NASA's Safety, Reliability, and Mission Assurance Digital Future





Wednesday, January 25th, 8 – 10am

Anthony John DiVenti Jr.

NASA Office of Safety & Mission Assurance (OSMA)



The 69th Annual Reliability & Maintainability Symposium

Overview and Outline (1 of 2)

- Background: The Perfect Storm
- Introduction: SMA's Challenge
- OSMA's Safety & Mission Success (S&MS) Framework
- Enabling a Model-Based (MB) Interoperable Digital Environment
- Transformative Building Blocks
- Emerging Capabilities and Benefits
- Next Steps

Preliminary

Background: *The Perfect Storm*

Digital Transformation (DT)

[**dij**-i-tl trans-fer-**mey**-shuhn] *noun*:

Employing digital technologies to change a process, product, or capability so dramatically that it's unrecognizable compared to its traditional form.

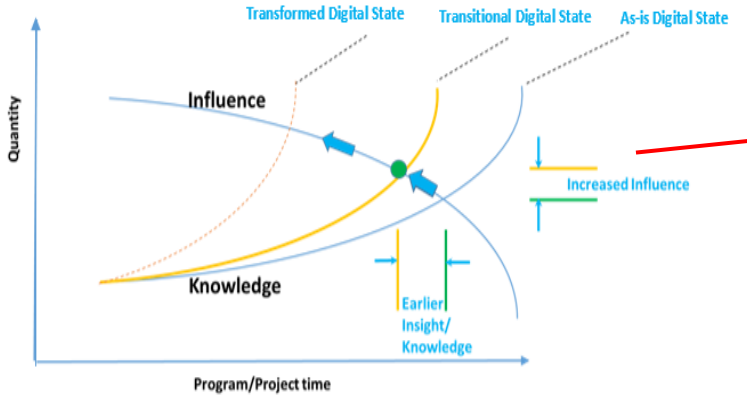
From Maps to Apps…
Digital Transformation has already changed our world



NASA's DT Strategic Framework (7/31/22)



Introduction: *SMA's Challenge*

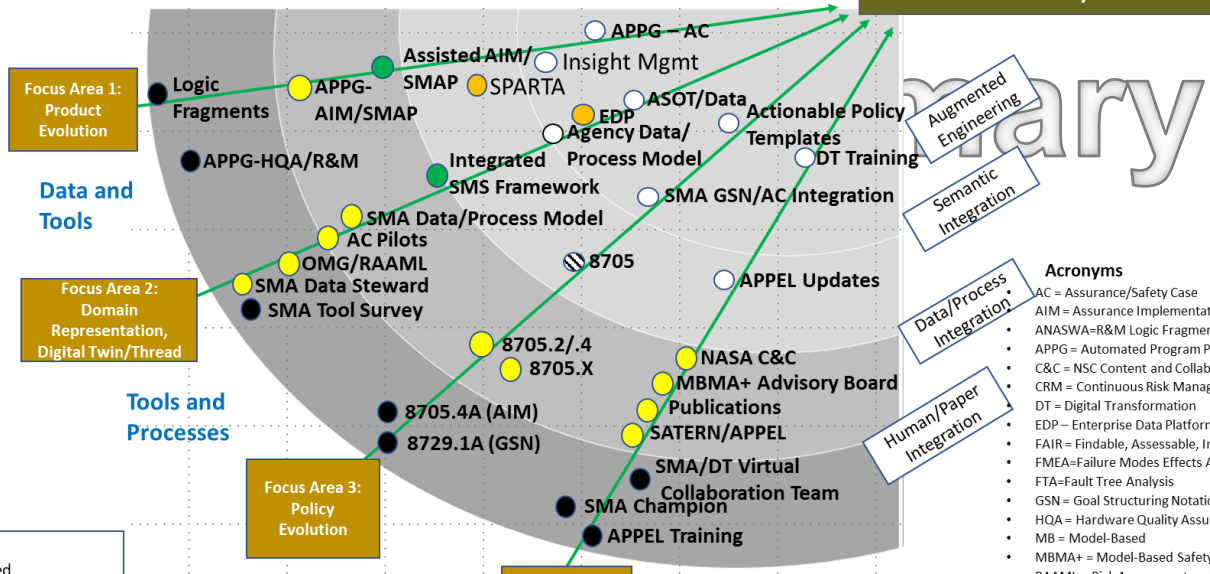


Support Critical Decision Making

1. Increased Decision Velocity,
2. Risk Integration and Robust Contextualization
3. Maximize Efficiency

"Risk Posture"
"Risk Acceptance"

