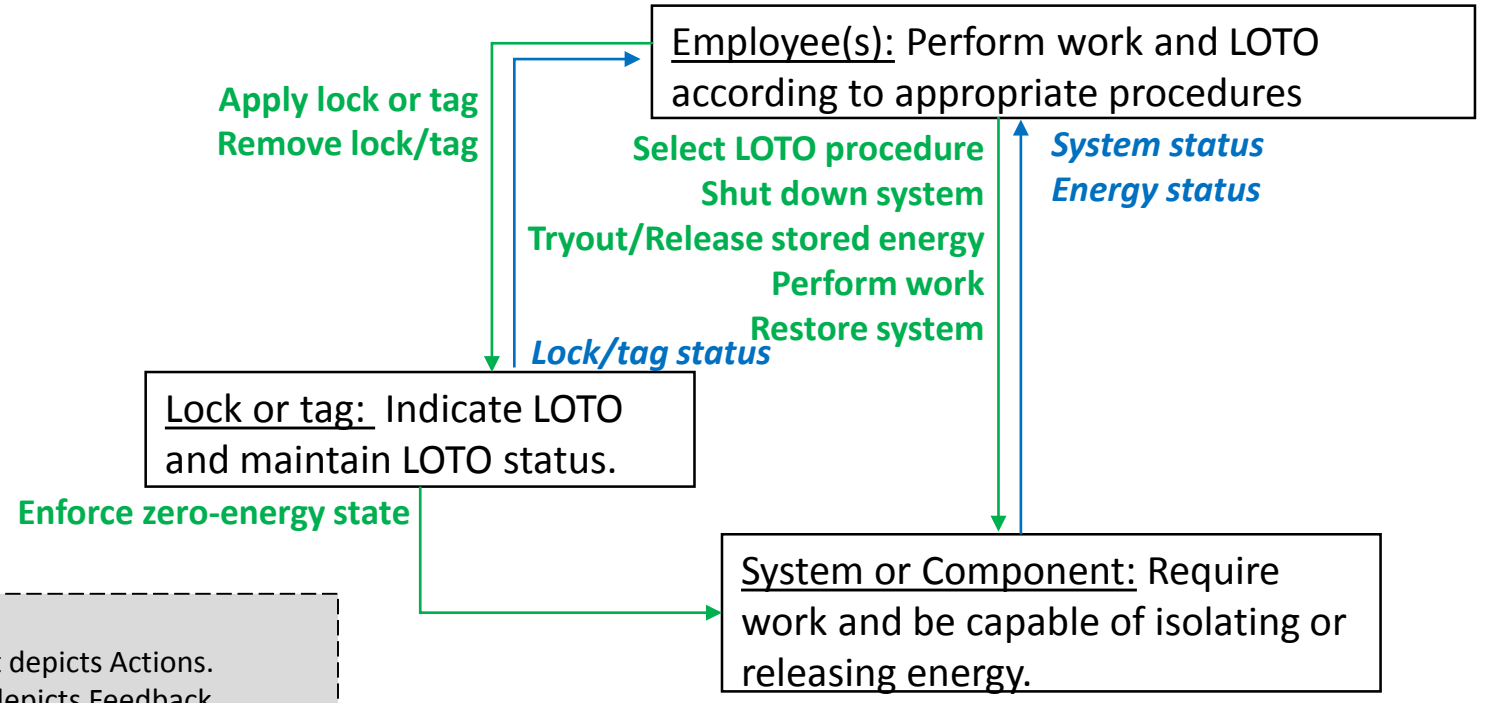
Accident or Loss	Hazard	Safety Constraint
A-1: Workers are killed or injured on the job.	H-1: Workers are exposed to hazardous energy.	SC-1: Workers shall not be exposed to hazardous energy.

Try your hand at creating a simple LOTO control model, adding an employee to the model below and showing the actions and feedback

OSHA 29 CFR 1910.147: *requires employers to establish a program and utilize procedures for affixing appropriate lockout devices or tagout devices to energy isolating devices, and to otherwise disable machines or equipment to prevent unexpected energization, start up or release of stored energy in order to prevent injury to employees.*



