National Aeronautics and Space Administration

OSMA's Emerging Digital "Assurance Case" Framework

NEPP 2022

Presented by: Tony DiVenti, NASA R&M Technical Fellow

Acknowledgements: Homayoon Dezfulli, John Evans, Jeannette Plante and Frank Groen/NASA HQ; Ewen Denny & Ganesh Pai/NASA ARC and KBR; Steve Cornford, Martin Feather, and Todd Paulos/NASA JPL; Rebekah Austin and Ken LaBel/GSFC; Arthur Witulski, Nag Mahadevan, Gabor Karsai, Brian Sierawski, Robert Reed, and Ron Schrimpf/VU

www.nasa.gov

NASA

OSMA
OFFICE OF SAFETY & MISSION ASSURANCE

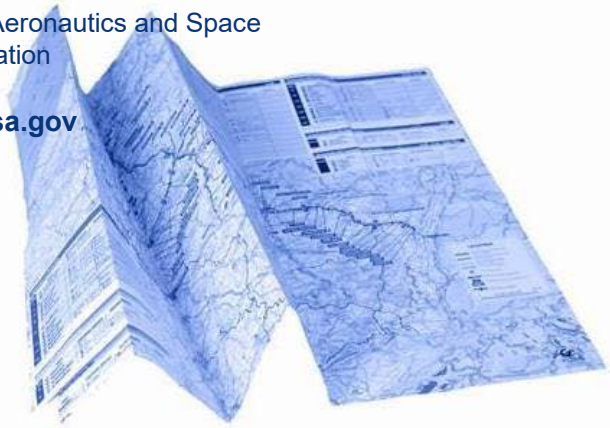
MASCD

Outline

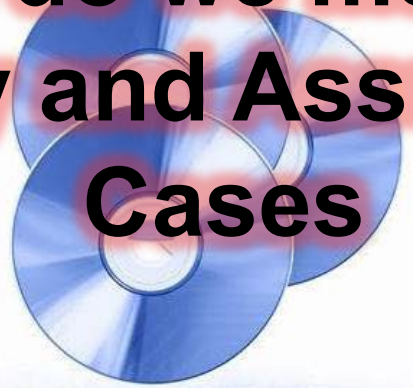
- **What do we mean by Safety and Assurance Cases**
  - Descriptions
  - Broad Adoption
  - Definitions and Shaping Concepts
  - Conceptual Illustration
- **Other NASA Building Blocks**
  - R&M GSN/Objectives Hierarchy Application
  - NASA and VU GSN Application to Radiation Assurance Case (SEAM)
  - QA Ontology Framework
  - Objectives-driven, case-assured approach, S&MS Approach
- **OSMA's Emerging Digital "Objectives Hierarchy/Assurance Case" Framework**
  - Automated Program Plan Generator (APPG)
  - Digital On-Ramp to a NASA Interoperable, Enterprise, Environment

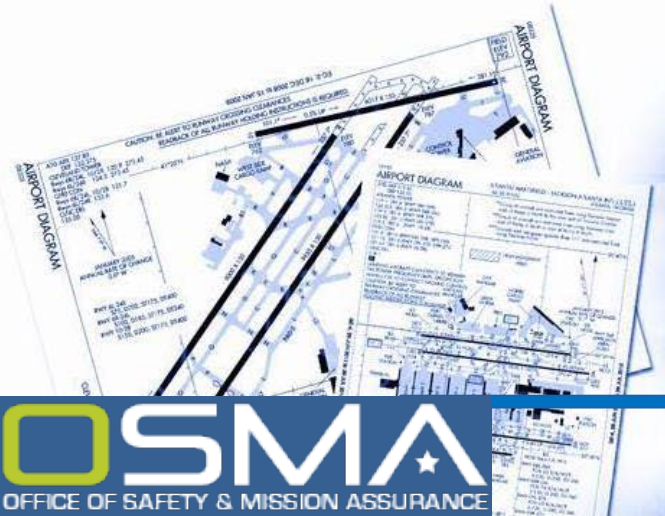
National Aeronautics and Space Administration

www.nasa.gov



What do we mean by Safety and Assurance Cases





Safety (Assurance) Case

- Comprehensive, auditable, safety risk management artifact
- Authoritative record that
  - Safety risks have been identified, are well understood
  - Processes and mechanisms in place for risk reduction
    - Driver for development
- Explicit claims and evidence connected by rationale (argumentation)
- Properties
  - Compelling, comprehensive, convincing, valid, justifiable, defensible, …

