34th Annual INCOSE international symposium

hybrid event

Dublin, Ireland
July 2 - 6, 2024

Product Assurance in the Model-Based System Engineering Ecosystem: Learning from Various Vertical Lift Platforms (#347)

Timothy Russell

Presentation Outline

- Introduction
  - Series Objective
  - Presentation Objective
- Observations
  - Systems Engineering Fundamentals
  - Centralization
  - External Tool Linkages
- Future Considerations
- Conclusion

Introduction

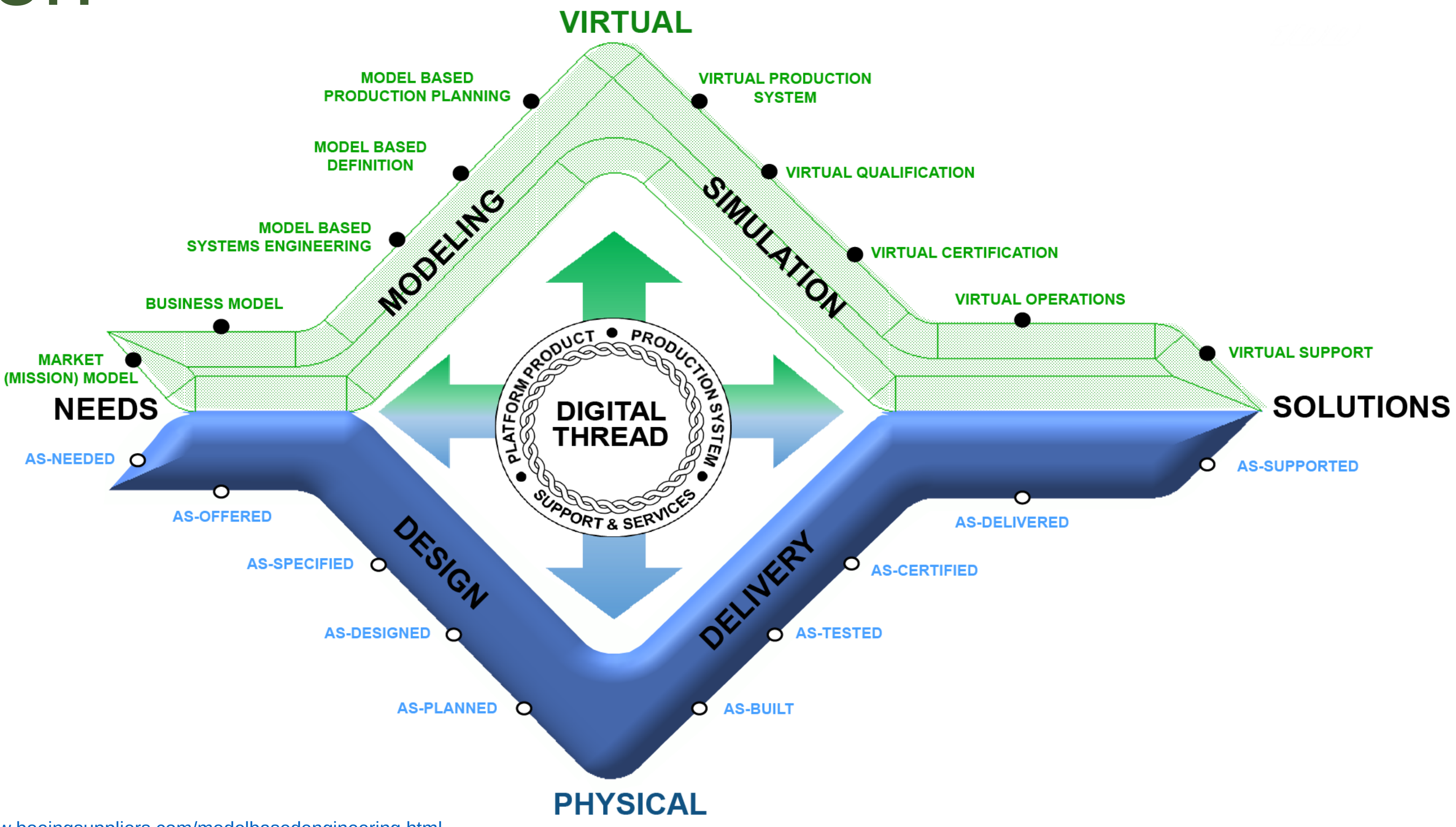
Overview

- Boeing is reimagining how we design, build, test, and support its products/services across the full lifecycle