Possible Answer:
Simple LOTO Control Model



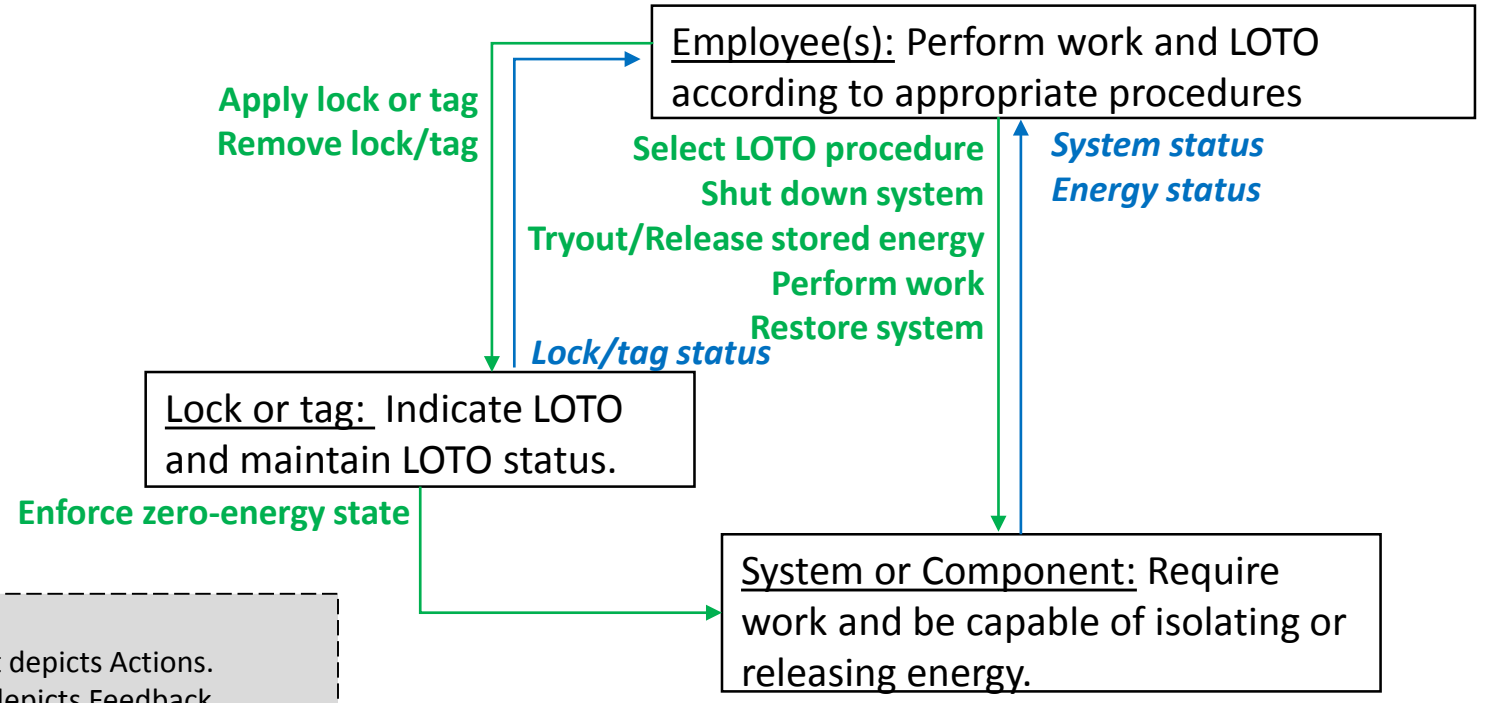
LOTO Complexities—what if you added another employee?

Primary Employee. A Primary Employee (PE) is appointed …when work on a job requires hazardous energy control and more than one employee working. The PE is responsible for establishing the LOTO and …installing the Lockout Devices and LOTO Tags. The PE is also responsible for removing the Lockout Devices and LOTO Tags, …and restoring the system as required after the completion of the work.