Broad Adoption

- Piper Alpha Report (Cullen Inquiry), 1990
  - Recommended application of safety cases to offshore installations
  - Subsequently adopted by UK Ministry of Defense, Def-Stan-00-56 (MOD), 2004
- Now widely used in many safety-critical industries
  - Offshore Oil & Gas (Cullen 1990), Defense, Medical, Transportation (Road, Rail and Air), Nuclear
- Defense aviation
  - Military aircraft, largely in UK and Australia
- Civil Aviation
  - By ICAO for RVSM implementation over Africa, Asia
  - EUROCONTROL
  - JARUS – UAS
- Increasing usage in the U.S.
  - FDA – infusion pumps
  - FAA – UAS operational approval
  - Nuclear Regulatory Commission
- Automotive
  - ISO 26262 Functional safety
  - ISO 21448 Safety of the intended functionality
  - UL 4600 Safety of autonomous products

Definitions and Shaping Concepts

NASA System Safety Handbook- Vol 1 (2011), (H. Dezfuli et al) – "The safety case concept has also been extended to apply to additional system attributes beyond just safety, resulting in **"Assurance Cases"** and "Dependability Cases"

Safety Case (reference Wikipedia) – A **structured argument**, supported by evidence, intended to justify that a system is acceptable safe for a specific application in a specific operating environment.

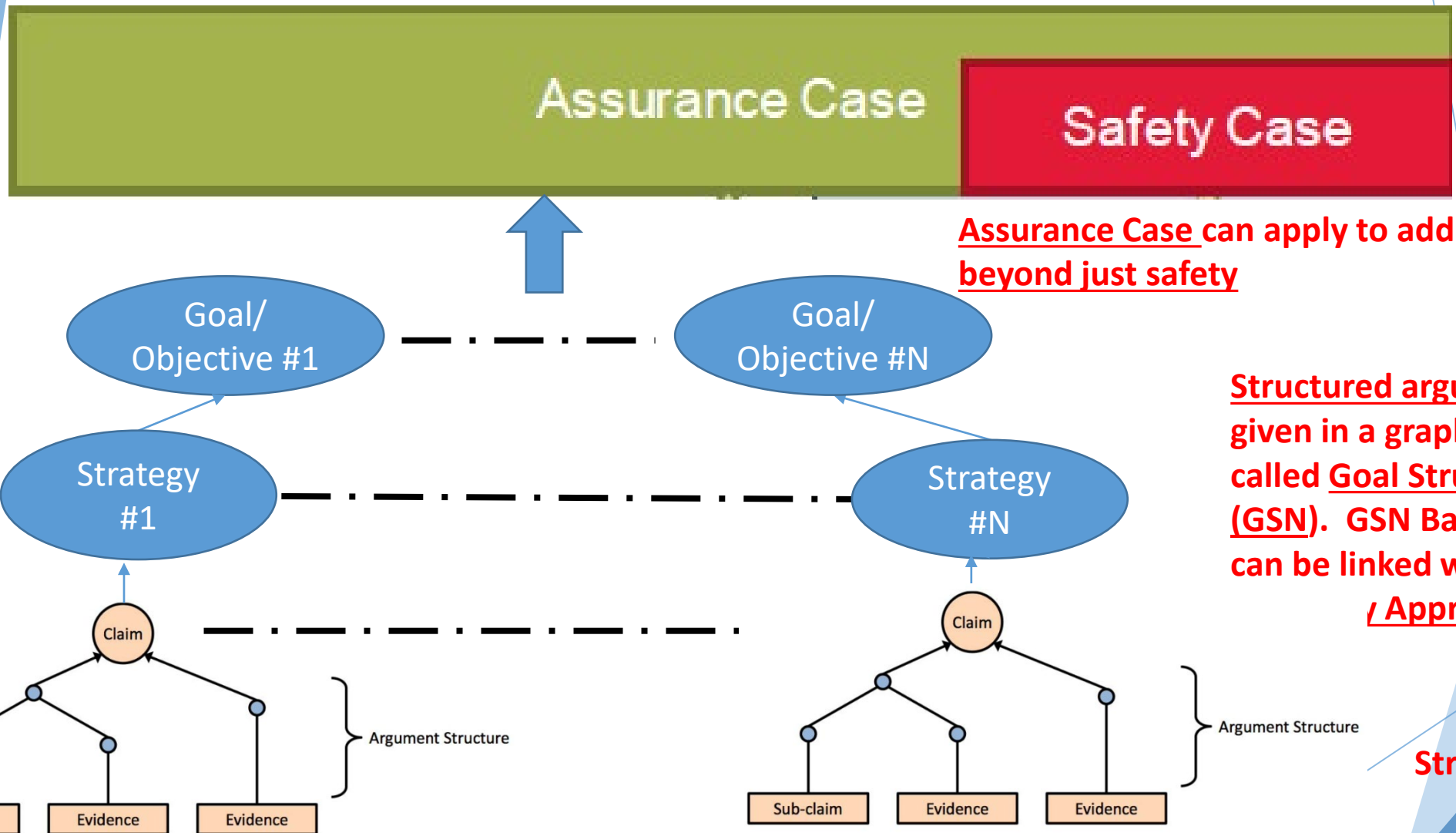
Assurance Case (reference "A Short Introduction to Assurance Cases, University of York, 2013) – A reasoned and compelling argument, supported by a body of evidence, that a *System,* Service, or organization **will operate as intended for a defined application in a defined environment.**