- Central to this reimagination is a comprehensive and unified digital ecosystem, of which MBSE is a crucial foundational element

Vision

Evolution of System Engineering (SE) to Model Based Engineering (MBE)



Source: https://www.boeingsuppliers.com/modelbasedengineering.html

Series Objective

- Discuss what can be learned from applying MBSE for Product Assurance (PA) or RAMPSSS
  - Reliability/Availability/Maintainability (RAM)
  - Product Support (PS)
  - System Safety (SS)

- Contexts
  - Products and Services
  - Hardware and Software
  - Military and Civilian
  - Full Lifecycle (Concept Development to Disposal)

Presentation Objective

- Kick off the series on MBSE for PA with a focus on:
  - System Safety
  - Civil/Military Rotorcraft Platforms (CRP/MRP)
  - Early Lifecycle
    - Starting with Conceptual Development
    - Ending with Detailed Design

- Observations
  - Systems Engineering Fundamentals
  - Centralization
  - External Tool Linkages

Systems Engineering Fundamentals

Observations

SE Fundamentals

- SE fundamentals are still vital for MBSE
- MBSE tools do not absolve a program from the responsibility of executing solid SE fundamentals
- CRP is presented as an example

CRP Initial Plan

Planned Program Baseline | **Internal Baseline/Milestone** | **External Baseline/Milestone**

- Operational Model Baseline (OMB) (Requirements)
- Functional Baseline (FBL) (Functions)
- Allocated Baseline (ABL) (Physical & Logical)

- Critical Design Review (CDR)

CRP Early Challenges

- New, large, and complex system

- Program was in jeopardy due to SE fundamentals
  - Minimal planned baselines/milestones
  - No tree/tier structure
  - Limited synchronization between
    - Requirements
    - Functions
    - Elements (Physical and Logical)

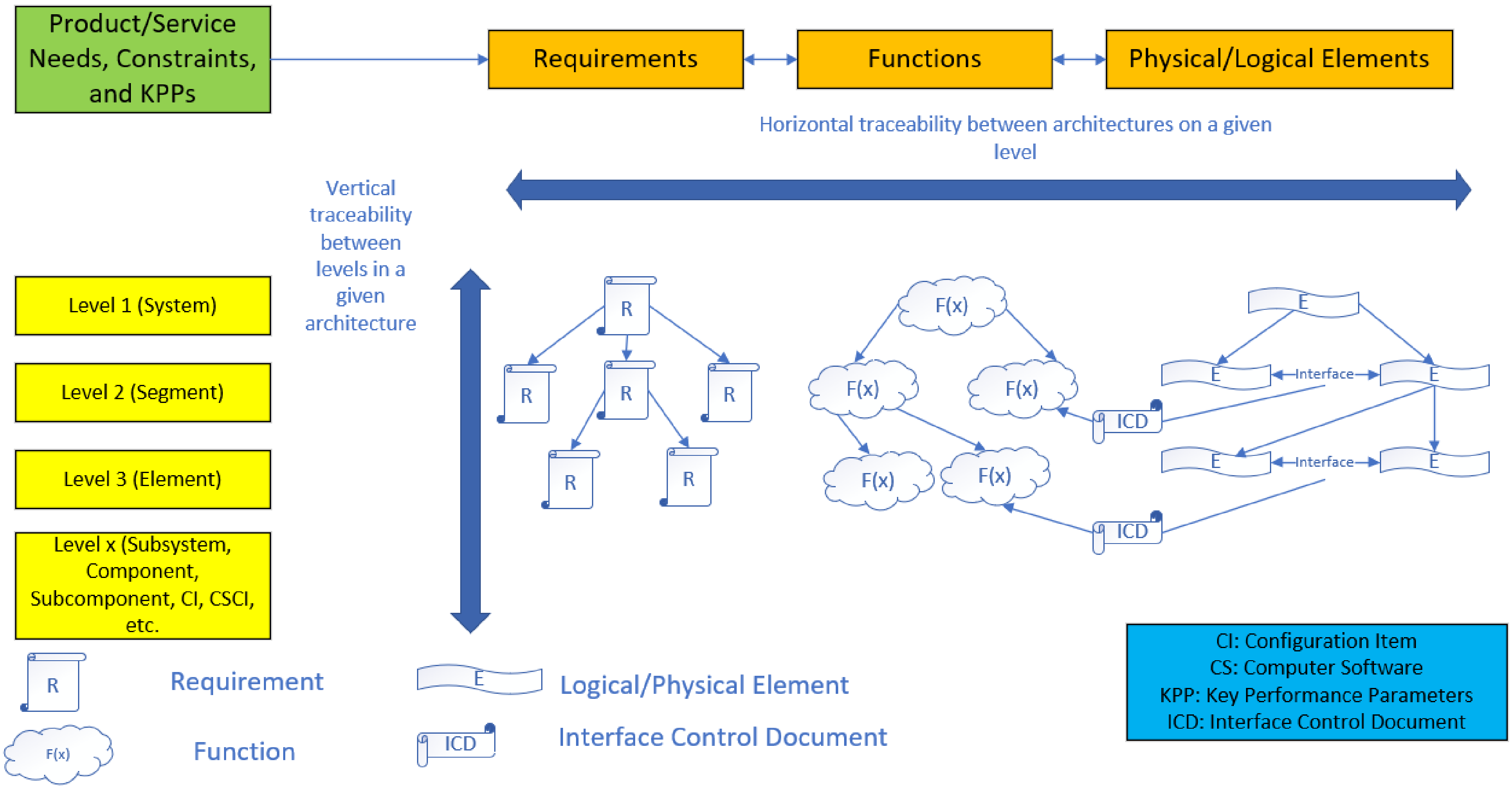
CRP Early Challenges (cont.)