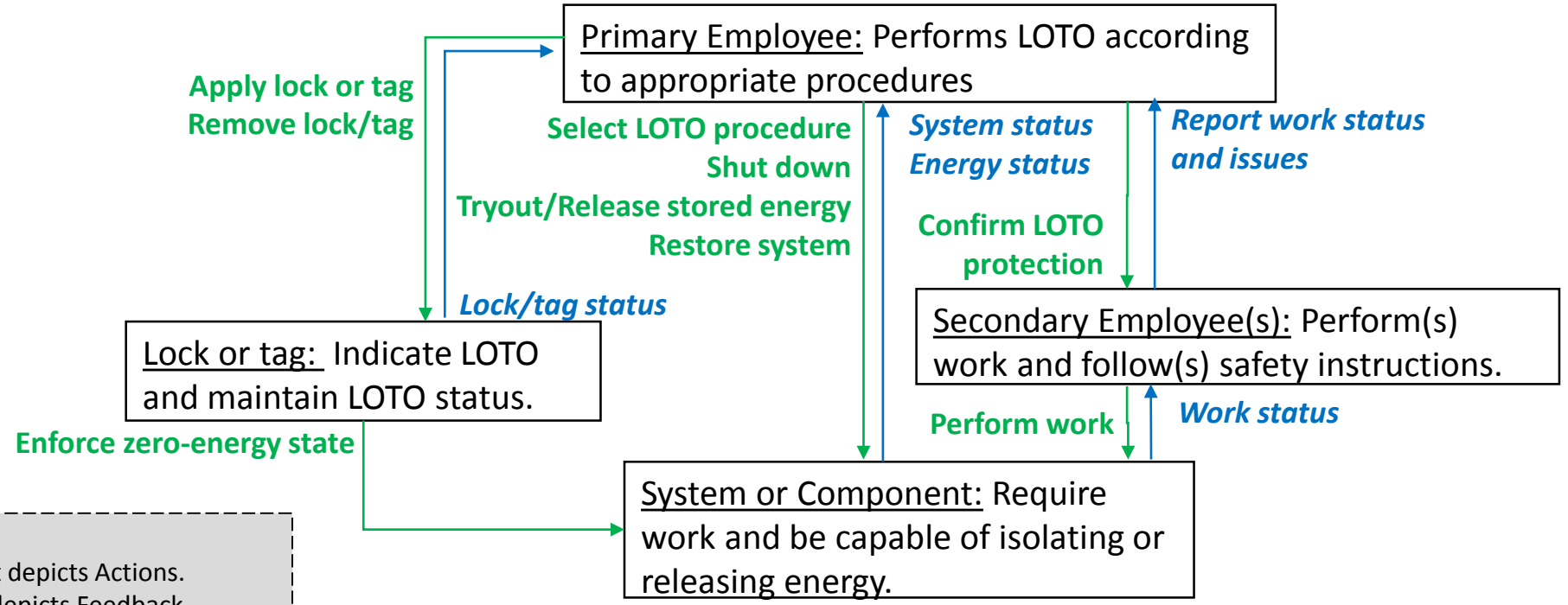
Secondary Employee. An employee(s) whose work requires lock out of aircraft/aircraft systems in order to perform work on the aircraft. A Secondary Employee (SE) can also be a Primary Employee when working in a group.

Assignment: Diagram and then discuss with a neighbor (handouts)

- How would the control model change to depict two Employees, a Primary Employee (who secures LOTO) and a Secondary Employee (who performs work under LOTO protection)?



Possible Answer: LOTO with Two Employees Having Separate Responsibilities



LEGEND
Green content depicts Actions.
Blue content depicts Feedback.

Next Step: Identify Unsafe Control Actions --Example of LOTO UCA's

Standard UCA Syntax:

*"**Controller** issues **Action/Type when or while Context or Conditions** are Present, **leading to a Hazard***

Sample Control Action	**Applying causes hazard**	**Not applying causes hazard**	**Wrong Timing or Order (Too soon/ too late)**	**Applied too long/ Ended too soon**
Perform work on system	**UCA-1**: Secondary Employee performs work on the system while the system is not locked out. [H1]		**UCA-2:** Secondary Employee performs work on the system too soon, before the system is locked out. [H1]	**UCA-3:** Secondary Employee continues to perform work on the system when lock-out protection is removed. [H1]
Remove Lock/tag	**UCA-4:** Primary Employee removes lock/tag while the system is still being worked. [H1]		**UCA-5**: Primary Employee removes lock/tag before the work is complete. [H1]	

Example Causal Scenarios

For each UCA, what are the plausible reasons or situations that could lead to that occurrence?

Secondary Employee performs work on the system while the system is not locked out (UCA-1)

- Scenario 1.1: because the Primary Employee (in charge of LOTO) had not yet performed LOTO and the Secondary Employees was not notified of this delay.
- Scenario 1.2 because the Secondary Employee does not believe the energy level is hazardous.
- Scenario 1.3: because the system had been locked out previously, but was no longer, and the Secondary Employee assumed it was still locked out.
- Scenario 1.4: because the Secondary Employee had previously performed this work when the system was not energized and had not experienced LOTO for this job before.
- And so on…

What are some other possible situations that could lead to this?

What if We Examine Other Losses?

