# Overview of
# Systems Theoretical Analysis, Modeling and Processes (STAMP) and Systems Theoretical Process Analysis (STPA) for Product and Production Systems Engineering

**Marc Nance**
**Director, The Boeing Company**

Safety
Integrity
Commitment

# STAMP Across Boeing

**Across Boeing, we have compiled a significant range of success stories for applying STAMP to a wide variety of systems engineering challenges**

- STAMP has uncovered numerous product, production system and automation design anomalies that were previously unknown and enabled conditions to be developed in the systems which could have lead to safety, quality and efficiency losses.
- STAMP is gaining broader usage among numerous commercial and military customers,

**Key Benefits**

- Able to address multiple, emerging properties of any system
  - **Includes cyber-security, quality, cost and schedule "losses" as well as safety**
- Can be applied to any system to complement existing modeling and analysis tools
  - Simplifies analysis for highly complex, software intensive systems
  - Analyzes systems hardware, software, human and environment interfaces and interactions
  - Method is applicable to all phases of product life cycle
  - Early lifecycle application of STAMP yields higher benefit to the program
- Proven to be more efficient and effective than traditional methods
- Scalable and modular approach tailored to fit program needs

**A World Class Standard for System Characteristic Analysis**

# What Makes STAMP Unique?

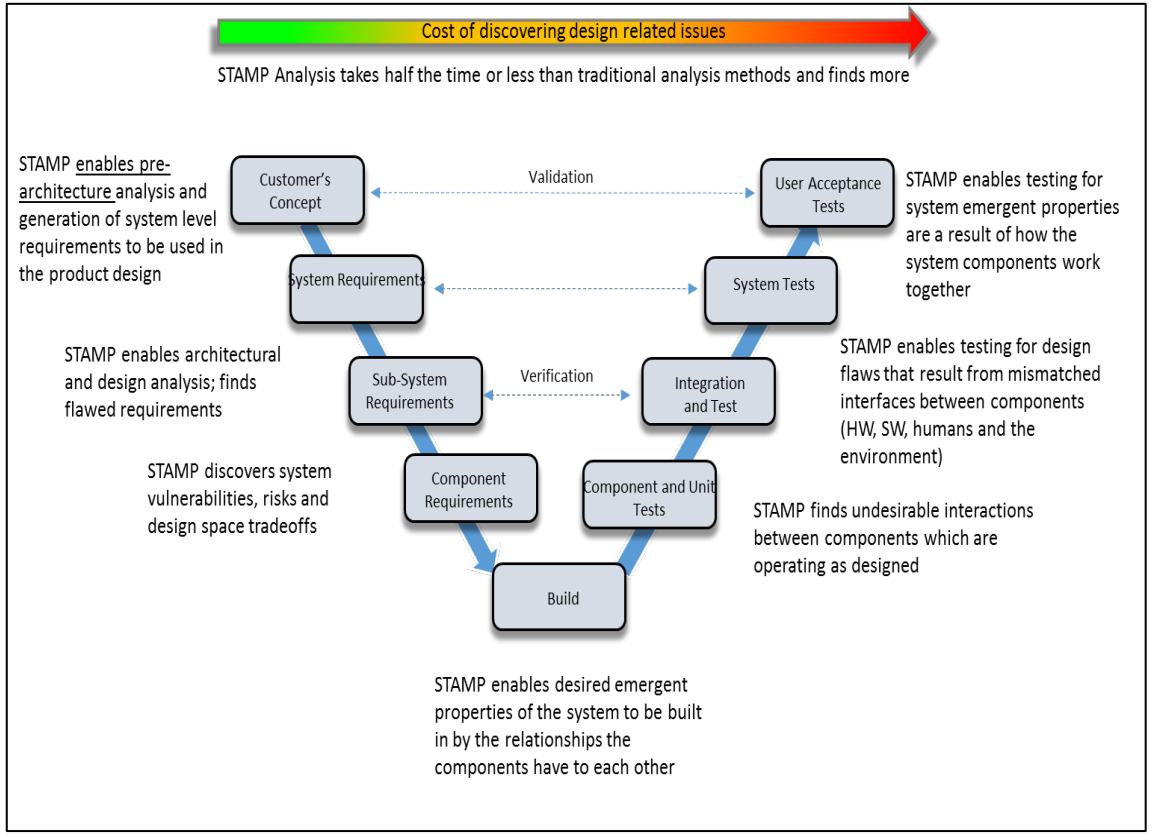
- **Overview**
  - Assumes quality, schedule, cyber-security and safety losses are a control problem, not a reliability problem
  - STAMP gives us the ability to simplify and analyze highly complex systems where thousands of interactions between HW, SW, humans and the environment occur on a continuous basis
  - Quality, schedule, security and safety are emergent properties of the system resulting from the relationships & interactions between the components
  - System failures do occur without component failures – analyzes interactions to determine why it happens, not just how it happens
  - STAMP is based on systems thinking – problems occur in the context of the larger system
  - STAMP does not require extensive probabilistic calculations which are often speculative due to the lack of reliability data for humans and software