- Requirements
  - Converting excerpts from standards directly into requirements
  - Single tier
- Functions
  - Mixing functions and subfunctions
  - Mixing hardware, software, and hybrid functions
- Physical/Logical Elements
  - Attempted to define architectures without predecessors
  - Attempting make/buy decisions

SE Trees & Traceability

Linkages

- Vertical
- Horizontal
- Requirements & Architecture
- Functional, Logical, & Physical Architecture
- Hardware & Software
- Customers, Integrators & Suppliers



Program Overview & Baselines

Planned Program Baseline	Internal Baseline/Milestone	External Baseline/Milestone
Operational Model Baseline (OMB) (Requirements) →	Initial Design Requirements Review (IDRR) →	System Requirements Review (SRR)
Functional Baseline (FBL) (Functions) →	Initial Design Functional Review (IDFR) →	System Functional Review (SFR)
Allocated Baseline (ABL) (Physical & Logical) →	Initial Design Concept Review (IDCR) →	Preliminary Design Review (PDR)
Product Baseline (PBL) (Physical & Logical) →	→	Critical Design Review (CDR)

CRP Success

- Program restructured and slowed down
- Program is now proceeding on the right path
  - Baselines and milestones added
  - Tiered trees implemented and synchronized between:
    - Requirements
    - Functions
    - Physical Elements
    - Logical Elements

Centralization

Observations

Centralization

- MBSE tools enable extremely powerful linkages to be established in a single central repository

- SS on MRP is presented as an example

Processes, Standards, & Tools

- Applicable Standards
  - Common: SAE ARP 4754A & 4761, S1000D Standard Numbering System (SNS)
  - MRP only: MIL-STD-882E, NAS 411 & 411-1 (Hazardous Materials)
  - CRP only: FAA and EASA

- Tools
  - DESE-CAMEO (MBSE)
  - DOORS (Requirements)
  - 3DX or Teamcenter (Design Engineering/Integration)
  - ADO or JIRA (Systems and Software Engineering Management)
  - Fault Tree Analysis
    - Windchill Risk & Reliability (WRR)
    - Reliability Workbench (RWB)
    - CAFTA

MRP Overview & Baselines

Planned Program Baseline	Internal Baseline/Milestone	External Baseline/Milestone
Operational Model Baseline (OMB) (Requirements)	Initial Design Requirements Review (IDRR)	System Requirements Review (SRR)
Functional Baseline (FBL) (Functions)	Initial Design Functional Review (IDFR)	System Functional Review (SFR)
Allocated Baseline (ABL) (Physical & Logical)	Initial Design Concept Review (IDCR)	Preliminary Design Review (PDR)
Product Baseline (PBL) (Physical & Logical)		Critical Design Review (CDR)

