Instantiating Safety and Mission Assurance as part of NASA's Evolving Digital Engineering (DE) ecosystem

Tony DiVenti
OSMA – MASCD
(NASA MBMA Program Lead & R&M Technical Fellow)

Tri SMAC 2024
June 2024

Acronyms

- AC = Assurance/Safety Case
- AIM = Assurance Implementation matrix
- APPG = Automated Program Plan Generator
- ASoT = Authoritative Source of Truth
- C&C = NSC Content and Collaboration Project
- CRM = Continuous Risk Management
- DE = Digital Engineering
- DT = Digital Transformation
- DRD = Data Requirements Document
- 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 (Note: inclusive of all Safety and Mission Assurance areas at NASA)
- MOU = Memorandum of Understanding
- NGOs = Needs, Goals, and Objectives
- NPD = NASA Policy Directive
- NPR = NASA Procedural Requirement
- RAAML = Risk Analysis and Assessment Modeling Language
- RIDM = Risk Informed Decision Making
- SMA = Safety and Mission Assurance
- SMAP = SMA Plan
- STD = Standard

Agenda

Background: Importance of a “Digital” SMA and Engineering Partnership

Key OSMA - OCE Focus Areas

- DE / MBMA / Digital SMA Implementation Plan and Strategic Roadmap Integration
- Common Data-Centric Approach to NPRs/NPDs/NASA-Specific STDs
- Digital Engineering Acquisition Best Practices (e.g., Contract DRD Template Language)
- Data flow in support of informing Milestone Review Decisions
  - Engineering V&V Framework
  - Case-Assured Framework

Next Steps

- Potential OCE and OSMA MOU

Background

Why: Engineering and SMA need to ***TRANSFORM*** to manage the growing complexity of systems, both development and operations, by integrating information sources, analysis processes, and tools that were largely Stove-Piped in the past to enable the seamless flow of information in support of NASA Missions

Engineering Role & Responsibilities

(Pull from NASA 1000.B, 7123.1, 7120.5)

Provides leadership, policy direction, functional oversight, assessment, and coordination for Engineering and related Technical Disciplines, including Systems Engineering.

Digital Engineering (DE): "An integrated digital approach that uses authoritative sources of systems data and models as a continuum across disciplines to support lifecycle activities from concept through disposal". [1]

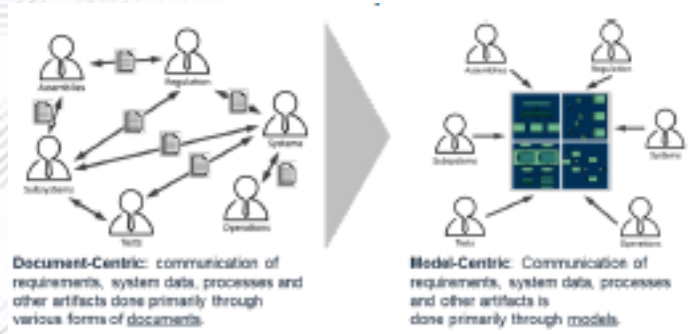
A ***digital engineering ecosystem*** includes Enterprise interconnected digital environments, stakeholder-networks, and semantic and ontological reasoning that allows the exchange of digital artifacts from an authoritative source of truth to serve the stakeholder communities' interests [1].

[1] U.S. Department of Defense (DoD) Digital Engineering (DE) Strategy, https://man.fas.org/eprint/digeng-2018.pdf

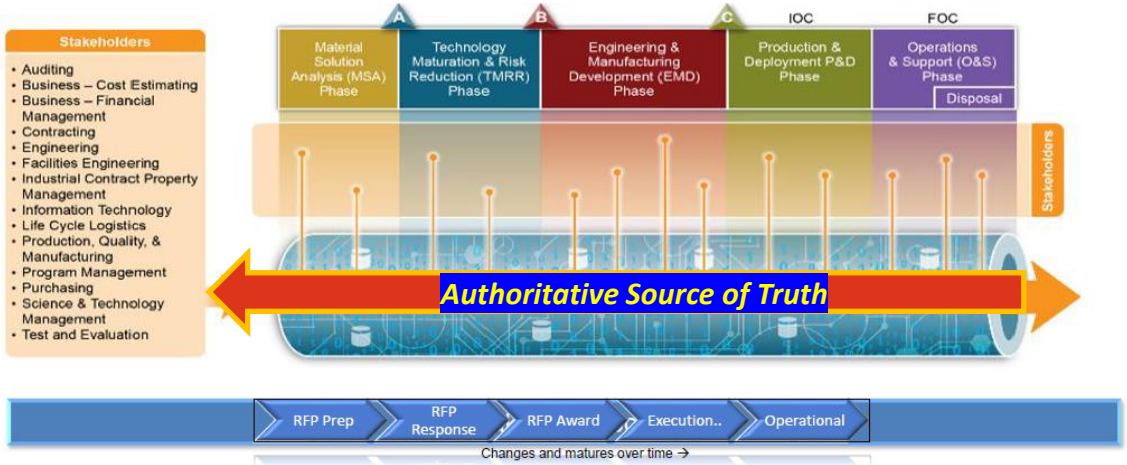
Safety & Mission Assurance Role & Responsibilities

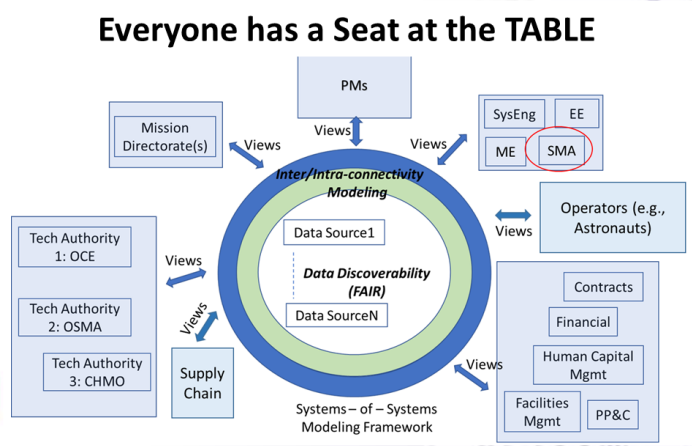
(Pull from NASA NPD 8700)

1. Acceptable Risk Levels for Crew Safety and Mission Success
2. Protect Public, Workforce, Property, and environment
3. Cultivate a Robust Safety Culture. Pursue Organizational/Technical Excellence to understand/reduce risks



Document to Data and/or Model Centric Modeling





Agenda

Background: Importance of a “Digital” SMA and Engineering Partnership

Key OSMA - OCE Focus Areas

- DE / MBMA / Digital SMA Implementation Plan and Strategic Roadmap Integration
- Common Data-Centric Approach to NPRs/NPDs/NASA-Specific STDs
- Digital Engineering Acquisition Best Practices (e.g., Contract DRD Template Language)
- Data flow in support of informing Milestone Review Decisions
  - Engineering V&V Framework
  - Case-Assured Framework