New Tool for Developing Safety Assurance Case Arguments (OSMA Article, 2020), (Ewen Denny and Ganesh Pai/ARC's KBR Wyle Services) –

"Traditionally, a safety case is a static thing," said Denney. "But really, what ***it should be is an active [framework]*** you use to govern your activities, so you update it when you learn more about……..the effectiveness of your mitigations and so on"

"The **structured arguments** are given in a graphical notation called ***Goal Structuring Notation (GSN)***, which has elements for capturing claims, reasoning strategies, evidence and contextual information. GSN-based arguments have close connections to the ***objective hierarchy's*** approach promulgated by NASA's Office of Safety and Mission Assurance."

Conceptual Illustration



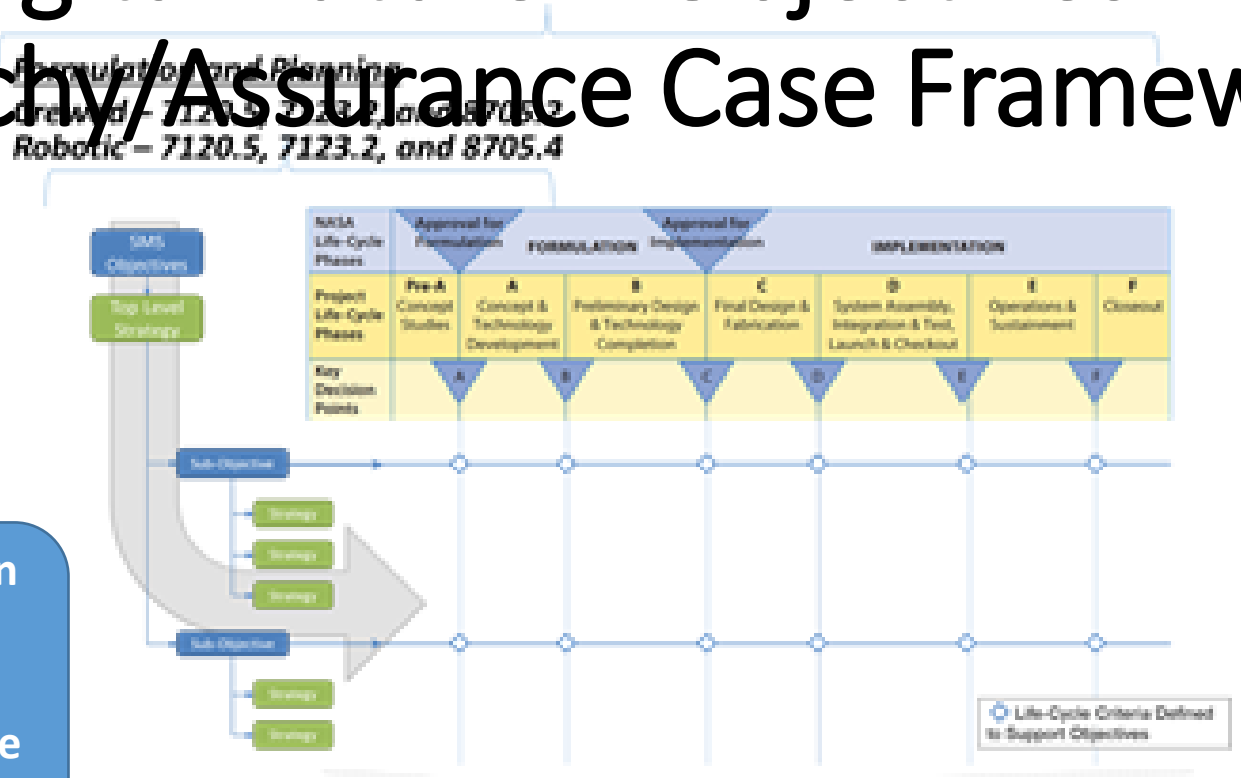
Assurance Case can apply to additional system attributes beyond just safety