**A Standard Methodology Being Utilized Throughout Industry**

# Systems Engineering Using STAMP

INTRODUCTION

- Finds faulty underlying assumptions from concept development that flow downstream as anomalies where it becomes increasingly costly to change
- Finds incomplete information – basis for further discussion with the customer
- Provides quality, efficiency, security and safety requirements to use in analyzing existing systems or for early architecture and preliminary design
- Keeps design flaws from flowing downstream where they are more costly to change
- Gives deeper insight into system vulnerabilities particularly for cyber-security




**Highest Leverage Early in Life Cycle**

# Success Stories
## 1. Early Program Analysis

- Identified potential design flaws during concept development:
  - 54 Pilot/Flight Management
  - 84 Avionics System
  - 23 Flight Control Computing system (FCCS) unsafe actions
  - 34 Flight Control Actuation
- Rapidly gaining support in the Department of Defense
- Opens up new opportunities for industry

# Success Stories

## 2. Factory Robotic Analysis

- Identified two potentially unsafe system conditions for the Robot and AGV to be in:
  - Violation of minimum separation distance from humans, airplane parts and buildings
  - Automated Ground Vehicle (AGV) violation of minimum separation distances with humans
- Identified 17 potentially unsafe system conditions resulting from unknown system design flaws
  - Only 2 of 17 were identified in previous analyses
- 38 causal scenarios
  - Answers “why” accidents are occurring
  - 38 potential controls and system design changes were considered with the design team for future implementation