Next Steps

- Potential OCE and OSMA MOU

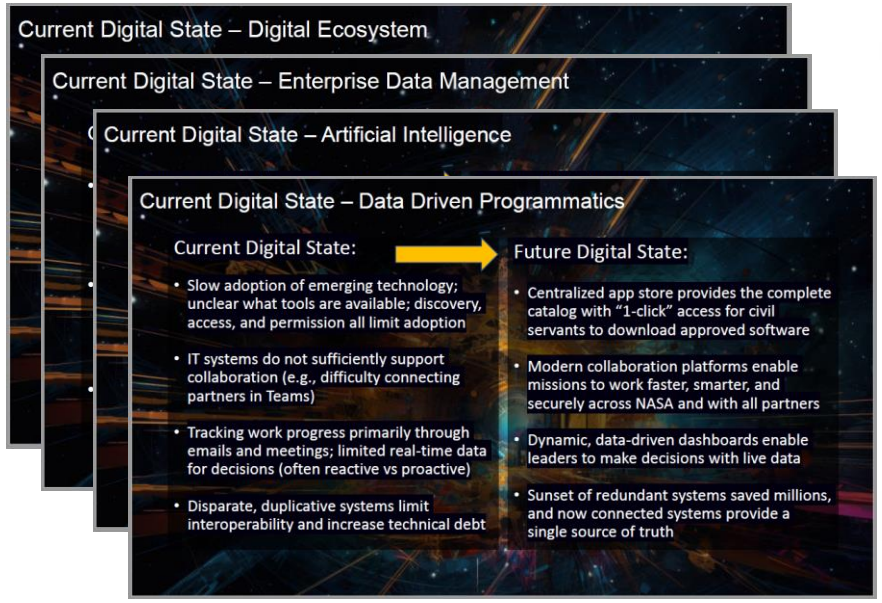
DE / MBMA / Digital SMA Implementation Plan and Strategic Roadmap Integration

Enterprise Gains → **Future Digital States (e.g., NASA 2040 Vision)**

Incremental short-term Gains
(Address Org Goals / Data Flow / Pain Points)

2023 2024 2025 20xx

- Digital Engineering (MBE/MBSE) Implementation Plan
- Digital SMA (MBMA) Implementation Plan
- Centers
- Govt/ Industry Partners



NASA's DT Initiative

Integrated Digital Engineering (DE) / MBMA / Digital SMA Implementation and Strategic Plan(s) — leverages → Agency Roadmap Manager (ARM)

DE / MBMA/ Digital SMA Implementation Plan and Strategic Roadmap Integration

Tactical (Incremental Gains): DE / Digital SMA Implementation Plan

OSMA / SMA Strategic Objectives

- Help Customer Products & Reviews
- Enable Risk Leadership
- Effective Policy
- Efficient Resources
- Applicable Processes
- Communication & Coordination
- Organizational Excellence
- Digital Capabilities

Digital SMA Strategic Objectives

- Robust, Evidence Based, Closed Loop Feedback Solicitation
- Digital Enablement of Risk Indicators
- Digital SMA Policy Implementation
- Maximize MBMA/Technology Solution Office (TSO) transformation efficiency
- Digital SMA Command Media, Tools, & Guidance
- Increase Internal / External Communication, Coordination, and Collaboration
- Cultivate Technical / Organizational Excellence part of the evolving Digital SMA / Engineering environments
- Provide overall Digital SMA Leadership, Cross Activity Alignment and Coordination

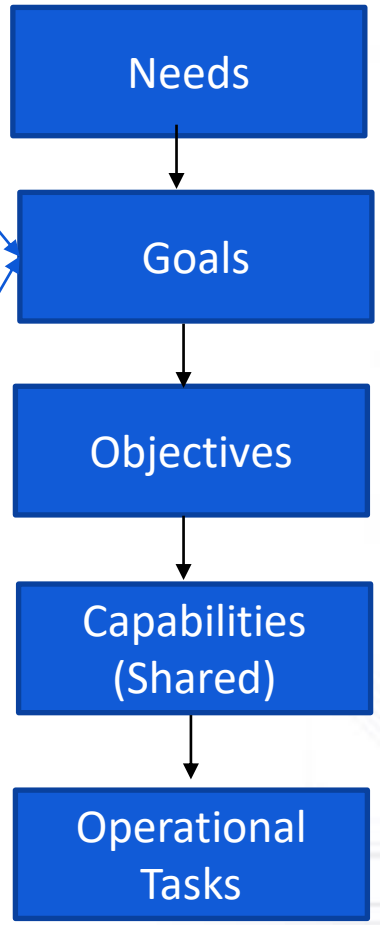
Engineering Needs

Improve how the Agency Engineering Domain operates over the entire NASA lifecycle by effectively managing complexity, reducing cost and schedule, and improving product integrity via the integration of processes, digital tools, and techniques along with seamless flow of information throughout the engineering system development life-cycle (concept development, design, testing and validation, manufacturing and operations).

DE Goals

- **G1 Lifecycle:** Establish a Digital Engineering (DE) strategy that can be integrated throughout the entire Engineering Life Cycle, aligning with NASA's mission objectives.
- **G2 Deployment:** Develop an interoperable, tailorable, and scalable deployment strategy for the Digital Engineering Ecosystem across the Centers including implementation options and methods.
- **G3 Guidance:** Establish the guidance for model development, tool integration and deployment, and formulation of data threads while ensuring alignment with the industry standards advocated by DE.
- **G4 ASoT:** Establish an approach providing stewardship, governance, security, traceability, and management of the engineering Authoritative Sources of Truth (ASoT), while ensuring the data within the ASoT are curated.
- **G5 Configuration/Change Management:** Evolve existing CM approaches for data-centric management of engineering baselines which enable teams to manage and track changes made throughout the entire product lifecycle.
- **G6 Digital Threads:** Develop strategies for Digital Threads/Ecosystem that improve collaboration, data exchange, design formulation, data-centric processes and workflows, operations, and insight, and data-informed decision making.
- **G7 Culture and Workforce:** Evolve NASA Culture and the Workforce by creating a demand for adoption of DE techniques, providing training, and cultivating a digital engineering community.