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

Structured argument

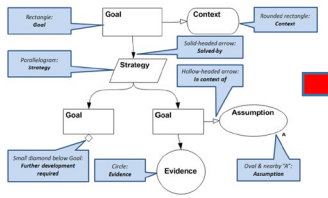
SMA Digital Future – Objectives Hierarchy/Assurance Case Framework

Objectives Hierarchy
Objective Driven Reqts & Accepted STDs

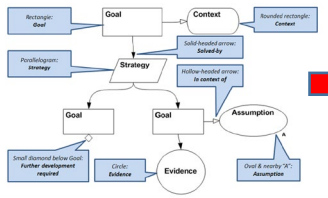


APPG AIM & SMA Plan Generation
(part of Project Plan)
INITIAL Assurance Case Argument

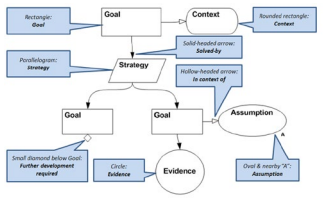
Design Assurance Case



I&T Assurance Case



Implementation Assurance Case



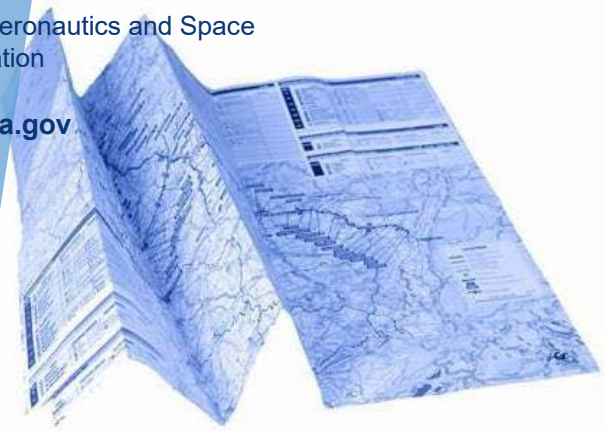
OPERATIONAL Assurance Case

Assurance Case Evolution

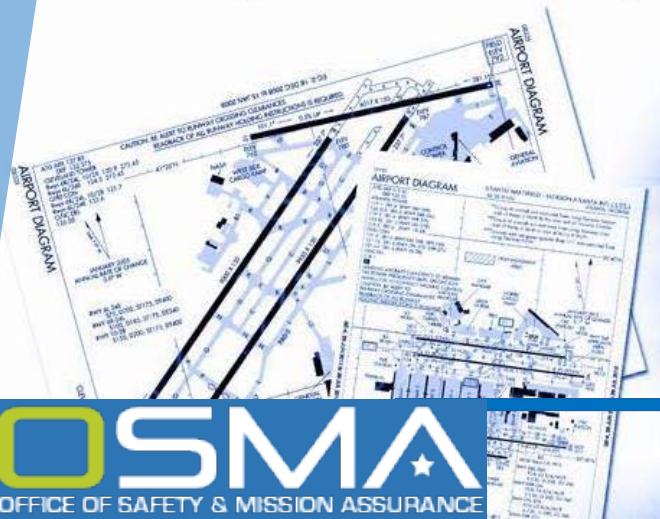
Traditionally, a Safety (Assurance) case is a static thing*, but it should be an active document *[framework]