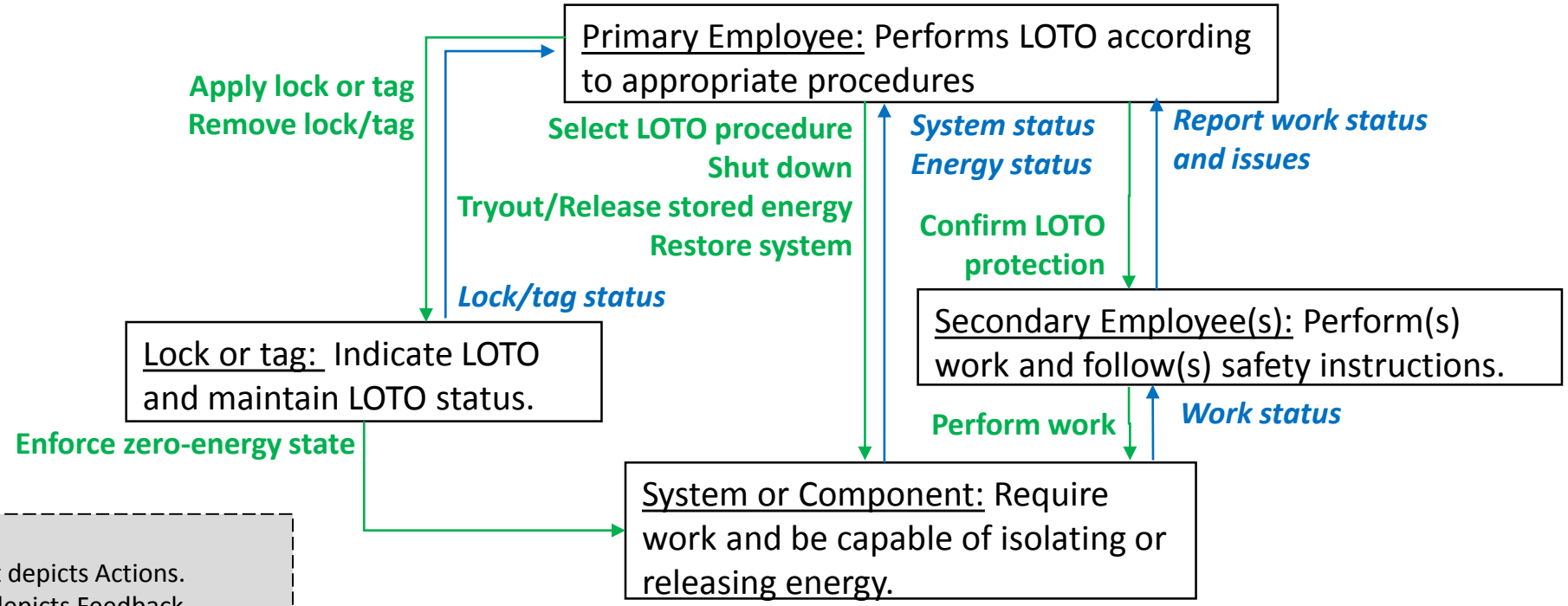
Accidents or Losses	Hazards
A-1: Workers are killed or injured on the job.	H-1: Workers are exposed to hazardous energy.
A-2: Systems or equipment are damaged.	H-2: Systems or equipment are exposed to excessive levels of hazardous energy.
A-3: Scheduled work is not completed on time.	H-3: Production, delivery and/or maintenance commitments are missed.

Control Action	**Applying causes hazard**	**Not applying causes hazard**	**Wrong Timing or Order (Too soon/ too late)**	**Applied too long/ Ended too soon**
Perform work on system	**UCA-1**: Secondary Employee performs work on the system while the system is not locked out [H1, H2].	**UCA-6:** Secondary Employee does not perform work on the system while the system is locked out [H3].	**UCA-2:** Secondary Employee performs work on the system too soon, before the system is locked out [H1, H2]. **UCA-7:** Secondary Employee delays performing work on the system after the system is locked out [H3].	**UCA-3:** Secondary Employee continues to perform work on the system when lock-out protection is removed [H1, H2]. **UCA-8:** Secondary Employee stops performing work on the system too soon when lock-out protection is still in place [H3].
Remove Lock/tag	**UCA-4:** Primary Employee removes lock/tag while the system is still being worked [H1, H2]	**UCA-9**: Primary Employee does not remove lock/tag when the work is complete [H3].	**UCA-5**: Primary Employee removes lock/tag before the work is complete [H1, H2]. **UCA-10**: Primary Employee delays removing the lock/tag after the work is complete [H-3].	N/A (discrete)

Next Exercise:

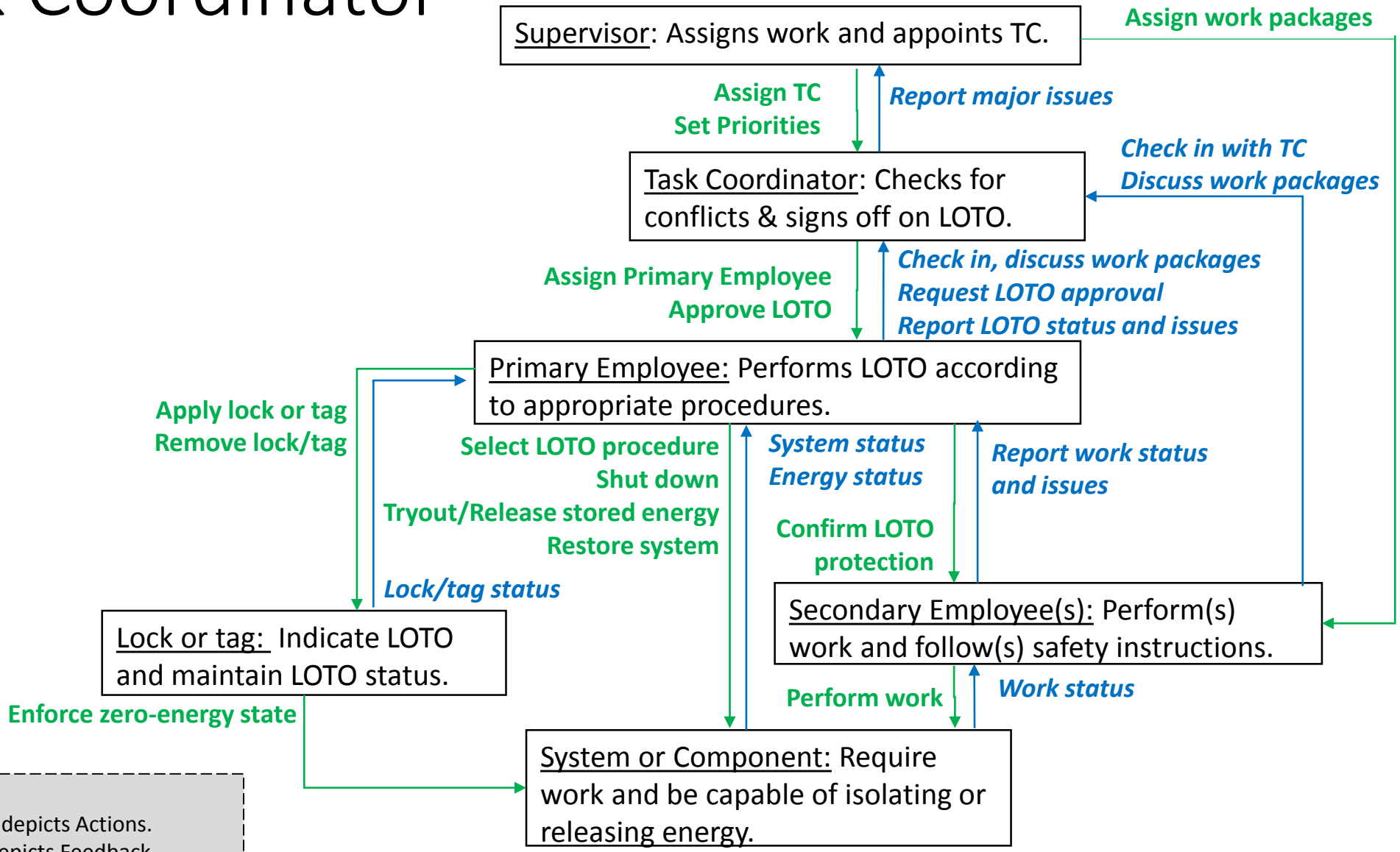
What happens when tasks that require LOTO have to be performed at the same time with tasks that don't?

- Hint: assume two more new controllers, a Supervisor, who assigns work, and a Task Coordinator who checks for conflicts and signs off on LOTO