Simplified United Architectural Framework (UAF) illustration

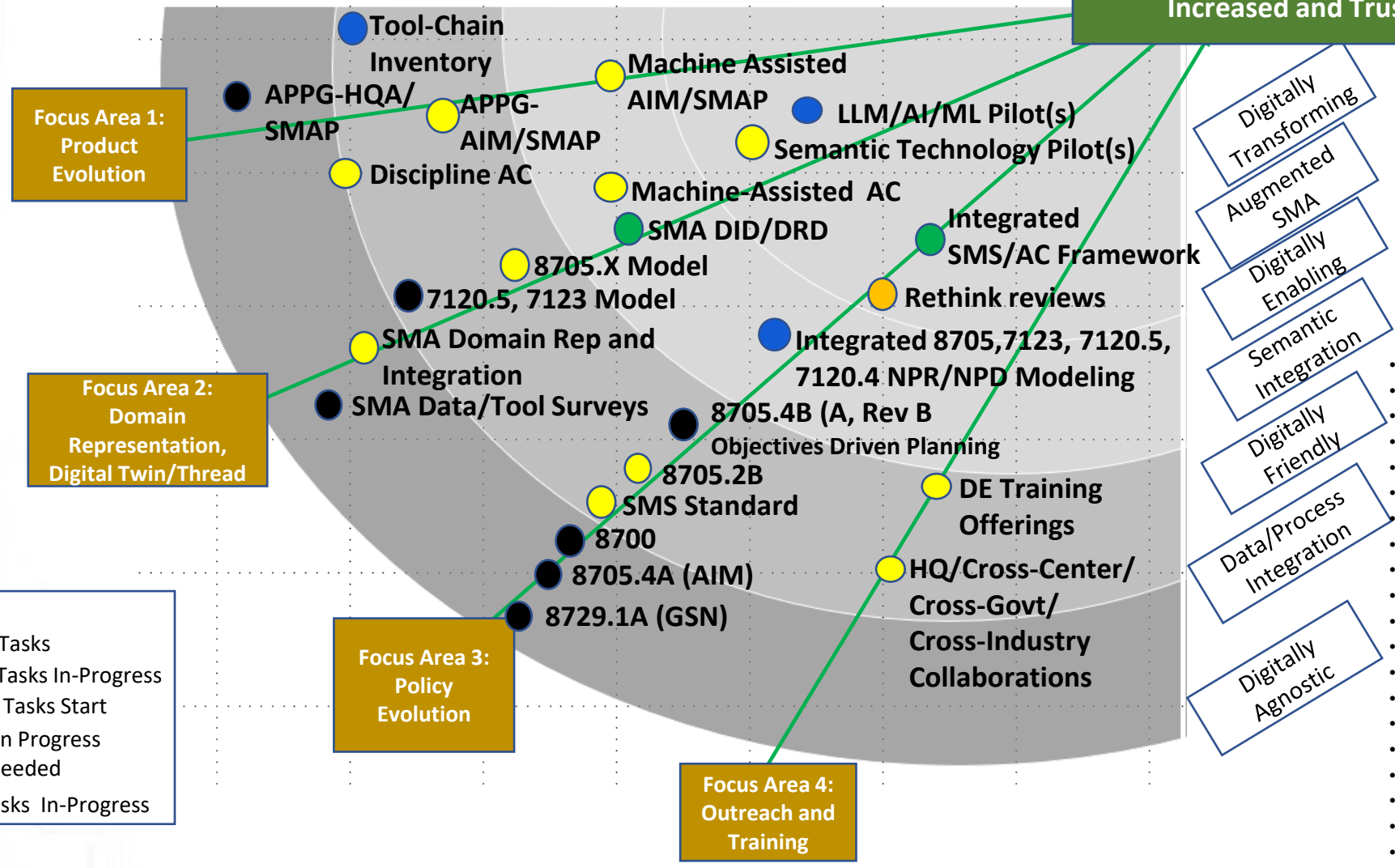


MBMA / Digital SMA Implementation Plan and Strategic Roadmap Integration

Strategic Focus: Transformation Gains towards a Future Digital State

Findable, Accessible, Interoperable, Reusable (FAIR)
Robust Contextualization
Maximize Efficiency
Increased and Trusted Decision Velocity

Evolving Digital SMA/ DT Strategic Roadmap



LEGEND

- Completed Tasks
- SMA-2024 Tasks In-Progress
- SMA- 2024 Tasks Start
- DE- Tasks In Progress
- Research Needed
- DE/SMA Tasks In-Progress

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)

DRAFT 5/17/2024

Common Data-Centric Approach to NPDs/ NPRs/ NASA Specific STDs

Objectives-Driven Development *provides an On-Ramp for Digital Objectives-Driven Planning and Assurance Case Framework*

"Parsing" the NPRs: an Example

From **NPR 8715.26, Sec 2.8:**

2.8 Chief, Safety and Mission Assurance

2.8.1 The Chief, SMA, is responsible for advising the Administrator and other senior officials on matters related to risk, safety, and mission success and serves as the lead SMA TA. To provide independent oversight of programs and projects in support of safety and mission success, the Chief, SMA, is responsible for:

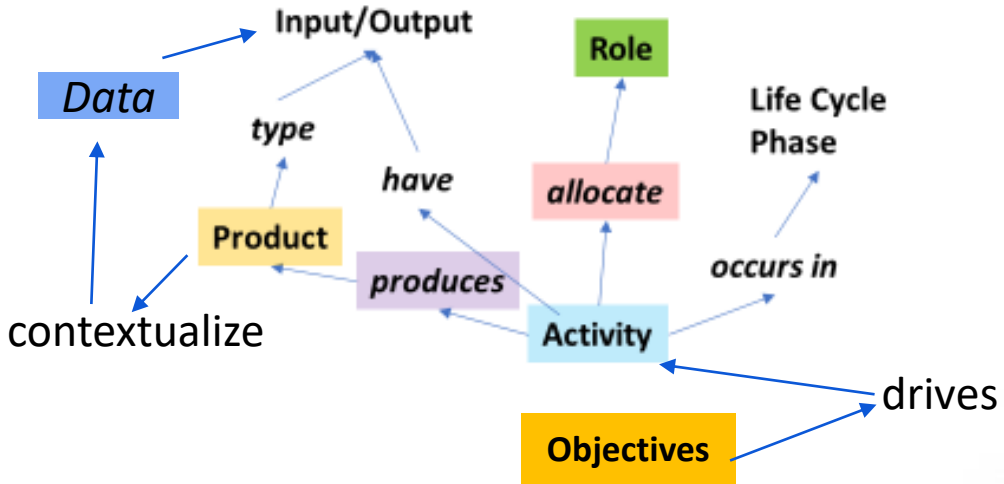
a. Appointing a technically-qualified NASA representative to the INSRB. Whenever possible, the NFSO should not serve as the INSRB member performing the review or administrative support for a NASA-sponsored mission because the INSRB and the NFSO have different roles

LEGEND

Role	An Actor/actor's part	Argument*	Structured Assertion
Activity	Things being done	Case*	Assurance Case
Product	Things produced	Objectives*	Intended results
allocation	Assigned	Data*	Actual Data itself
produces	Creates/Results In	Evidence*	Pieces of "proof"

- ***Note1:*** *Only part of the MetaModel is explicitly highlighted in the above "snippet"*
- ***Note 2:*** *Products / Data are further elaborated (decomposed) in various Standards. Structure still in discussions.*
- ***Note3:*** *This explicit traceability will enable broader use of Assurance Cases*

Simplified "Ontology"