National Aeronautics and Space Administration

www.nasa.gov



Other NASA Building Blocks that are being leveraged

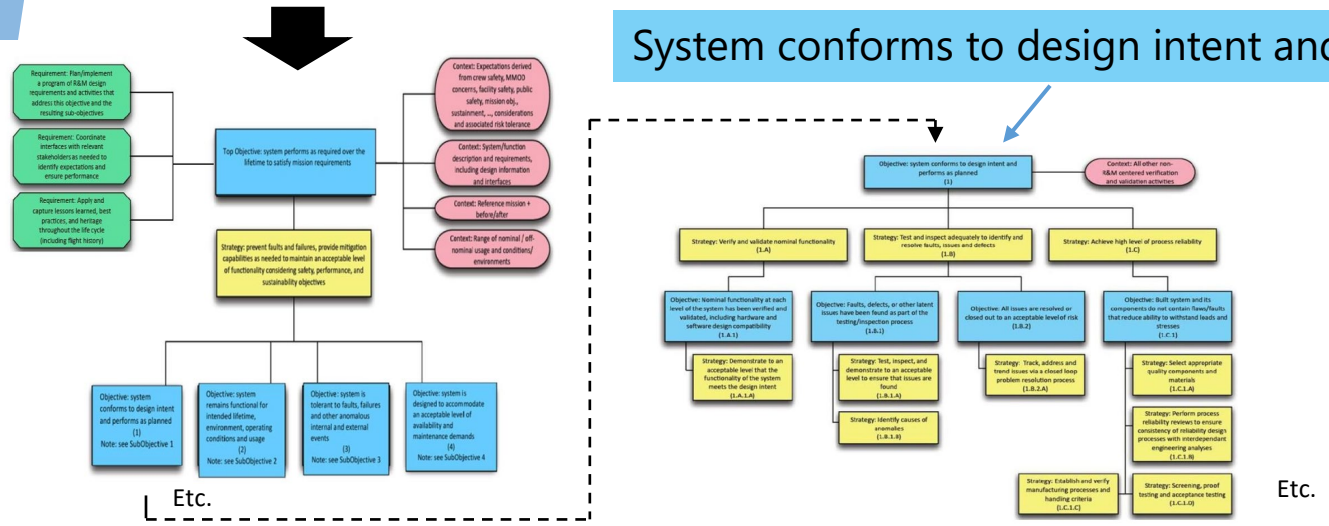


R&M Objectives Hierarchy and Assurance Cases

An **Assurance Case** is an organized argument that a system is acceptable for its intended use with respect to specified concerns (such as safety, security, correctness)[1]

(Encompasses other terms: Safety/Dependability/Security Case)

NASA-STD-8729.1A provides a Reliability and Maintainability **GSN/Objectives Hierarchy** showing the top-level concerns while systematically providing more specifics that a project will need to address to assure reliability is designed and built into systems



This hierarchy is a *starting point* for developing and/or reviewing an Assurance Case for a system's reliability

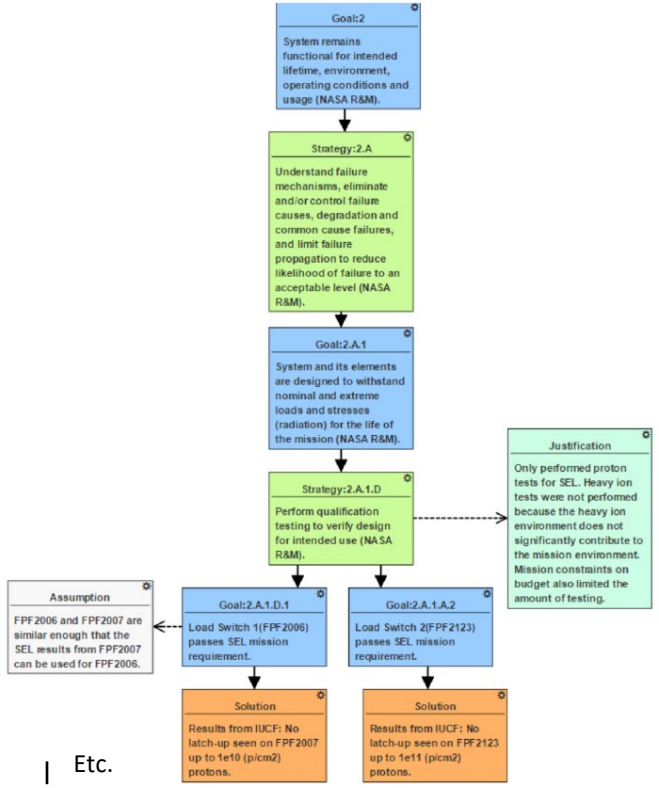
Other SMA/S&MS Objectives Hierarchy and Assurance Case Applications

Goal Structuring Notation in a Radiation Hardening Assurance Case for COTS-Based Spacecraft

Arthur Witulski, Rebekah Austin, John Evans[1], Nag Mahadevan, Gabor Karsai, Brian Sierawski, Ken LaBel[2], Robert Reed

Vanderbilt University
Institute for Space and Defense Electronics
1025 16th Av. S. Nashville, TN 37212
arthur.f.witulski@vanderbilt.edu

[1]NASA HQ, Office of Safety and Mission Assurance
[2]NASA Goddard Space Flight Center
Bldg 22, Room 050 Code 561
Greenbelt, MD 20771