Safety Artifacts

- Functional Baseline System Model (FBSM) in CAMEO for FBL/IDFR/SFR
  - Aircraft Functional Hazard Assessment (AFHA)
  - System-Theoretic Process Analysis (STPA)
  - System Requirements Hazard Analysis (SRHA)

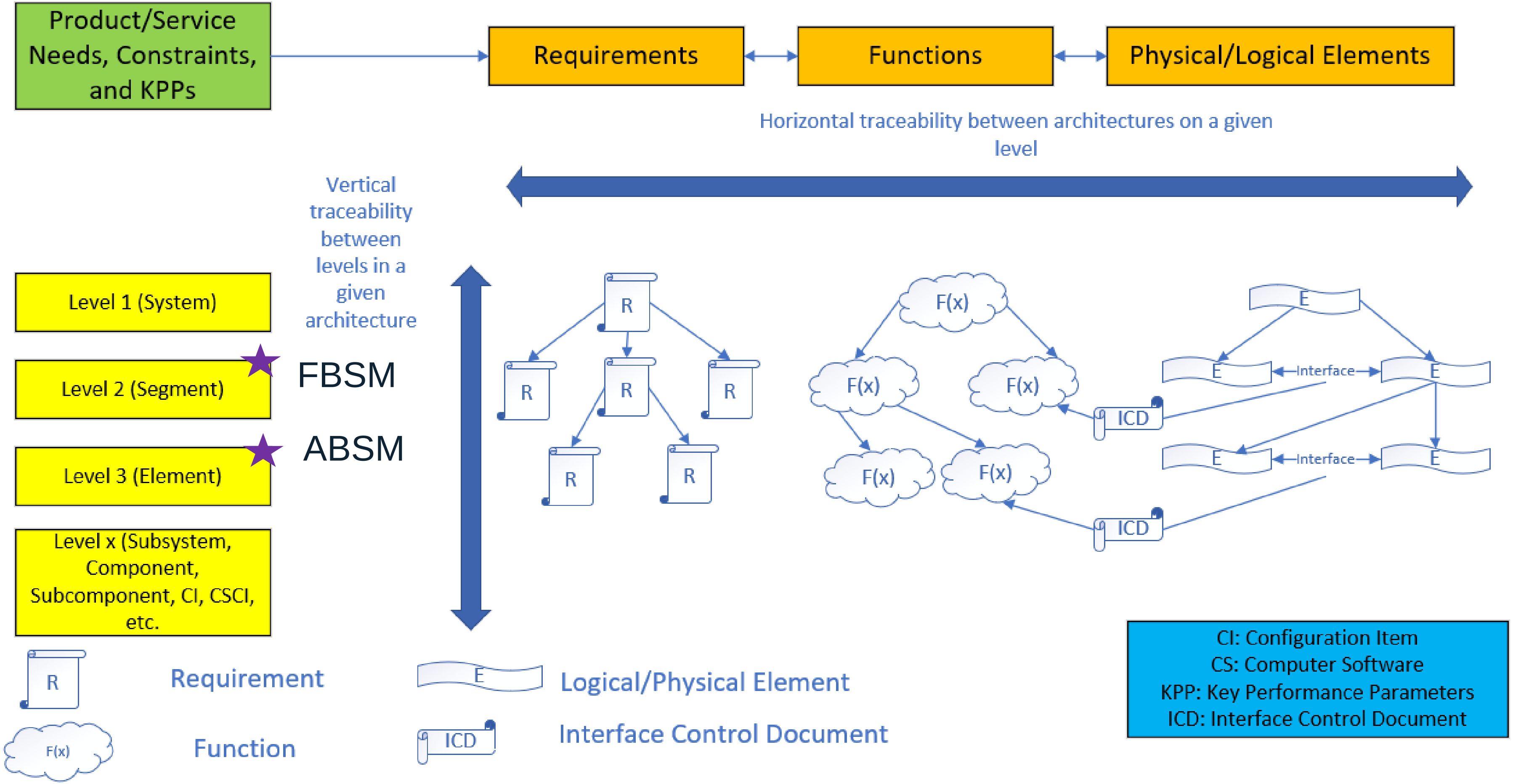
- Allocated Baseline System Model (ABSM) in CAMEO for ABL/IDCR/PDR
  - System Functional Hazard Assessment (SFHA)
  - Preliminary System Safety Assessment (PSSA)
  - System/Subsystem Hazard Analysis (SHA/SSHA)
  - Preliminary Software Safety Critical Functional Analysis (PSSCFA)