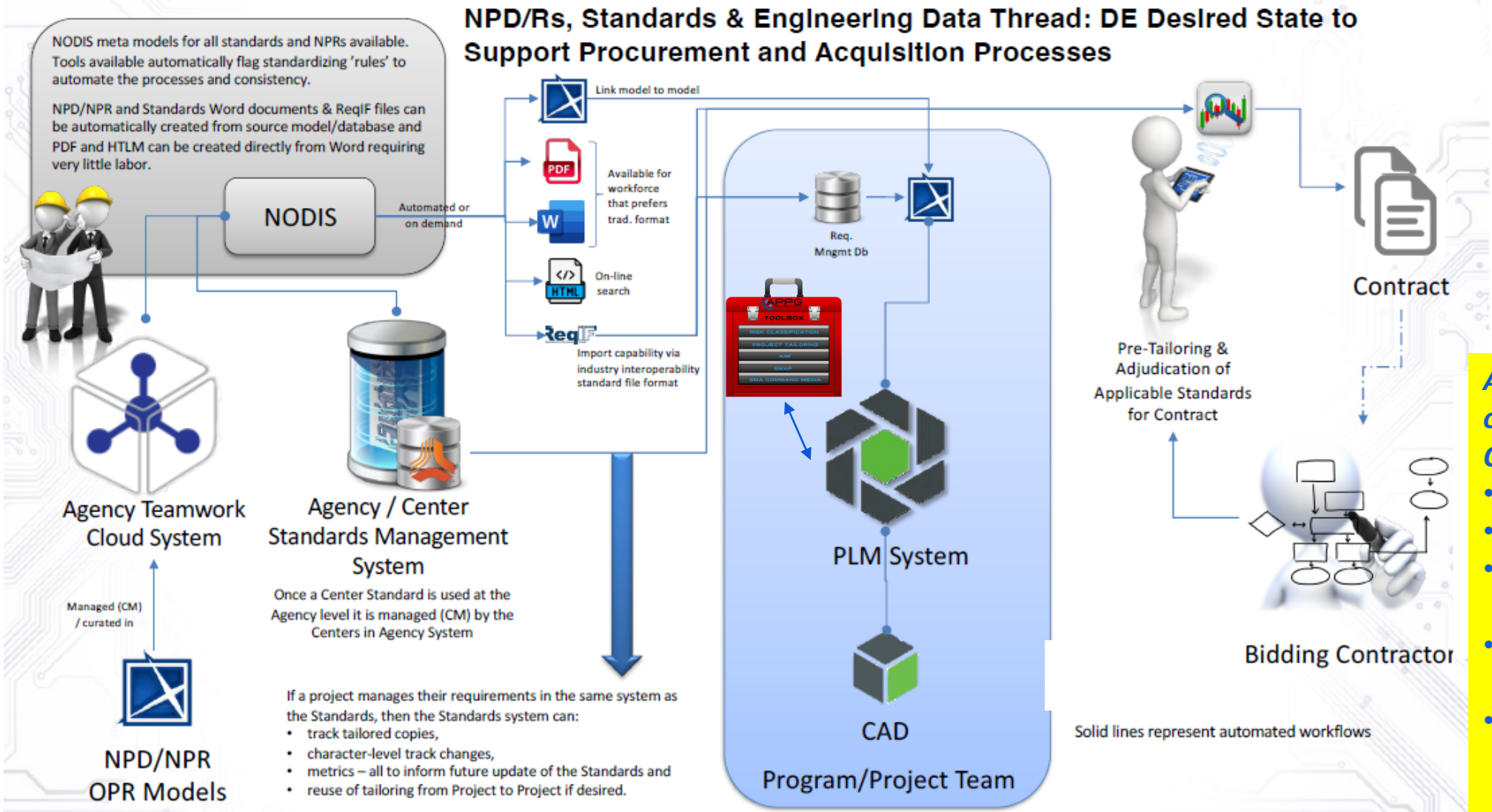


**Information not shown in the NPR 8715.26 illustration*

Digital Engineering Approach to Planning across the Lifecycle

Project Formulation → Project Design/Development → Operations

(Reference NASA-HDBK-1004)



DRDs/ DIDs

Define Required Artifacts, Data, Data Structure (e.g., Evidence)

Approach enables definition of SMA and Engineering Objectives-Driven:

- ***Products***
- ***Data***
- ***Human Readable Interfaces***
- ***Machine Readable Interfaces***
- ***Machine-Assisted Planning and Contract development***

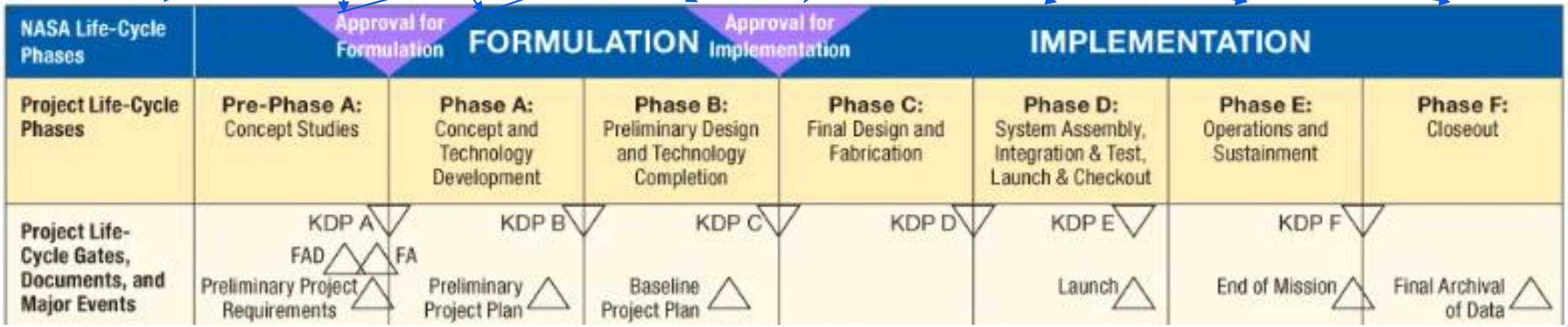
Data flow in support of informing Milestone Reviews Decisions

Define Required Inputs

Plans/Contracts/ DRDs/ DIDs
Define Required Artifacts, Data, Data Structure (E.g., Evidence)

Information Pipeline
(e.g., Data Sources, Data Brokers, Tool –to –Tool Chain Mapping, Data Threads, Data Tapestry, Interoperability)

Required Outputs in support of "V&V" or "Assurance Case" Decision Making



(Reference NASA-HDBK-1004 as a starting point)

Agenda

Background: Importance of a “Digital” SMA and Engineering Partnership

Key OSMA - OCE Focus Areas

- DE / MBMA / Digital SMA Implementation Plan and Strategic Roadmap Integration
- Common Data-Centric Approach to NPRs/NPDs/NASA-Specific STDs
- Digital Engineering Acquisition Best Practices (e.g., Contract DRD Template Language)
- Data flow in support of informing Milestone Review Decisions
  - Engineering V&V Framework
  - Case-Assured Framework

Next Steps

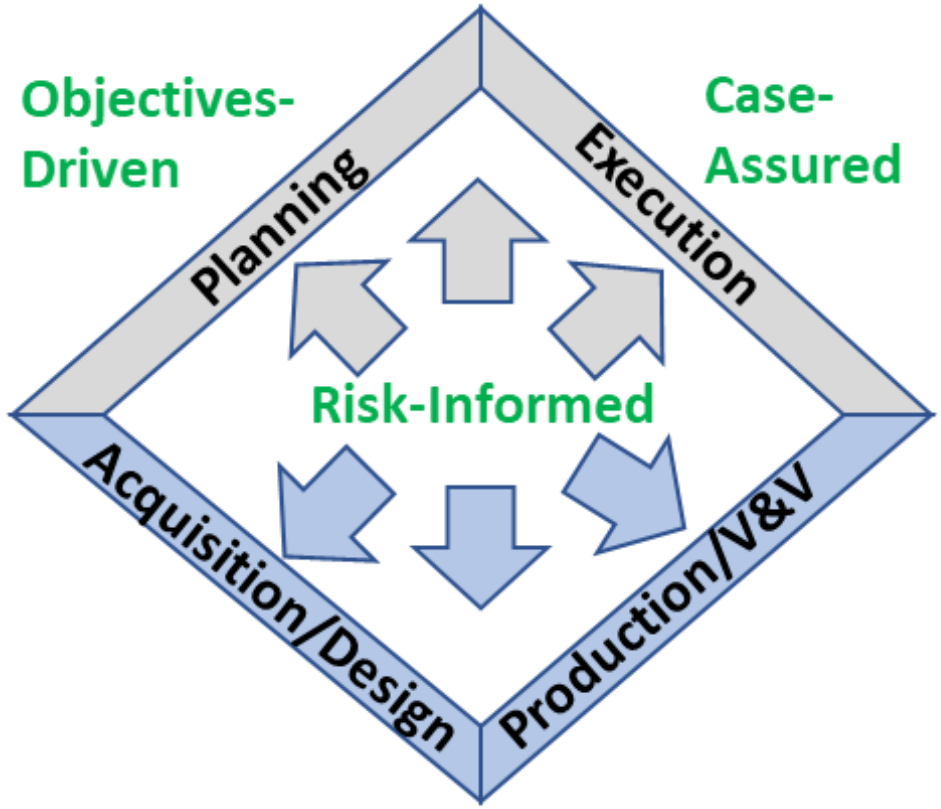
- Exploration of a formal ***OCE and OSMA MOU***