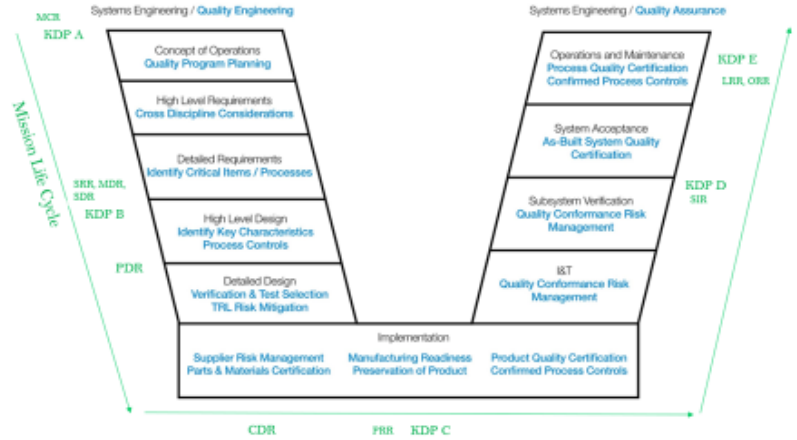


Etc.

Hardware Quality Assurance

Code	Name
QA01	**QA Program Strategy and Foundations**
QA01.1	QA Program Foundation
QA01.	
QA02	
QA03	**Quality Data Management and Records Management**
QA04	**Design for Quality**
QA04.1	Design, Construction, Verification Specifications
QA04.2	Requirements Controls
QA04.3	Design Review Considerations
QA04.4	Technical Standards baseline
QA04.5	Design Validation
QA05	**NASA Acquisitions and SCRM**
QA05.1	QMS PQA Process
QA05.2	Pre-Procurement
QA05.3	Contract Preparation
QA05.4	Crosscutting Concerns and QMS Surveillance Post Procurement
QA05.5	Quality Implementation Plan (developer)
QA06	**Production Readiness**
QA06.1	Production Readiness General
QA06.2	QMS Conformance with AS9100
QA07	**Production Quality Assurance**
QA07.1	First Party Controls
QA07.2	Second-party QA
QA08	**Integration and Test**
QA09	**NASA Product Acceptance Process and Data**
QA10	**Launch and Mission Operations**
QA11	**Risk Management**
QA11.1	Risk Management General
QA11.2	Review Boards
QA11.3	Corrective Action Request
QA11.4	Self Assessment
QA11.5	Supplier design or process change risk mitigation

Ontology → Data Structures → Data Acquisition → Data Sharing → Populating Models → Understanding the State of the System



NPR 8735.2C QA Policy Ontology *(draft)*:

- ~400 Limbs, branches, and leaves; 11 "limbs" are main QA process elements
- Designed for associating data: requirements, results, records
- NASA mission lifecycle order

Etc.

Extending Objectives Hierarchies not only to other SMA Discipline Areas, but to our Aligned Set of NPD 8700 Top Objectives

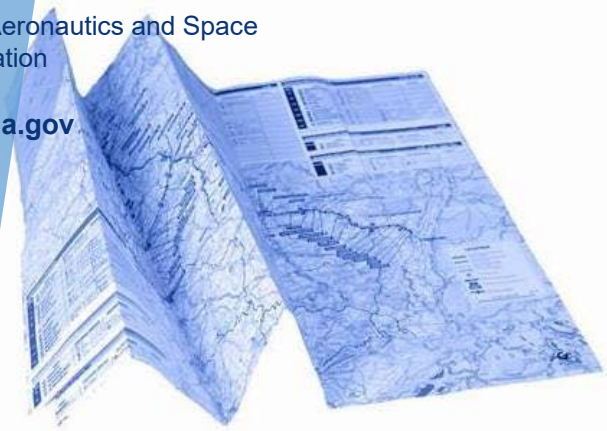
- SMA/S&MS activities have traditionally been planned and addressed via individual SMA Disciplines
- Makes these SMA/S&MS activities vulnerable to being Siloed.
- Need a Framework to begin Integrating various Discipline activities/Objective Hierarchies together around a broader SMA/S&MS Objectives Hierarchy and Assurance Case Framework.