- Reports
  - System Safety Program Plan (SSPP)
  - Hazardous Material Management Program Plan/Report (HMMP/HMMPR)
  - Critical Safety Item (CSI) Plan & Preliminary Candidate List
  - Operating & Support Hazard Analysis (O&SHA)
  - Aircraft & System Fault Tree Analysis (AFTA/SFTA)

SE Trees & Traceability

Linkages

- Vertical
- Horizontal
- Requirements & Architecture
- Functional, Logical, & Physical Architecture
- Hardware & Software
- Customers, Integrators & Suppliers



MBSE/SS Linkages (Hazards)

- Requirements, functions, architectures, & hazards are all in CAMEO

- AFHAs & SFHAs in CAMEO allow direct linkages to requirements, functions, & other safety artifacts
  - Requirements
    - Hazard linkage to requirements goes beyond safety-tagging
    - Provides context about why a specific requirement is safety-tagged & what hazard(s) it is tagged to
    - Shows all of the requirements tagged to a specific hazard
  - Functions
    - Hazard linkage to functions facilitates assignment of initial Functional Development Assurance Levels (FDALs)
    - FDALs captured in PSSCFA based on severities of hazards linked to functions
  - FHAs linked directly to SHAs/SSHAs for assignment of Risk Assessment Codes (RACs) to each individual hazard

- **Powerful linkages in CAMEO make it vital to establish requirements specification trees & a master function library as quickly as possible to feed into FHAs, establish initial FDALs in the PSSCFA, determine preliminary RACs in the SHAs/SSHAs, & minimize rework**

MBSE/SS Linkages (STPA)

- STPA pathfinder was completed
  - Identified in the customer's statement of work
  - Performed in CAMEO with support from Design, Enterprise Safety, Cybersecurity, & select suppliers
  - Delivered in the FBSM

- Findings
  - 44 tier 3 requirements
  - 153 lower-level candidate requirements identified
  - Effort undertaken while the program in general was focusing on tier 1 & tier 2 requirements
  - Requirements could be linked to STPA's Undesirable Control Actions (UCAs) similar to hazards from FHAs

- **STPA effectively supplemented traditional safety approaches by facilitating discovery of lower-level safety requirements earlier than they otherwise may have been identified**

External Tool Linkages

Observations

External Tool Linkages

- Not everything can be easily captured, analyzed, and delivered via a MBSE model at this time
- Other tools are needed once SS looks beyond itself to additional disciplines
- SS on MRP is presented as an example

Fault Trees (System Safety)

- Aircraft & system-level fault trees were done in Windchill Risk & Reliability (WRR)
  - AFTAs for aircraft-level functions/hazards (examples: Aviate, Navigate)
  - SFTAs for system-level functions/hazards (example: to provide engine motive force)
  - FTAs for lower-level functions/hazards were not developed unless needed to inform design trade studies

- WRR enabled robust fault tree integration by collecting FTAs into a single model
  - Consolidation into a single model vs a single file for each individual FTA
  - Vertical integration (SFTAs feeding into AFTAs, like loss of single engine feeding into loss of lift)
  - Horizontal integration (SFTAs feeding into each other, like hydraulics feeding into dependent mechanical systems)
  - Updates could propagate through all fault trees simultaneously
  - Proof-of-concept for importing supplier FTAs from other tools into WRR was successfully demonstrated, but not expanded upon (example: engine FTAs from supplier)

- **WRR successfully collected & linked FTAs within a single model to enable vertical & horizontal integration, along with faster update propagation**

Fault Trees (MBSE)

- WRR also enabled robust integration between System Safety, Reliability, & Product Support
  - System Safety, Reliability, & Product Support harmonized artifacts early via common numbering (S1000D SNS)
  - SFTAs functions/hazards were managed with S1000D, linking physical & functional architectures
  - Reliability also planned to use WRR to house & update their Failure Modes Effects & Criticality Analyses (FMECAs)
    - FMECAs failure modes could eventually have been used directly in FTAs (typically SFTAs, but possibly AFTAs)
    - FMECAs feed into Maintainability, Testability, & Publications artifacts, all of which were managed via S1000D
    - FMECAs also feed into Critical Safety Item (CSI) Candidate List