OCE and OSMA MOU

OCE and OSMA beginning to explore an MOU around the following:

- NGOs to MBMA / Digital SMA Objectives Roadmap and Implementation Plan integration
- Common Data-Centric Approach to NPRs/NPDs/NASA-Specific STDs
- Digital Engineering Acquisition Best Practices (e.g., Contract DRD Template Language)
- Data flow in support of informing Milestone Review Decisions
  - Engineering V&V Framework
  - Case-Assured Framework

Any Questions



NASA Project Life Cycle

BACK-UP

OSMA Strategic Objectives

#1 – **Help Customer Products & Review** - Increase Responsiveness to Mission, Institutional, & National Needs

(e.g., Customer focused, Data-Driven, Closed-Loop)

#2 – **Enable Risk Leadership** – Catalyze Culture of Technical & Organizational Risk Leadership & Management

(e.g., Technical Guidance, Risk-Informed Enablers / Tools)

#3 - **Enable Effective Policy** – Enable Missions and Institutions to Effectively & Efficiently Implement SMA

(e.g., Tool Enabled Objectives-Driven Policy Planning and Implementation)

#4 – **Efficient Resources** - Maximize Effectiveness of Resources for Internal Initiatives and Operations

(e.g., OSMA Objective-Funded Activity Alignment; Cross-Domain alignment around common needs/capabilities)

#5 - **Enable Processes** – Make SMA Processes / Services More Objectives-driven and Risk Informed

(e.g., Objectives-Driven Process controls, Risk Informed Planning)

#6 – **Increase Communications and Coordination** – Increase Internal and External Communication, Coordination, and Collaboration

(e.g., Forums, Cross Domain Forums, Communication Vehicles)

#7 – **Enable Organizational Excellence** – Cultivate Technical and Organizational Excellence

(e.g., Resource Development, Training, Best Practices)

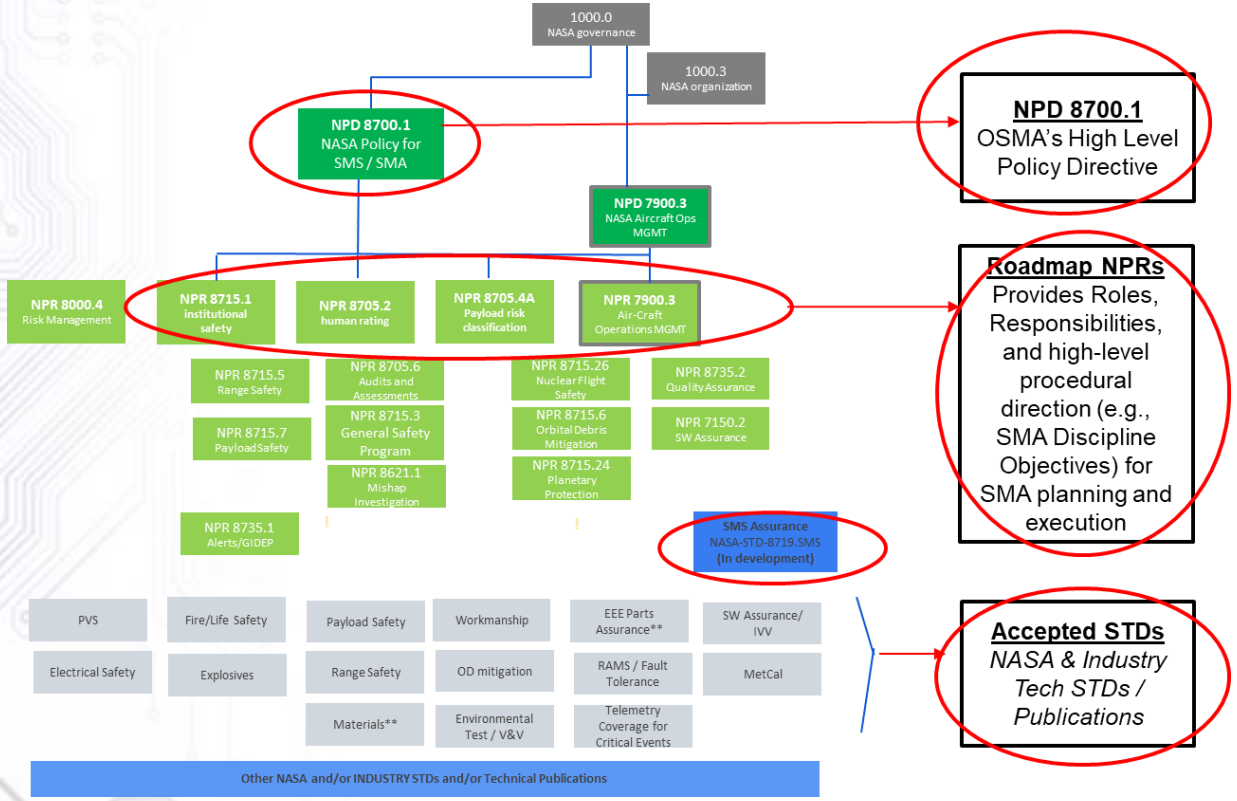
#8 – **Build Capabilities** – Adjust Capabilities & Tools to Support Emerging Needs

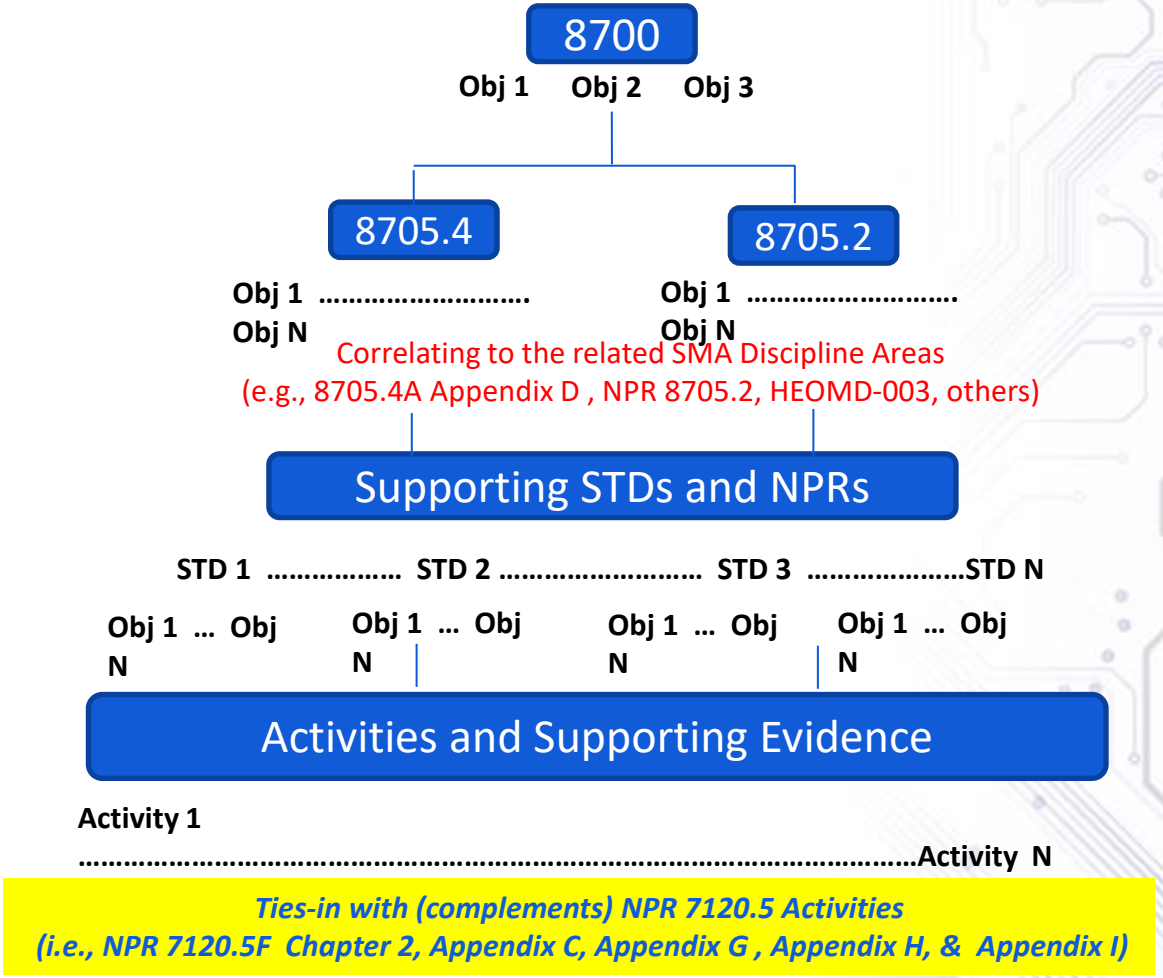
(e.g., Digital SMA Strategy, Digitally enable Workforce / Capabilities , Data Access for Decision Making)