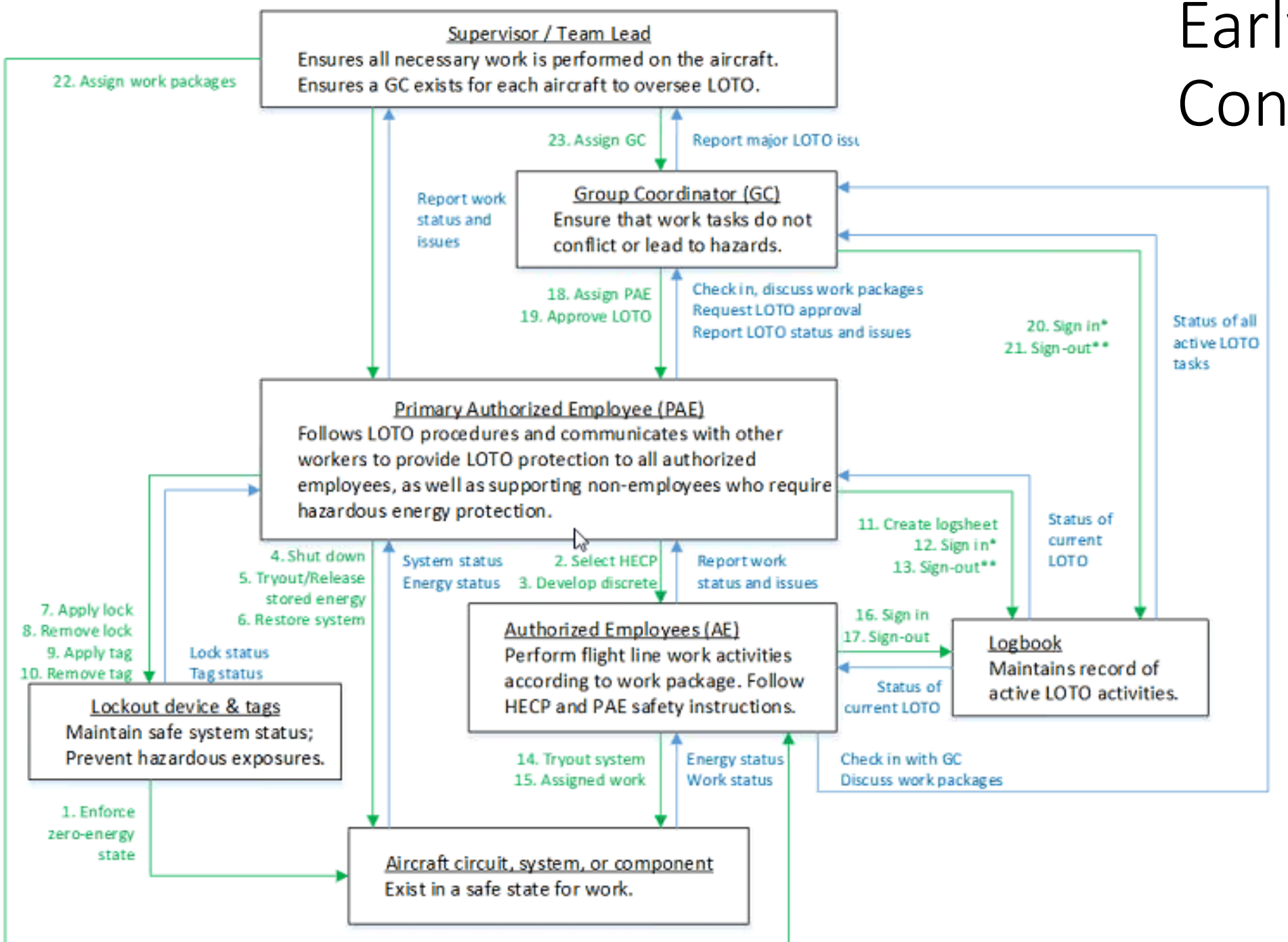
LEGEND
Green content depicts Actions.
Blue content depicts Feedback.

Possible Answer: Addition of Supervisor and Task Coordinator



LEGEND
Green content depicts Actions.
Blue content depicts Feedback.