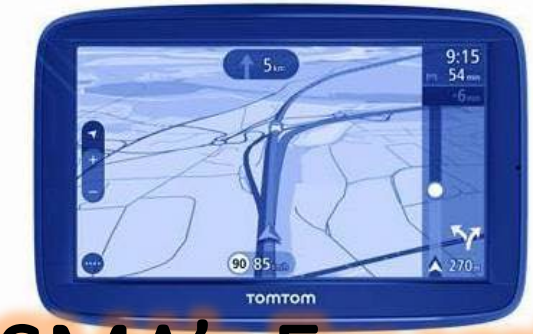
NASA SMA Disciplines

Aviation Safety	Institutional Safety	NASA Advisories and GIDEP	Range Flight Safety
Construction Safety and Fall Protection	Lifting Devices and Equipment	Nondestructive Evaluation	Reliability and Maintainability
EEE Parts	Mechanical Systems Assurance	NSRS	Risk Management
Electrical Safety	Meteoroid Environment	Nuclear Flight Safety	Safety Culture
Explosives and Pyrotechnics Safety	Metrology and Calibration	Orbital Debris	SMSR
Facility System Safety	Mishap Investigation	Payload Safety	Software Assurance and Software Safety
Fire Protection	Model-Based Mission Assurance	Planetary Protection	Supply Chain Risk Management
Human Factors		Pressure Systems	System Safety
Human Rating		Quality	Workmanship

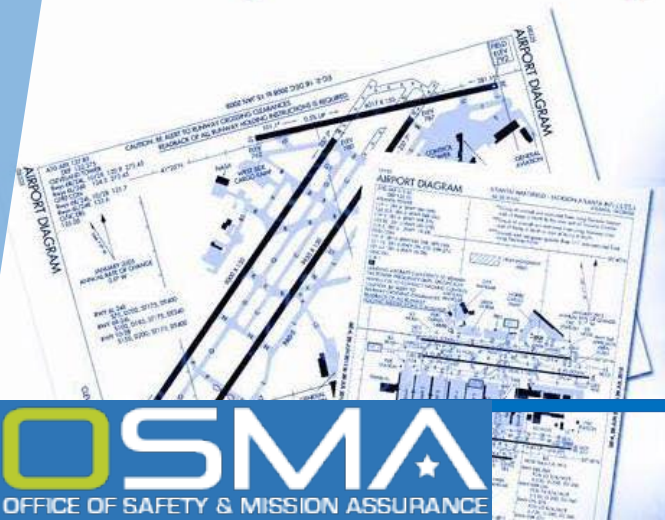
National Aeronautics and Space Administration

www.nasa.gov





OSMA's Emerging Digital Objectives Hierarchy and Assurance Case Framework



OSMA
OFFICE OF SAFETY & MISSION ASSURANCE

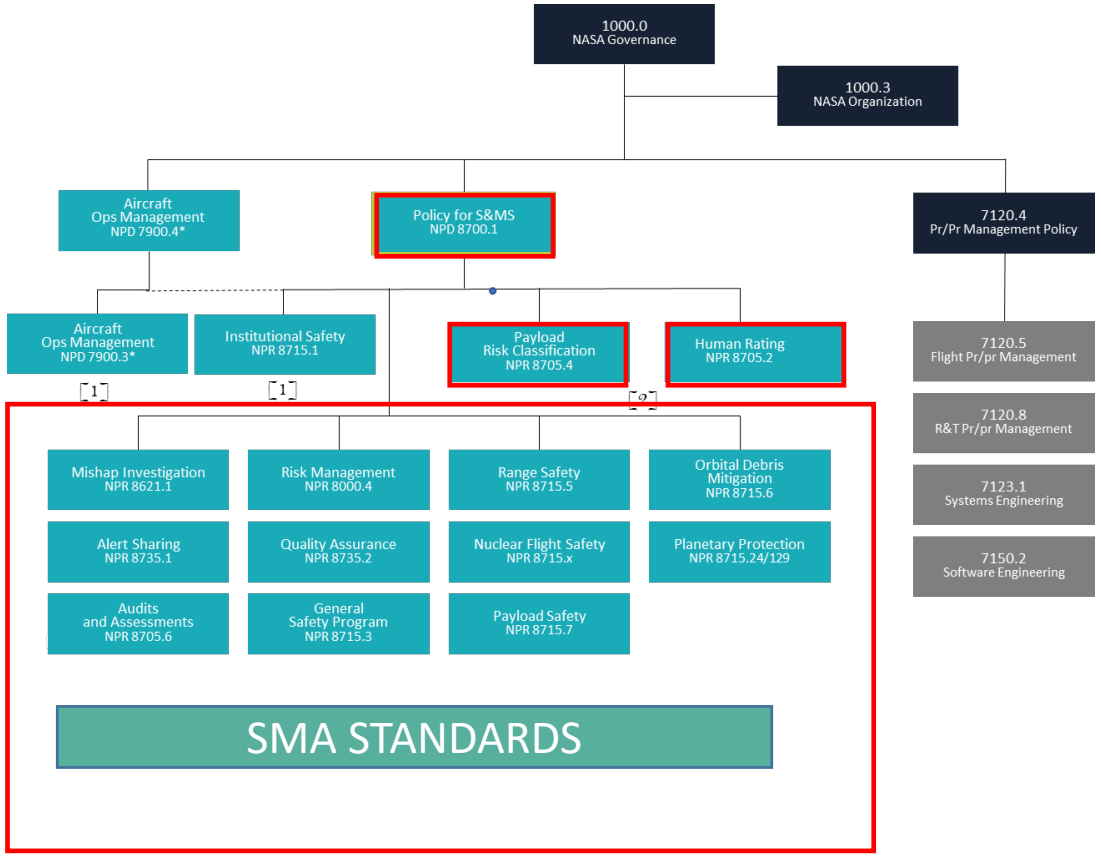
Mission Assurance Standards and Capabilities Division
OSMA HQ-GD000