Objectives-Driven Reqts and Use of Accepted STDs

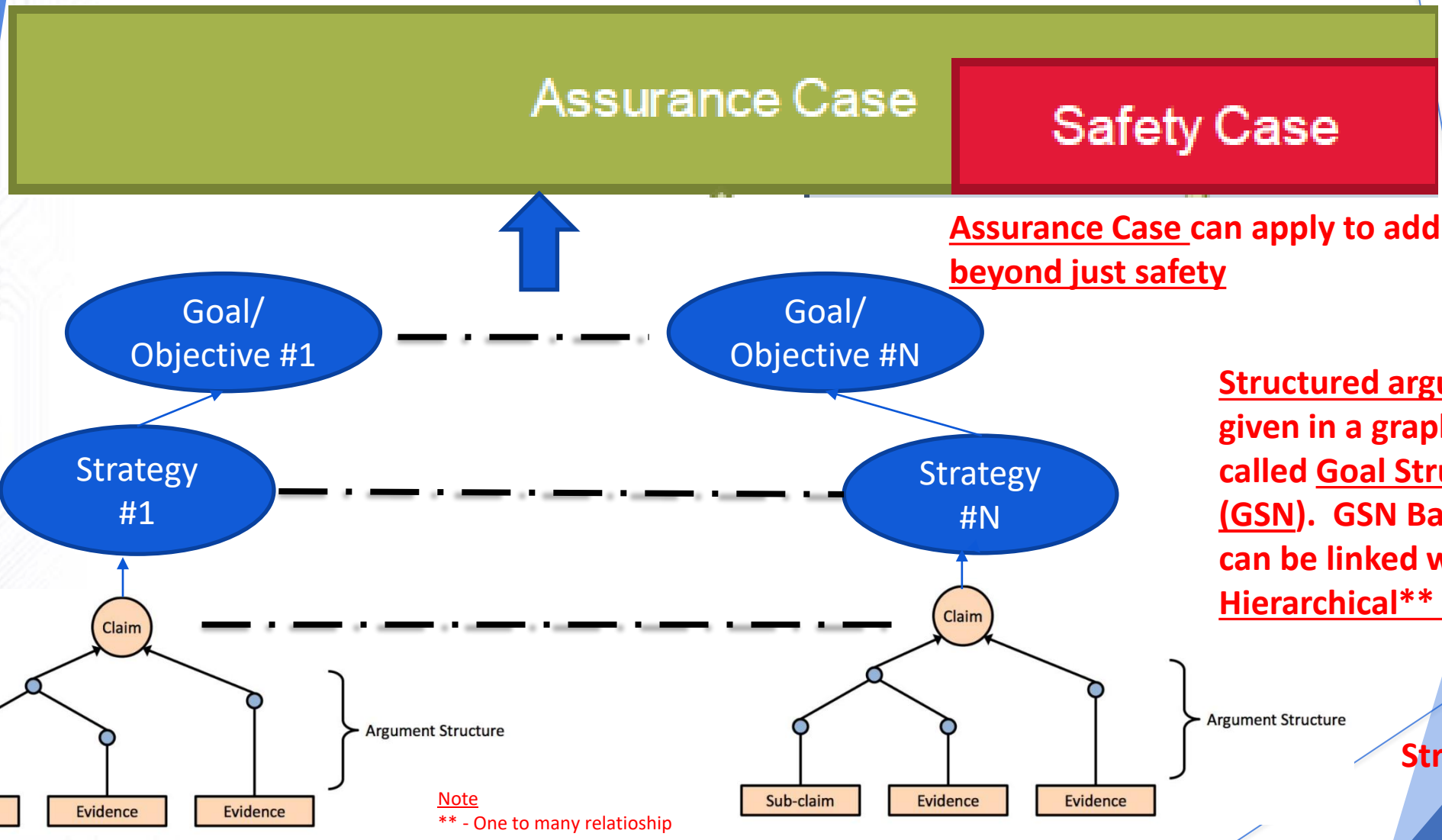
OSMA's Policy Enabled <u>Objectives Hierarchical Structure</u> *provides an <u>On-Ramp for Digital Objectives-Driven Planning and Assurance Case Framework</u>*

- Top-Level SMA and Mission Objectives
- SMA Discipline Area Objectives
- Risk Posture/Risk Class Objectives Driven
- Accepted (including Alternatives) Standards





Conceptual Illustration



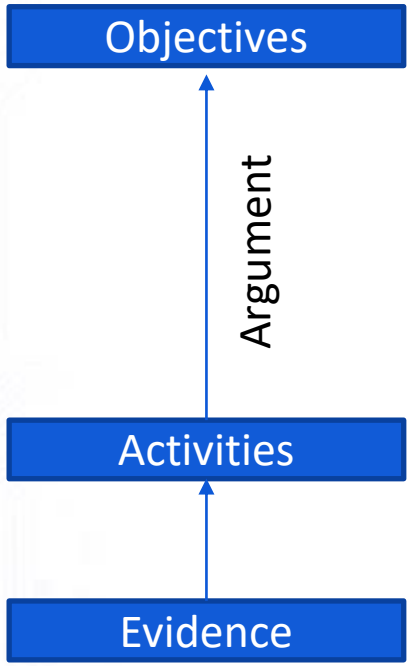
Assurance Case can apply to additional system attributes beyond just safety

Structured arguments can be given in a graphical notation called Goal Structure Notation (GSN). GSN Based Arguments can be linked with an Objectives Hierarchical** Approach.