Early LOTO Control Model

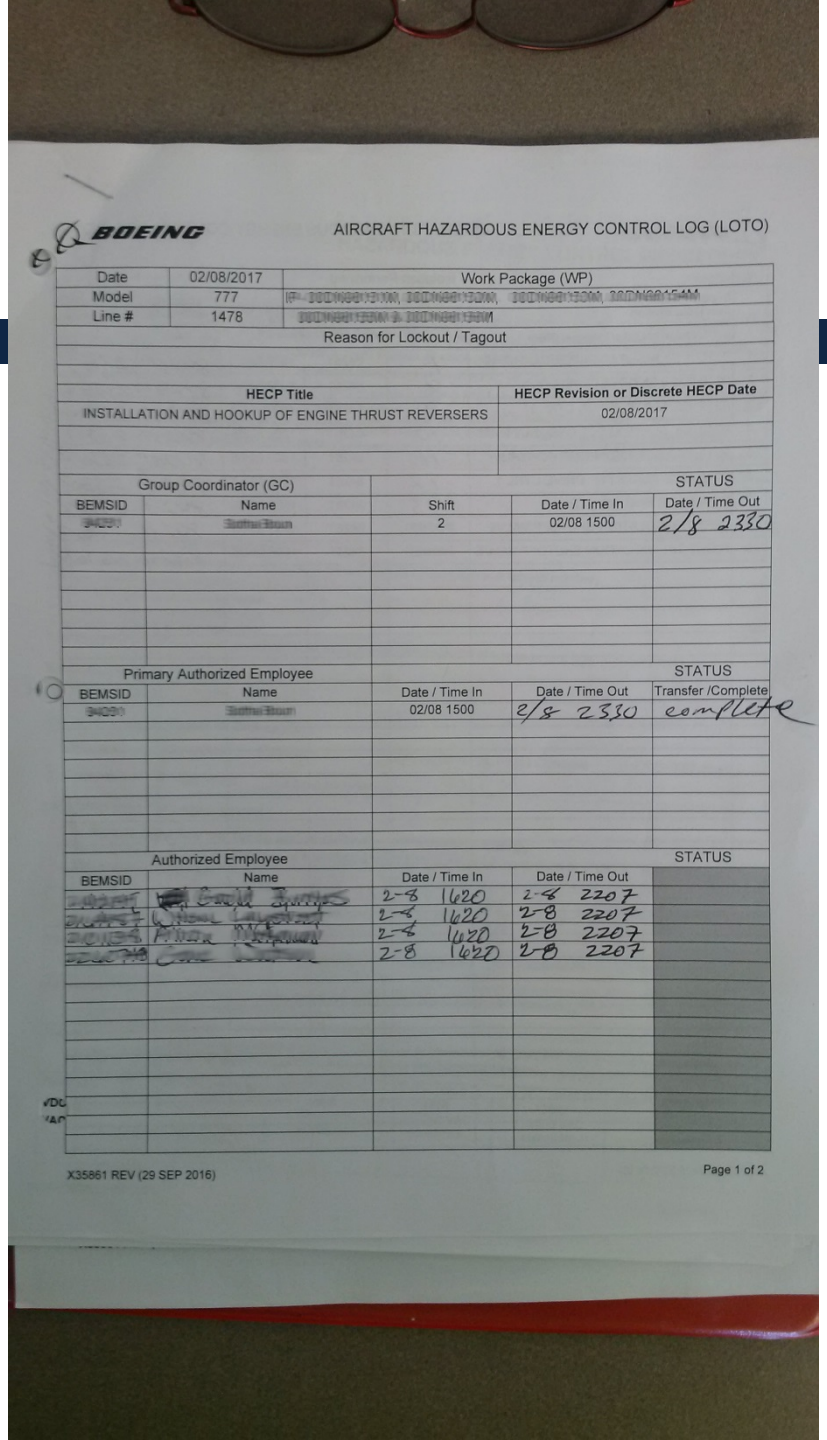


Many STPA Results Involved Hazards with the Logbook*

For Example…

- **Controller:** (Secondary) Authorized Employee (AE)
- **Control Action:** AE signs into LOTO Log Sheet
- **Unsafe Control Action**: AE does not sign into the Log Sheet when LOTO is active because…
- **Causal Scenarios**:
  - … AE can't find the sheet
  - … AE forgot
  - … AE thought someone else filled it out

*See paper on The Human Element in STPA later in this conference (Juhnke).



BOEING

AIRCRAFT HAZARDOUS ENERGY CONTROL LOG (LOTO)

Date	02/08/2017	Work Package (WP)
Model	777	[redacted]
Line #	1478	[redacted]

Reason for Lockout / Tagout

HECP Title	HECP Revision or Discrete HECP Date
INSTALLATION AND HOOKUP OF ENGINE THRUST REVERSERS	02/08/2017

Group Coordinator (GC)

BEMSID	Name	Shift	Date / Time In	STATUS Date / Time Out
[redacted]	[redacted]	2	02/08 1500	2/8 2330

Primary Authorized Employee

BEMSID	Name	Date / Time In	Date / Time Out	STATUS Transfer /Complete
[redacted]	[redacted]	02/08 1500	2/8 2330	complete