- WRR limited in its abilities to directly integrate with CAMEO
  - Automated feed from WRR into CAMEO was not feasible; FTA results had to be manually entered into SHA/SSHA
  - Proof-of-concept for importing FTAs directly into CAMEO was successfully demonstrated, but was not pursued

- **WRR & S1000D successfully laid the foundation for robust integration between System Safety, Reliability, & Product Support, but WRR was limited in its abilities to integrate with CAMEO**

Fault Trees (Civil-Military Integration)

Non-Military Unique

- Catastrophic:
  - <1E-09 per FH (extremely improbable)
  - No single-point failures
- Hazardous: <1E-07 per FH (extremely remote)
- Major: <1E-05 per FH (remote)
- Minor: no requirement
- Consistent with civil standards & ARP 4761

Risk Matrix

Severity / Probability Per FH	Catastrophic 1	Critical 2	Marginal 3	Negligible 4
Frequent >1E-03 A				
Probable >1E-04 but <1E-03 B				
Occasional >1E-05 but <1E-04 C				
Remote >1E-06 but <1E-05 D				
Improbable >1E-07 but <1E-06 E				
Very Improbable <=1E-07 but >Baseline F				

Risk Level Key			
HIGH RISK	SERIOUS RISK	MEDIUM RISK	LOW RISK

Military Unique

- Catastrophic:
  - <1E-07 per FH (very improbable)
  - No single-point failures
- Critical: <1E-06 per FH (improbable)
- Marginal: <1E-05 per FH (remote)
- Negligible: no requirement
- Consistent with military standards derived from MIL-STD-882E's risk matrix, risk levels, severity criteria, & qualitative probability criteria

Future Considerations

Future Considerations

- CAMEO experienced major performance issues using the 2019 version due to the volume of data; upgrade to the 2021 version resolved them sufficiently to complete Preliminary Design phase

- Integration of System Safety content into MBE
  - O&SHA hazards into CAMEO (similar to FHA hazards), with linkages to Design & Publications ecosystems, requirements, & artifacts
  - HMMPR content into 3DX and/or Publications ecosystem, requirements, & artifacts
  - CSIs into CAMEO, DOORS, 3DX, and/or Publications ecosystems, requirements, & artifacts
  - Potential viability for CAMEO as part of a hazard tracking database system, safety escalation processes, and/or Safety Management System (SMS), possibly in conjunction with other tools

Future Considerations (cont.)

- Fault trees
  - Windchill Risk & Reliability also experienced major performance issues due to volume of data; Preliminary Design phase was still completed, but tool improvements were insufficient to overcome these issues & issues likely would have worsened as volume of data grew
  - Integration of FMECA failure modes into SFTAs was not feasible during Preliminary Design, but may be feasible during Detailed Design or later
  - If failure modes & hazards can be linked to in-service data once a platform is fielded, then it may be possible to create a loss model with quantified safety metrics that could be monitored as key safety performance indicators

- STPA potential future applications
  - Engine Controls
  - Modular Open Systems Approach (MOSA) or similar concept
  - Embedded Training
  - Manned-Unmanned Teaming
  - Cybersecurity

Future Considerations (cont.)

- Modularity & customization in MBSE capability suites is essential
  - Selecting applicable MIL-STD-882 tasks for military programs
  - Selecting applicable enterprise, civilian, & military frameworks for MBSE, safety, & certification
    - Hybrid software safety processes (example: MIL-STD-882 & SAE ARP 4754/4761)
    - Hybrid/multiple risk matrices
      - Military platform aspiring to civil thresholds for its non-military unique hardware
      - Platform with individual matrices for individual customers
      - Differences between enterprise safety escalation & platform matrices
      - Derivative Aircraft
        - » Base aircraft certified by FAA
        - » Modifications certified by FAA and/or military (depending on program)
      - Multiple simultaneous civil frameworks (i.e. pursuit of parallel FAA & EASA certification)
- Consider possibilities for integration with proprietary tools

Future Considerations (cont.)