Transform

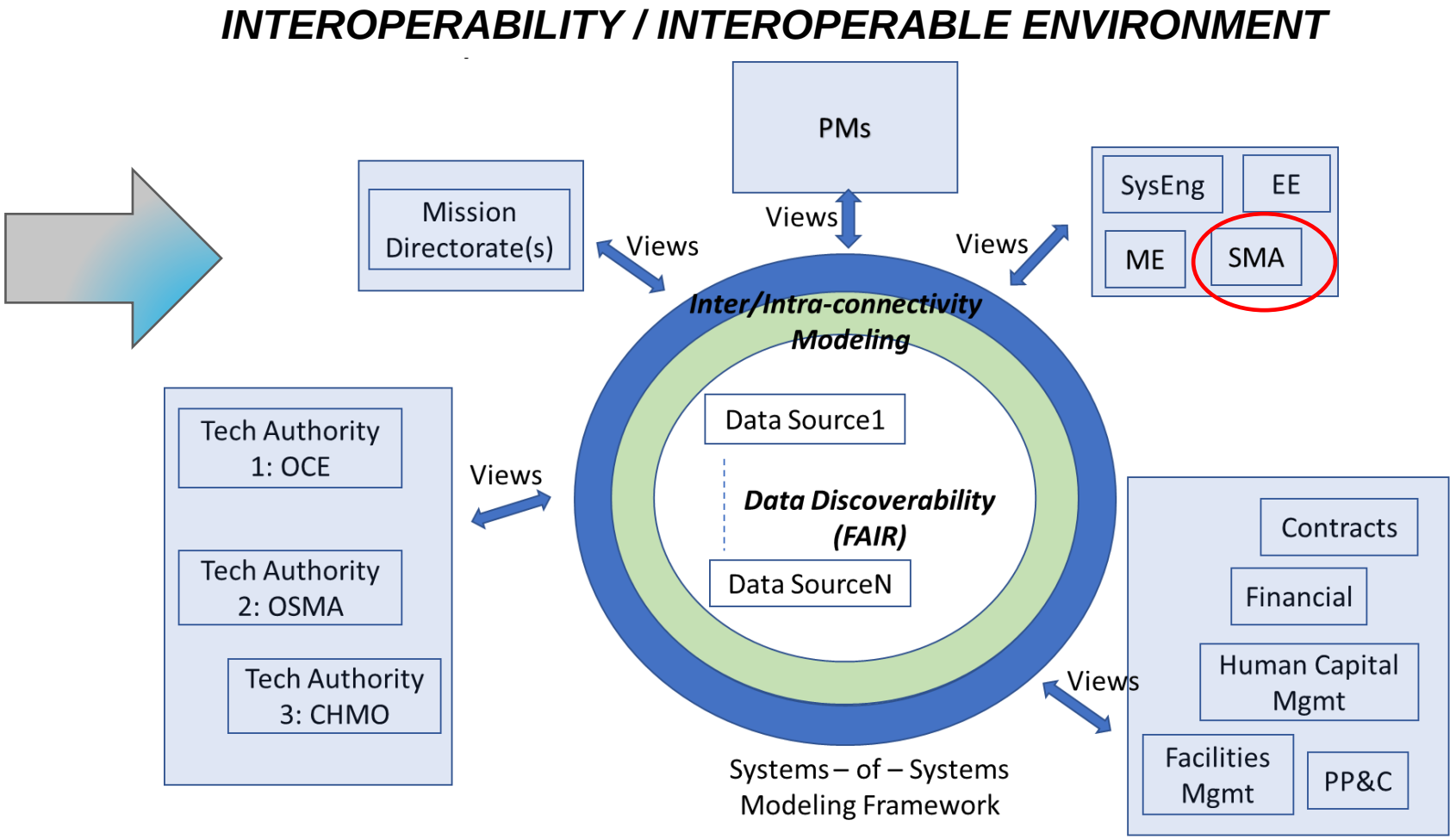


LEGEND
- Completed
- SMA-2022/23 InProgress
- SMA- 2023 Start
- DT-In Progress
- Research Needed