**A Systems Approach for Robotic System Safety**
**When we Focus on Safety and Quality, Cost and Schedule Will Follow**

# Success Stories

## 3. Development Hot Fire Test (HFT)

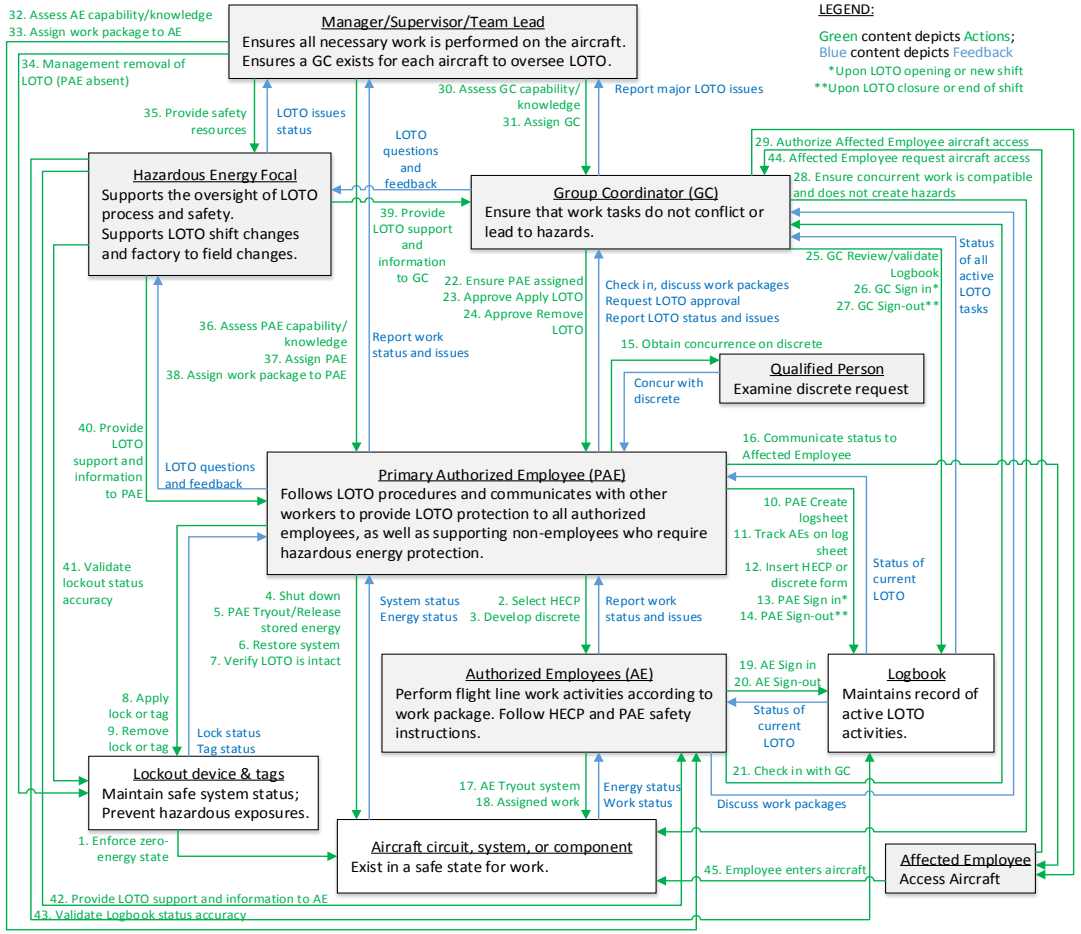
- Five types of hazards and test constraints were identified, including safety and mission assurance (test success) objectives
- From the control model, 86 potentially unsafe control actions, and 218 causal scenarios were examined
- 28 different mitigations to address the causal scenarios were identified and helped to finalize the test configuration
- The test team thought this was a valuable tool to provide a bottoms up safety assessment of the test execution process for the HFT and provided some good insights and corrective actions for the system design

**A Systems Approach for Complex System Testing- Taking Safety Seriously**

# Success Stories

## 4. Hazardous Energy Management Lock Out Tag Out Try Out (LOTO)

- Identified > 200 potentially unsafe control actions and nearly 1000 associated potentially unsafe conditions
- Found significant challenges with capturing and disseminating LOTO-related information correctly and completely
- Analyses are highly correlated with incident data
- Compelling results unified EHS and other production and delivery teams toward a single roadmap for an enterprise IT-based solution




**A Systems Safety Approach for a Complex Workplace System – Doing More to Keep People Safe**

# Success Stories

## 5. Production System STPA

- Potential production system losses identified as safety, quality, efficiency or security losses
- Identified 112 potentially undesirable system conditions that could lead to production system losses
- Found multiple missing control actions and feedback loops in current system
- Wrote ~ 156 requirements for the design of the new production system
- Customer responded positively to Boeing's analysis which proactively prevents production losses from occurring

**A Systems Safety Approach for a Complex Production System Focusing Workplace Efforts on Zero Incidents and Accidents**

# Conclusion

- Safety & quality are linked – STAMP/STPA supports both
- Greatest benefits with complex systems with hardware, software and human interaction
- Provides different perspective than industry standard tools, e.g. failure modes & effects analysis
- Relatively simple & straightforward to use