- Embedding system engineers within the Integrated Product Teams (IPTs) (including System Safety) was a very valuable practice & proved to be a highly effective structure
  - Made tools/processes easier for IPTs
  - Ensured MBSE structure, standardization, & discipline throughout the program
  - Gave IPTs a voice in System Engineering forums

- System Safety teambuilding
  - All experience levels needed & welcomed
  - All traditional system safety skillsets are still needed
  - MBSE skillset is also necessary for the team to succeed
    - Multiple system safety engineers also had MBSE expertise in addition to our embedded system engineer
    - Had organic expertise been absent, there may have been need for multiple embedded system engineers
  - Hybrid skillsets were very helpful (system safety practitioners with prior experience in piloting, handling qualities, design, reliability/availability/maintainability, project management, system engineering, product support, etc.)

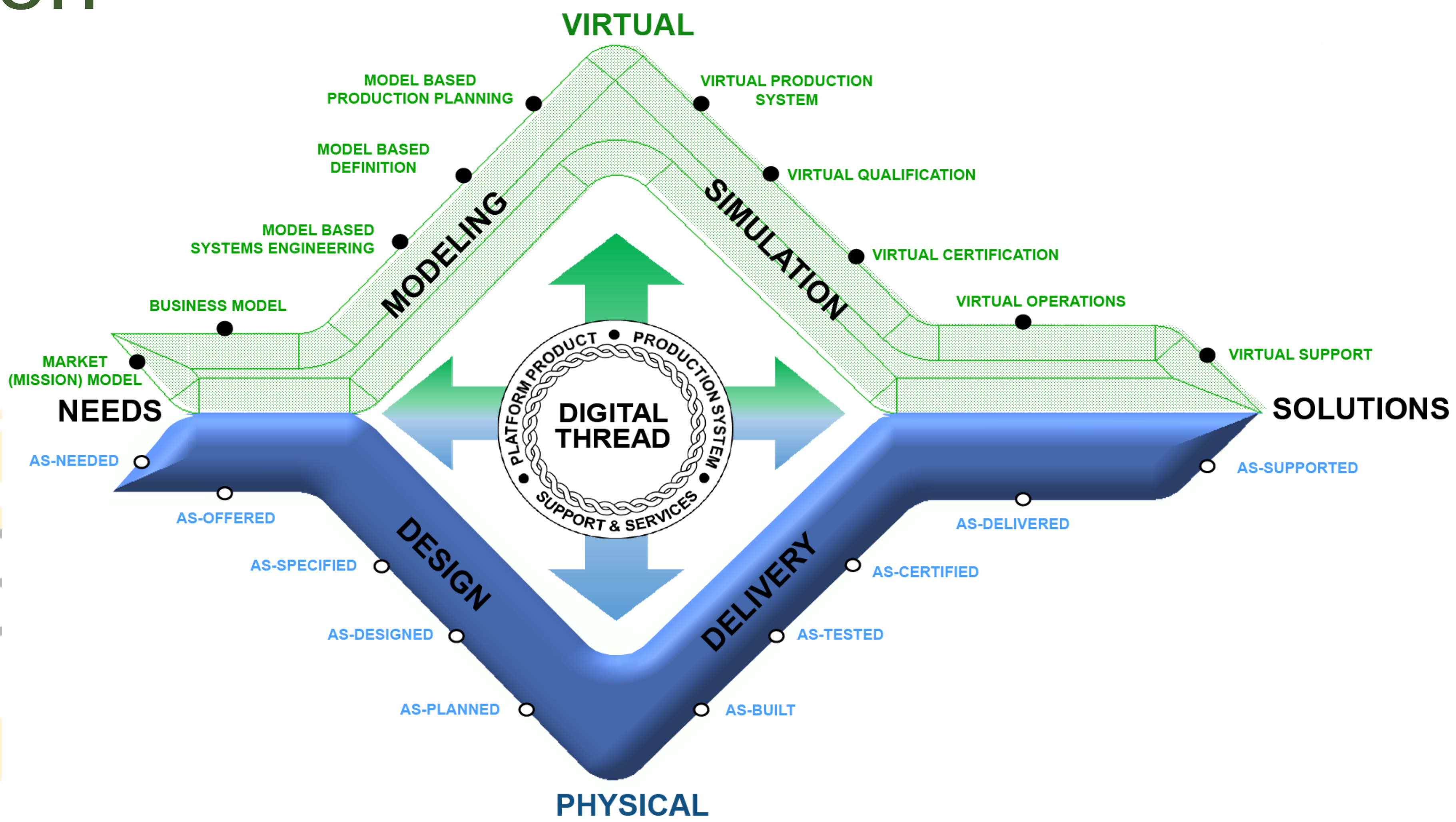
Future Considerations (cont.)