Acronyms
- AC = Assurance/Safety Case
- AIM = Assurance Implementation matrix
- ANASWA=R&M Logic Fragment Engine
- APPG = Automated Program Plan Generator
- C&C = NSC Content and Collaboration Project
- CRM = Continuous Risk Management
- DT = Digital Transformation
- EDP – Enterprise Data Platform
- FAIR = Findable, Assessable, Interoperable and Reusable
- FMEA=Failure Modes Effects Analysis
- FTA=Fault Tree Analysis
- GSN = Goal Structuring Notation
- HQA = Hardware Quality Assurance
- MB = Model-Based
- MBMA+ = Model-Based Safety and Mission Assurance
- RAAML = Risk Assessment and Modeling Language
- RIDM = Risk Informed Decision Making
- SMA = Safety and Mission Assurance
- SMAP = SMA Plan
- SPARTA=Smart Project and Reviews with Transformative Analytics (SPARTA)

MASTER 4.15.22

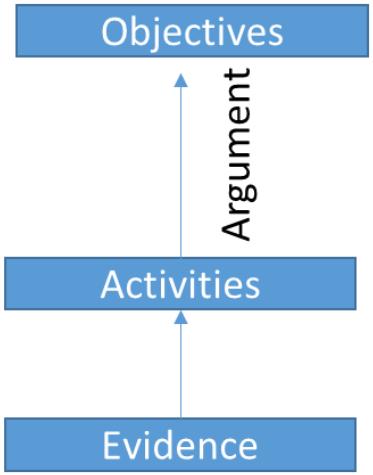
Introduction: *SMA's Challenge*



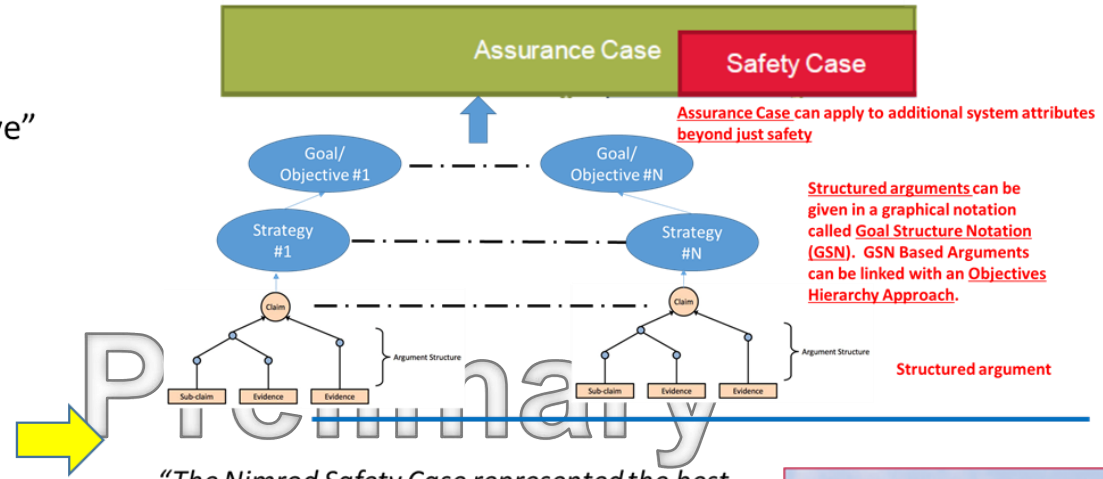
OSMA's S&MS Framework

Objectives-Driven Hierarchy

They contrast with "prescriptive" requirements (must do X, Y, Z)



An **Assurance Case** is an organized argument that a system is acceptable for its intended use with respect to specified concerns



"The Nimrod Safety Case represented the best opportunity to capture the serious design flaws …which had lain dormant for years. ***If the Nimrod Safety Case had been drawn up with proper skill, care, and attention,*** *the catastrophic fire risks …, would have been identified and dealt with, and the loss of XV230 in September 2006 would have been avoided"*[2]