Structured argument

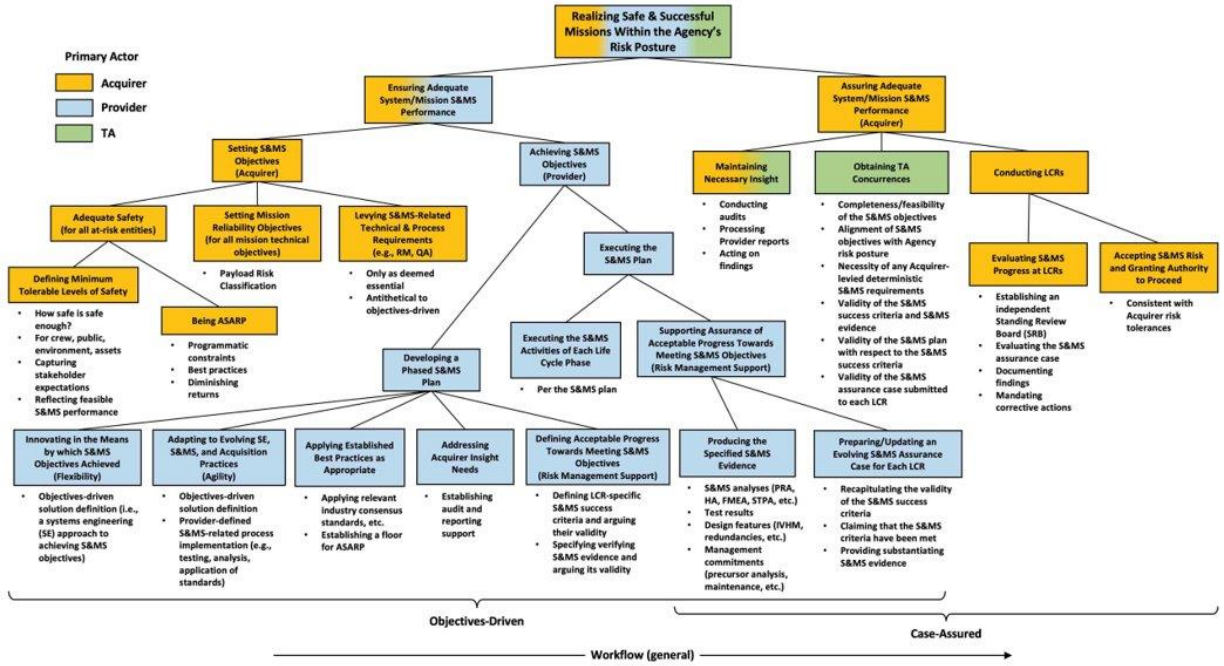
Objectives-Driven Hierarchy

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



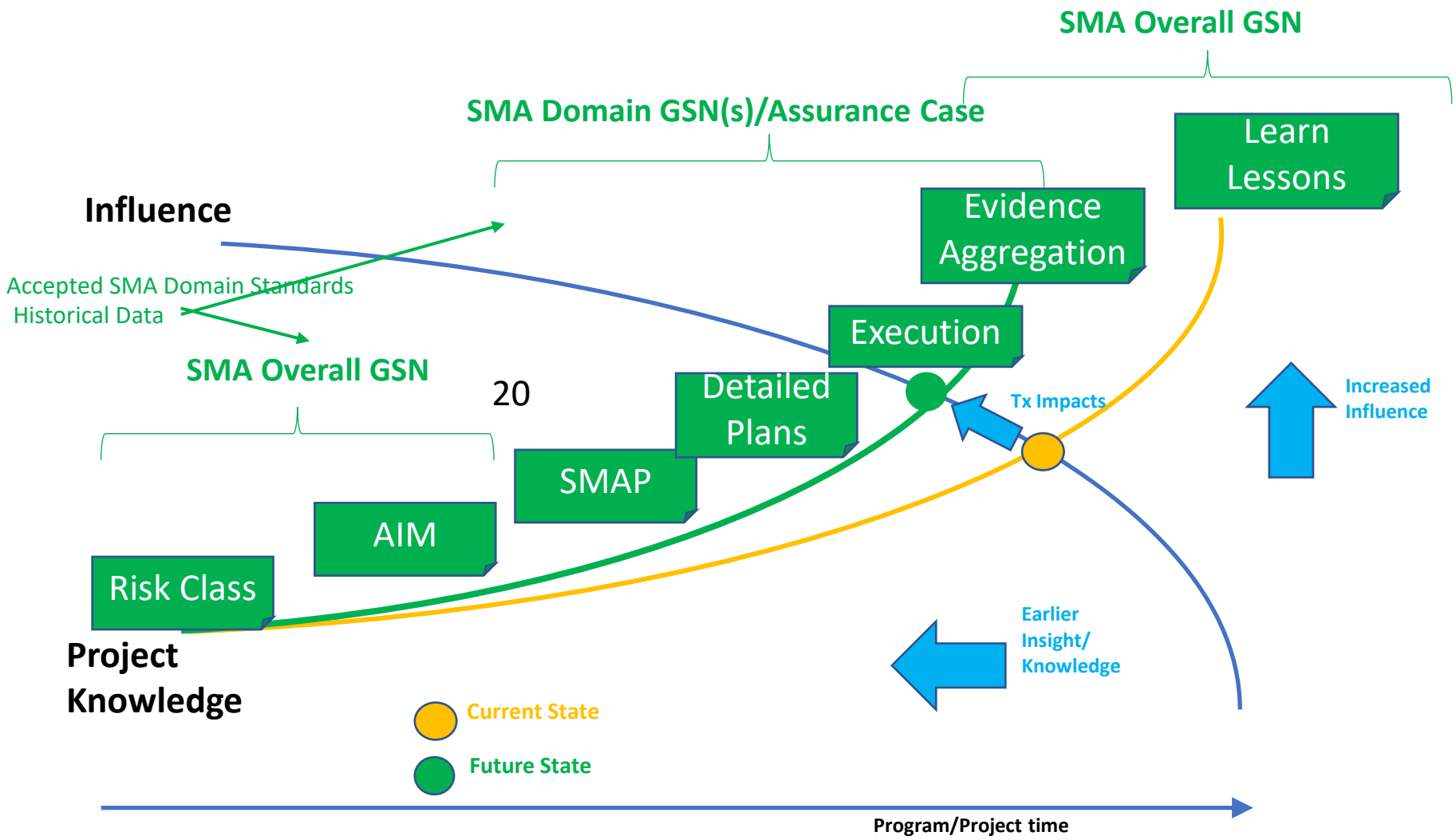
An **Assurance Case** is an organized argument that a system is acceptable for its intended use with respect to specified concerns

“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

Optimal SMA Planning – In Synch with on-going Knowledge and Influence Transformations and Impacts



Key SMA Tranformational Impacts

- Faster (Decision Velocity)
- More efficient
- More robust information
- More Trusted
- Re-Usable
- etc

Agency DT Engine

NASA's Strategic Framework & Implementation Plan outlines the following activities on an annual basis to unify and drive transformational activities

1 Ignite Transformation

Facilitate **Tx Target Community-owned Roadmaps** & near-term priority actions to align DT intent & goals across NASA

2 Connect Plans

Coordinate like **Organizational DT Plans** that respond to the DT Strategic Framework to synchronize DT intents

3 Integrate Solutions

Analyze **Integrated DT Solutions Portfolio** vs. Roadmaps / priorities for redundancies & gaps to identify leveraging opportunities & inform investment decisions by OCIO, DT & other organizations

4 Facilitate Adoption

Measure **DT Progress** on funded Org DT Plans vs. Roadmaps/Priorities; elevate & address cross-cutting barriers via **DT Catalyst Projects**; celebrate & share **DT Successes & Exemplars**

Remember, Digital Transformation is not a goal, it's a lever. A big one……To achieve Organization & NASA Goals

OSMA/ SMA

Refine "Tx Engineering's" Roadmap by integrating Digital SMA Plan with Digital Engineering's (DE) Needs, Goals, and Objectives (NGO) plan

Update & connect OSMA's Digital SMA Plan using the Agency Roadmap Manager (ARM)

Support ITSB, ITMB, DE Leadership Team, NEW DT Working Group, and NEW SMA MB to influence Investment Decisions