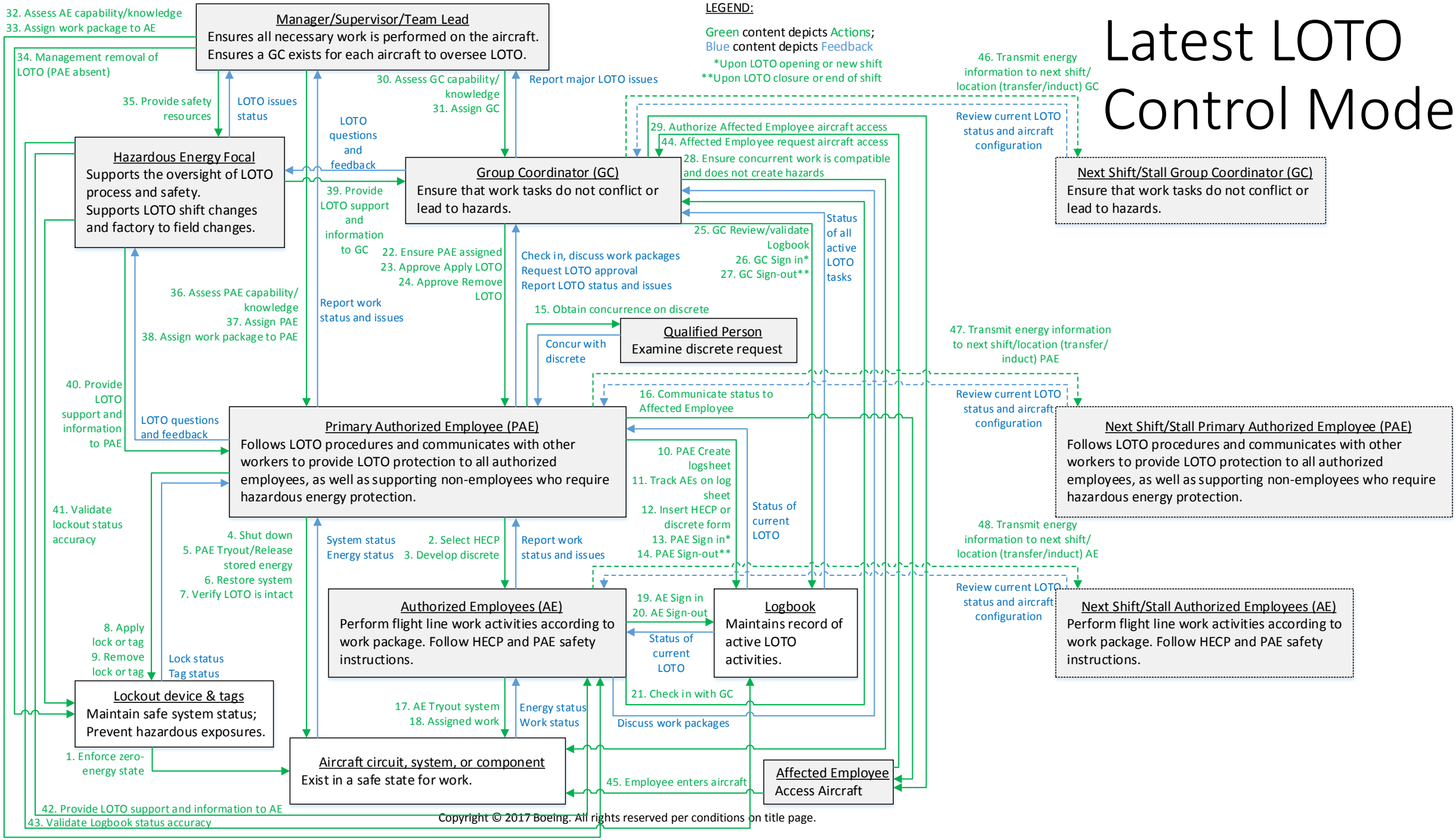
Authorized Employee

BEMSID	Name	Date / Time In	Date / Time Out	STATUS
[redacted]	[redacted]	2-8 1620	2-8 2207	
[redacted]	[redacted]	2-8 1620	2-8 2207	
[redacted]	[redacted]	2-8 1620	2-8 2207	
[redacted]	[redacted]	2-8 1620	2-8 2207	

X35861 REV (29 SEP 2016)

Page 1 of 2

Latest LOTO Control Mode



STPA Challenges*

- 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?

*See paper on Using STPA Trend Analysis later in this conference (Belvin)

Unique Aspects of STPA for Workplace Safety

- Workplace STPA is similar to traditional product safety STPA, save that nearly every controller and process is likely to be human.
- A more challenging distinction is that these human controllers in the system often represent more than one individual or possibly a team.
  - Can be hard to know what level of modeling detail needs to be captured
  - Causal scenarios may be specific to an individual or subset of individuals
- But even with single individuals representing unique components in the system, people also exhibit significant variability over time.
  - Performance will be inconsistent and subject to many factors
    - Learning
    - Fatigue
    - Attentional distraction
    - Memory lapses
    - Decision biases and errors
    - Mood and arousal
  - Can be hard to capture the range of possible expected behaviors completely
- As with most analysis techniques, the value is doing just enough assessment to support system changes that will mitigate the identified hazards.
  - Be mindful of the realistic opportunities for change in the system and focus on those.

In Summary

- STAMP & STPA are very well suited to the analysis of safety hazards in the workplace.
- STPA process is highly modular and scalable to address targeted areas of interest
  - But recommend modeling the whole system at a high level first, to capture all of the relevant influences
- STAMP provides a very comprehensive understanding of the problems, system-wide, and helps bring diverse stakeholders together in finding solutions.
  - Can support a better business case for system-level changes
- Unlike many classical safety methods, (RCCA, review boards, etc) STPA is highly proactive, and does not require actual incidents/injuries to be effective.
- Can result in more exhaustive list of hazards to be mitigated than business leaders would like to hear
  - May need to offer a prioritization and recommended resource management approach toward mitigation
- Effective application requires key participation from human performance experts and a solid user research approach with a pool of end users
  - These represent the most knowledgeable “system experts” to drive STPA results.


BOEING

Handout