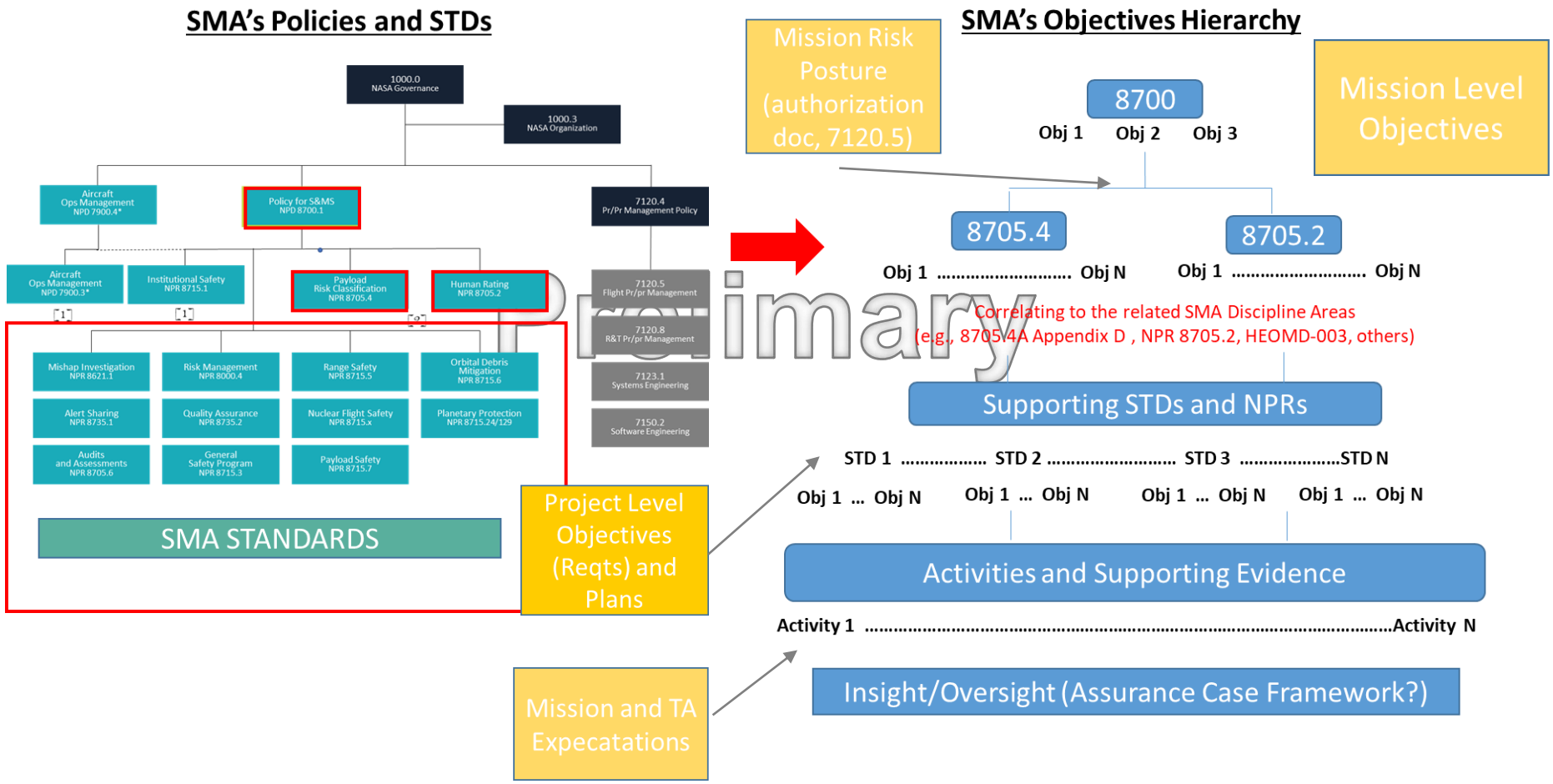
Assurance Cases, starting from Objective Hierarchies, enable our "transformed" SMA Framework