Lead / support DT related projects and share progress (both Agency DT and SMA funded activities)

Origins of Digital SMA

MBMA Program
- Trilateral WG
- MIAMI support
- RAMS papers
- RAAML

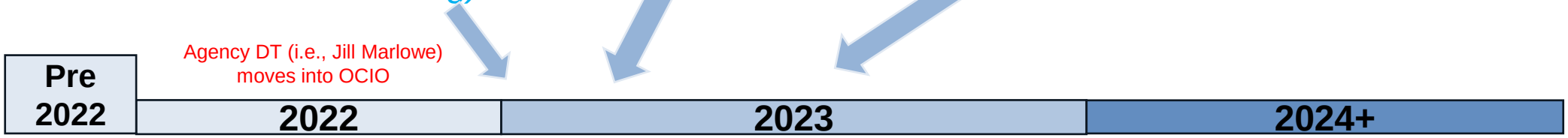
KSAO Program
- NASA-wide STAR
- NMIS
- QCARD

Agency DT ReOrg (Agency DT Strategic Framework/ARM)
4 Transformation Target Areas (Discovery, Operations, Engineering, Decision-Making)*

OSMA/OCE partnership around DE / DE Eco System

Development of OSMA's Strategic Objectives (1-8) and **Obj#8 Digital SMA Team**

NASA's Digital Transformation Initiative



Extension of MBMA into DT **(MASCD + KSAO)**
Extend beyond Reliability/ Modeling to other Disciplines/ Areas, Automated Program Plan Generator (APPG)

SMA grouped under the Digital Eng (DE) Workstream
Also includes links with Decision-Making & Ops

MBMA/ KSAO Partnership
Initial Digital SMA Planning around 8 OSMA strategies

Realignment/ Reorganization of Digital SMA-related Activities
OSMA Leadership/ SMA MB Forums

Digital SMA Partners and Activities

Summary and Notable Examples

Key Players and Activities

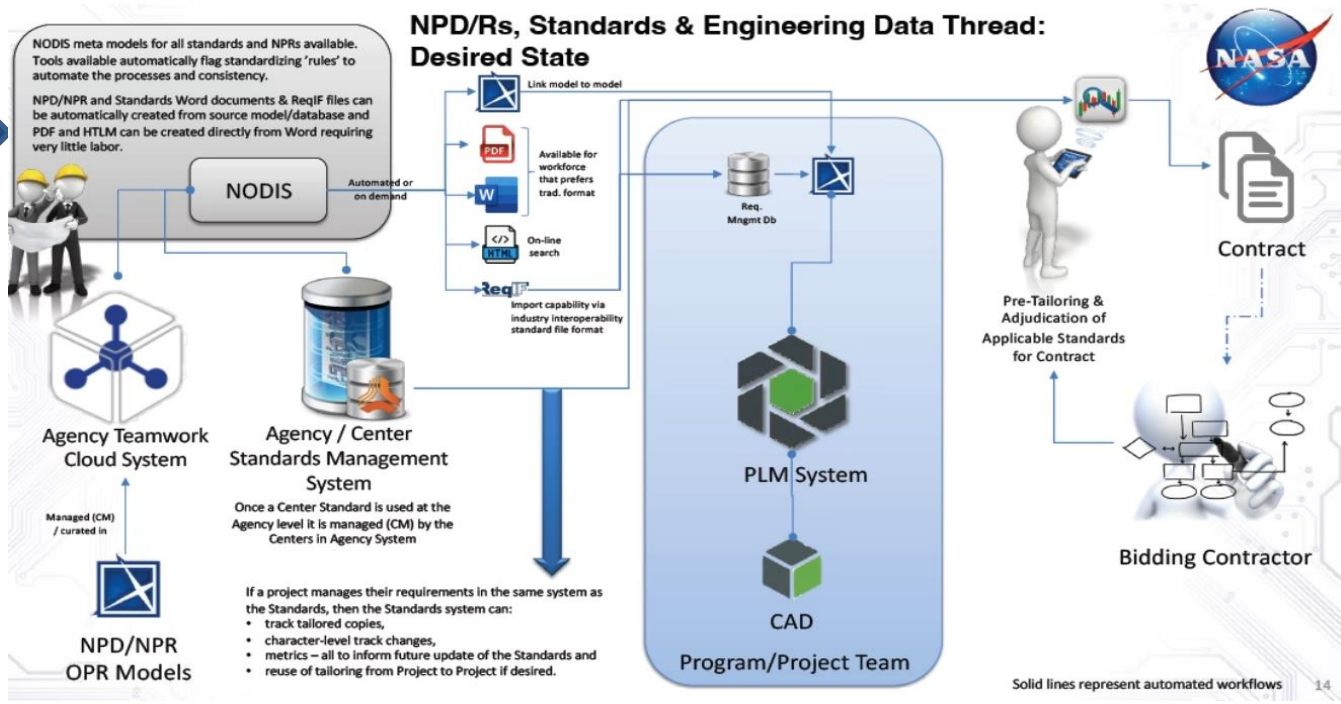
- SMA In-Kind: SMA Disciplines, SMA Policy Mgmt (~25 tasks)
- NASA Partner: OCE, OCIO, OCE, NODIS (~6 tasks)
- External Partner (~4 tasks): OUSD/DoD – Army DevCommand, etc.; SDOs – SAE, OMG, etc.,; Govt-Industry Consortiums – RAMS, FEDEF – INL, etc., Trilateral – ESA, JAXA, Universities – FL Institute of Technology, etc.: Aerospace Companies – LM, NGST, etc.
- OSMA KSAO (~6 tasks):
- OSMA MBMA (~5 tasks)

30+ tasks!

All focused on Digital SMA's Strategic Objectives

Cross-TA NPR Meta-Model Development and Machine Assisted Planning

(with OCE, OCIO, OES, NODIS, SMA Policy Management)



LEGEND

ARM *= Agency Roadmap Model*
DSO *= Digital SMA Objective*
DE *= Digital Engineering,*
DoD *= Department of Defense*
DT*= Digital Transformation*
ESA *= European Space Agency*
JAXA = *Japanese Aerospace Exploration Agency*
KSAO *= Knowledge Sharing and Analysis Office*
MBMA *= Model Based Mission Assurance*
OES *= Office Executive Secretary*
OMG *= Object Management Group*
OUSD – *Office Undersecretary of Defense*
RAMS *= Reliability and Maintainability Symposium*
SAE *= Society of Automotive Engineers*
SDO's *= Standards Development Organization*

MBMA Program Background

MBMA Overview:

It is important that SMA data, activities and products are integrated as part of the evolving MBSE and broader Digital Engineering environment, This includes integration of concepts and language, as well as integration of data, products, and processes.

Model-Based Systems Engineering (MBSE) focuses on creating and exploiting domain models as the primary means of information exchange between engineers, rather than on document-based information exchange. Domain models include both data and behavior.

Moving forward, the concepts and processes of S&MA must be accurately represented in the evolving Digital Engineering Eco System, while remaining broadly accessible by the S&MA community. Thus, the SMA activities must also address the following primary objectives:

1.Representing S&MA concepts and **information** in SysML, and
2.Providing Interfaces to MBSE tools and data therein ("lowering the barrier to entry").

Corresponding products and deliverables of this Program shall include:

- Ontologies, Shared Capabilities, and Guidance (e.g., Profiles and Model Elements)
- Views and Viewpoints, and approaches for interacting with the models as part of the broader Digital Eco System/MBSE environment.
- Papers, Pilots/Pilot effort documentation, presentations and other outreach activities
- The organization and implementation of the annual MBMA Workshop.