- At Boeing, we are iteratively crystalizing our MBSE/PA experiences for inclusion into our digital ecosystem via Solution Kits

- Solution Kits:
  - Updating and linking existing knowledge
    - Processes (what to do)
    - Training (how to do it)
    - Design Practices (reasons why, experience, ‘tribal knowledge’)
  - Creating adaptive MBSE starter kits to use
    - General enough to be applicable to many situations
    - Specific enough to be actionable and ensure enterprise-wide standardization or commonality to the extent practicable
  - Constantly iterating based on feedback

Vision

Evolution of System Engineering (SE) to Model Based Engineering (MBE)



Source: https://www.boeingsuppliers.com/modelbasedengineering.html

Conclusion

Presentation Summary

- Kicked off the MBSE for PA Series with a presentation focused on
  - System Safety on CRP and MRP
  - Early Lifecycle (Starting with Conceptual Development and ending with Detailed Design)
- Demonstrated how MBSE & related tools enabled powerful linkages between requirements, functions, architecture, hazards, artifacts, & teams
- Showed MBSE was used for System Safety analyses to great effect, increasing efficiency, fidelity, & interconnectivity (within & between artifacts)
- Discussed what worked well & what lessons were learned while executing programs
- Highlighted future considerations for analytical integration & expansion
- Emphasized key lessons:
  - SE fundamentals are vital for MBSE; MBSE tools do not absolve a program from needing solid SE fundamentals
  - MBSE tools enable extremely powerful linkages to be established in a single central repository
  - Not everything can be easily captured, analyzed, and delivered via a MBSE model at this time
- Connected MBSE and PA to Boeing's ongoing digital transformation via MBSE/PA solution kits

Acronyms

- ABL: Allocated Baseline
- ABSM: Allocated Baseline System Model
- AFHA: Aircraft Functional Hazard Assessment
- AFTA/SFTA: Aircraft & System Fault Tree Analysis
- CDR: Critical Design Review
- CRP: Civilian Rotorcraft Platform
- CSI: Critical Safety Item
- DAL: Development Assurance Level
- DD: Detailed Design
- EASA:
- FAA:
- FBL: Functional Baseline
- FBSM: Functional Baseline System Model
- FDAL: Function Development Assurance Level
- FH: Flight Hour
- FMECA: Failure Modes Effects & Criticality Analysis
- FTA: Fault Tree Analysis
- HMMP/R: Hazardous Material Management Program Plan/Report
- IDCR: Initial Design Concept Review
- IDFR: Initial Design Functional Review
- IDRR: Initial Design Requirements Review
- IPT: Integrated Product Team
- MBE: Model-Based Engineering
- MBSE: Model-Based Systems Engineering
- MOSA: Modular Open Systems Approach
- MRP: Military Rotorcraft Platform
- O&SHA: Operating & Support Hazard Analysis
- OMB: Operational Model Baseline
- PA: Product Assurance
- PBL: Product Baseline
- PD: Preliminary Design
- PDR: Preliminary Design Review
- PS: Product Support
- PSSA: Preliminary System Safety Assessment
- PSSCFA: Preliminary Software Safety Critical Functional Analysis
- RAC: Risk Assessment Code
- RAM: Reliability/Availability/Maintainability
- RWB: Reliability Workbench
- SE: Systems Engineering
- SFHA: System Functional Hazard Assessment
- SFR: System Functional Review
- SHA/SSHA: System/Subsystem Hazard Analysis
- SMS: Safety Management System
- SRHA: System Requirements Hazard Analysis
- SRR: System Requirements Review
- SS: System Safety
- SSPP: System Safety Program Plan
- STPA: System-Theoretic Process Analysis
- UCA: Undesirable Control Action
- WRR: Windchill Risk & Reliability

34th Annual INCOSE international symposium

hybrid event

Dublin, Ireland
July 2 - 6, 2024

www.incose.org/symp2024
#INCOSEIS