Enabling an MB Interoperable Environment

Policy Enabled

Integrated Objectives Hierarchy/Assurance Case Framework

On-Ramp for SMA Interoperability



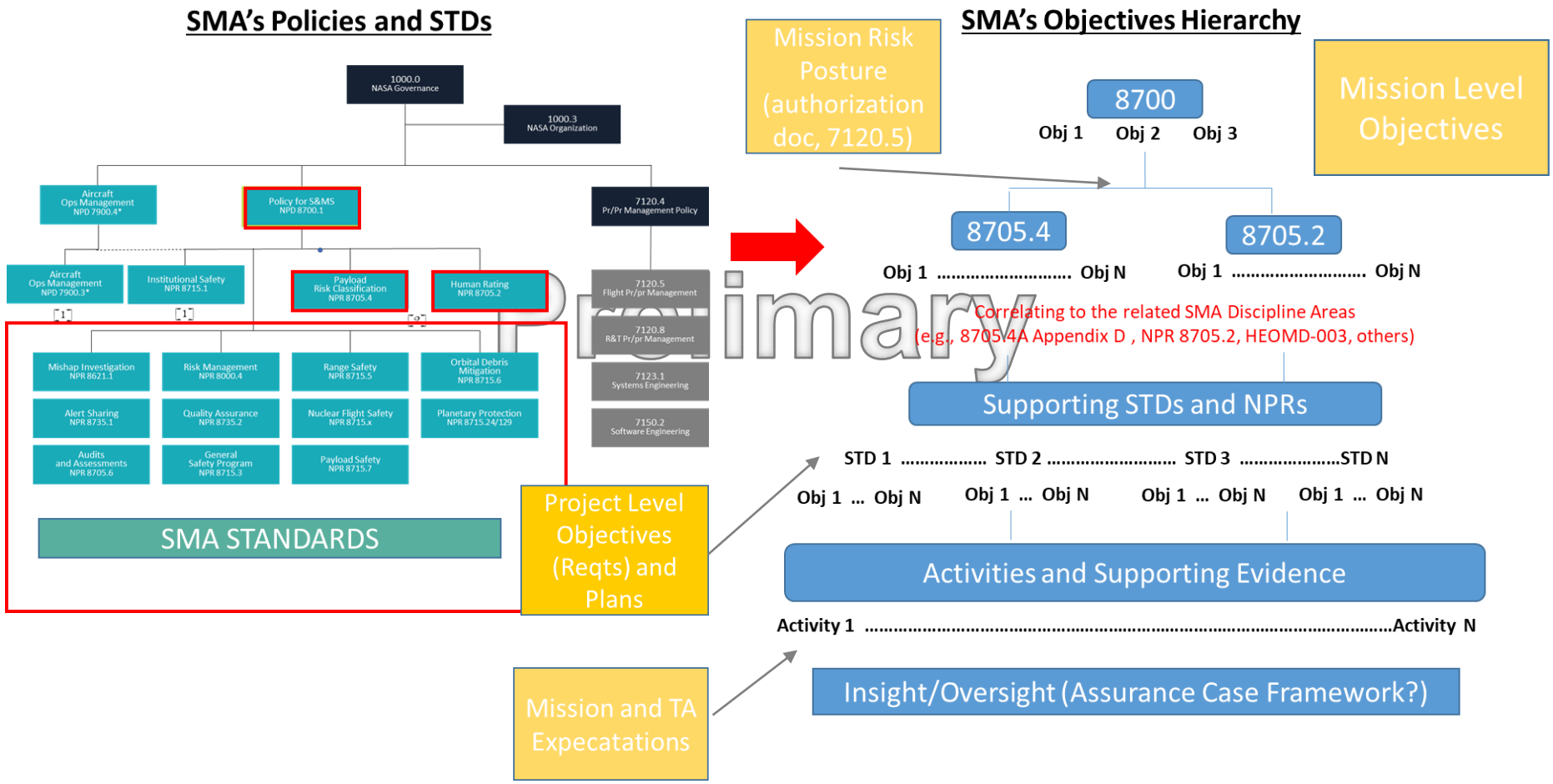
Primary

Enabling an MB Interoperable Environment

Policy Enabled

Integrated Objectives Hierarchy/Assurance Case Framework

On-Ramp for SMA Interoperability

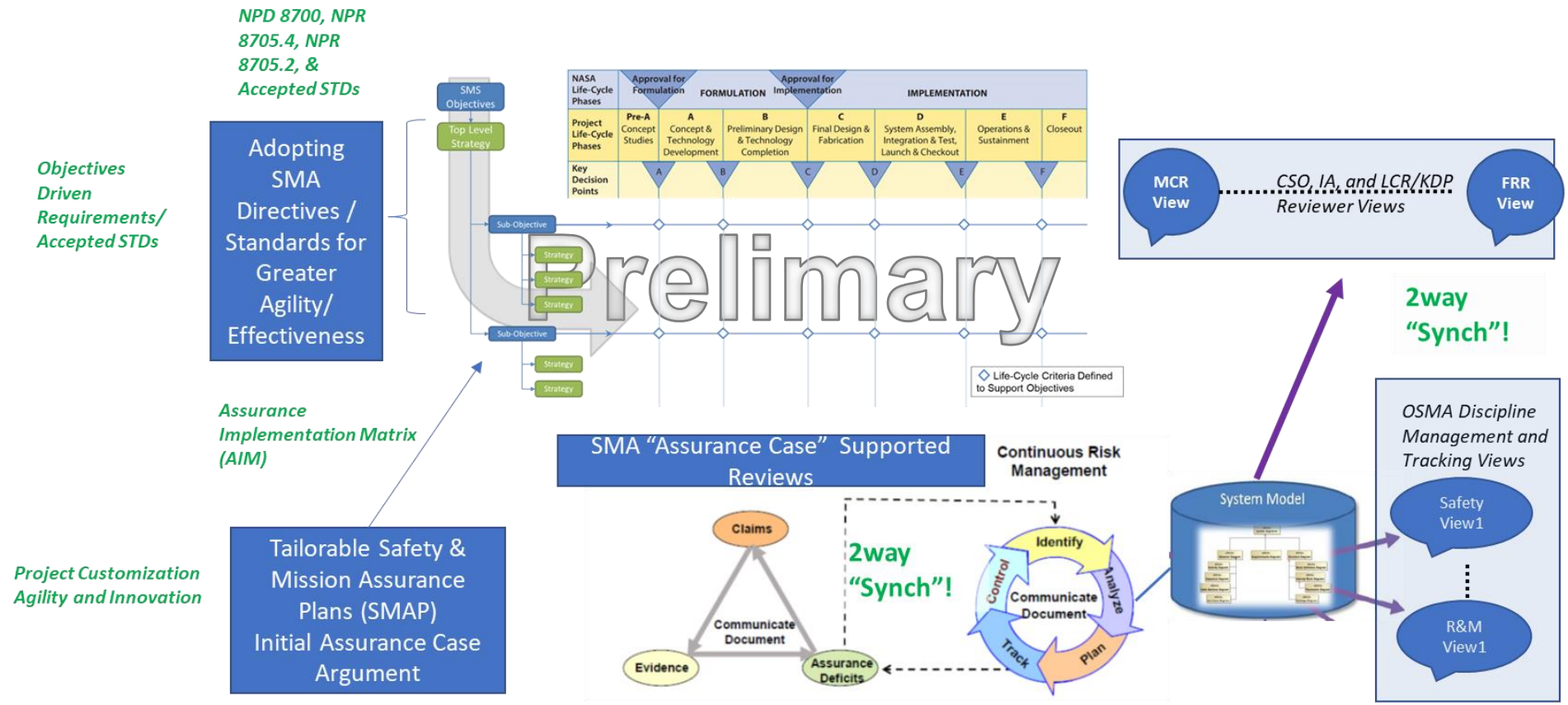


Primary

Enabling an MB Interoperable Environment

SMA's Digital Future

Digital Twin enabled Objectives Hierarchy/SMS Assurance Case Framework with Machine-Assisted Planning, Machine-Assisted Assurance Case Development, and Machine-Assisted Reviews



Transformative Building Blocks

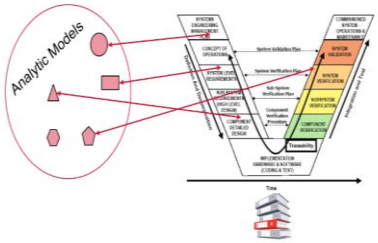


Policy

GSN, Objective Driven Requirements, Accepted STDs, Objectives Hierarchy

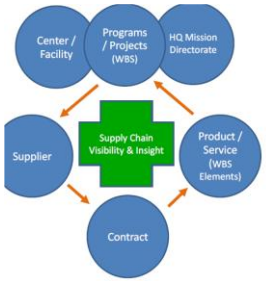
Processes/ STDs

Logic Fragments



Authoritative Source(s)
- EDP
- Digital Libraries

SMA Ontology



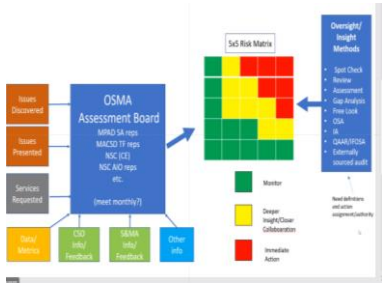
STDs / Common Languages
- OMG's SysML
- ISO/IEC 21838-2 (BFO)

Prelimary

Assurance Case Framework - Life Cycle Reviews, Safety & Assurance Case Development

Assurance Case(s)

SMS Framework/ Digital Twin



Emerging Capabilities and Benefits

Capabilities

- Machine Assisted Development and Analysis
  - APPG
    - AIM
    - SMAP
    - Contract Clauses
  - SysML Plug-Ins
- Machine-Assisted Reviews
- Top-Down / Bottoms – Up Traceability

Benefits

Prelimary

Summary & Conclusion

Prelimary

Next Steps and Future Work

- Questions to or from the audience

Prelimary