MASCD

Policy Enabled - Integrated Objectives Hierarchy

On-Ramp for SMA Interoperability

SMA's Policies and STDs



SMA's Objectives Hierarchy

8700

Obj 1 Obj 2 Obj 3

8705.4 8705.2

Obj 1 ..... Obj N Obj 1 ..... Obj N

Correlating to the related SMA Discipline Areas
(e.g., 8705.4A Appendix D , NPR 8705.2, HEOMD-003, others)

Supporting STDs and NPRs

STD 1 ..... STD 2 ..... STD 3 .....STD N

Obj 1 ... Obj N Obj 1 ... Obj N Obj 1 ... Obj N Obj 1 ... Obj N

Activities and Supporting Evidence

Activity 1 .....Activity N

Automated Project Plan Generator (APPG) Engine

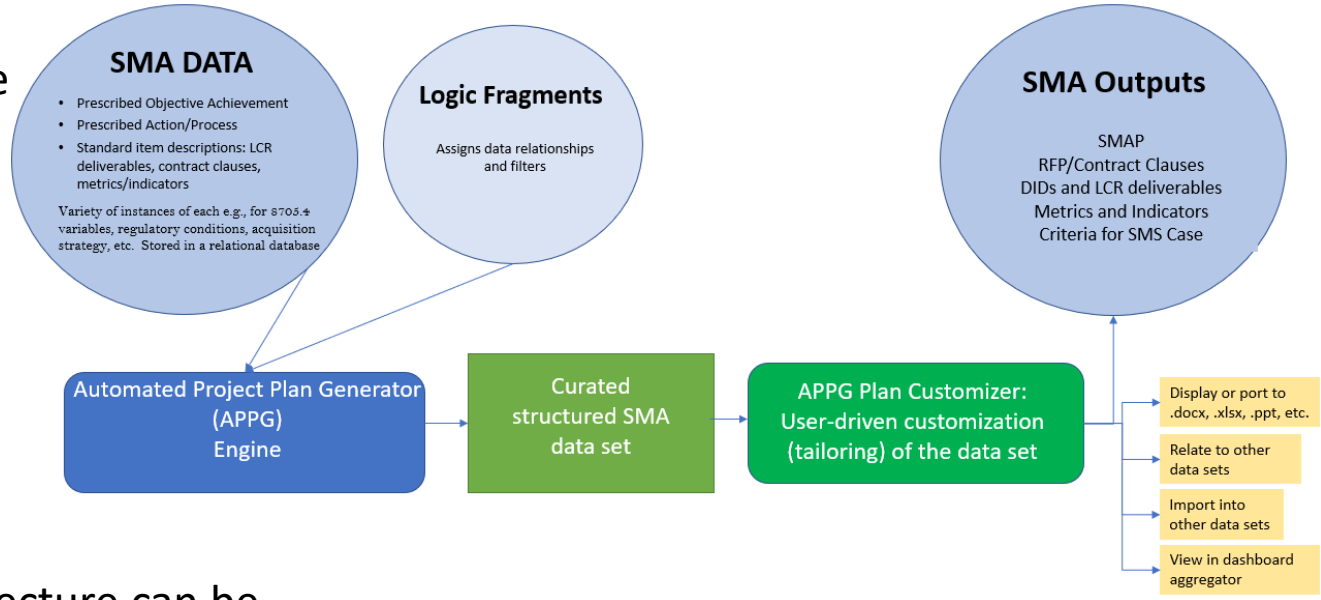
Repeatable, SME-curated, OSMA-endorsed recommendations on demand

OJT: Learn as tool is used

Project experts have direct access to editing (tailoring) capability

Project personnel only spend time tailoring, not building content from the ground up.

Authoritative Source traceable to OSMA Policy

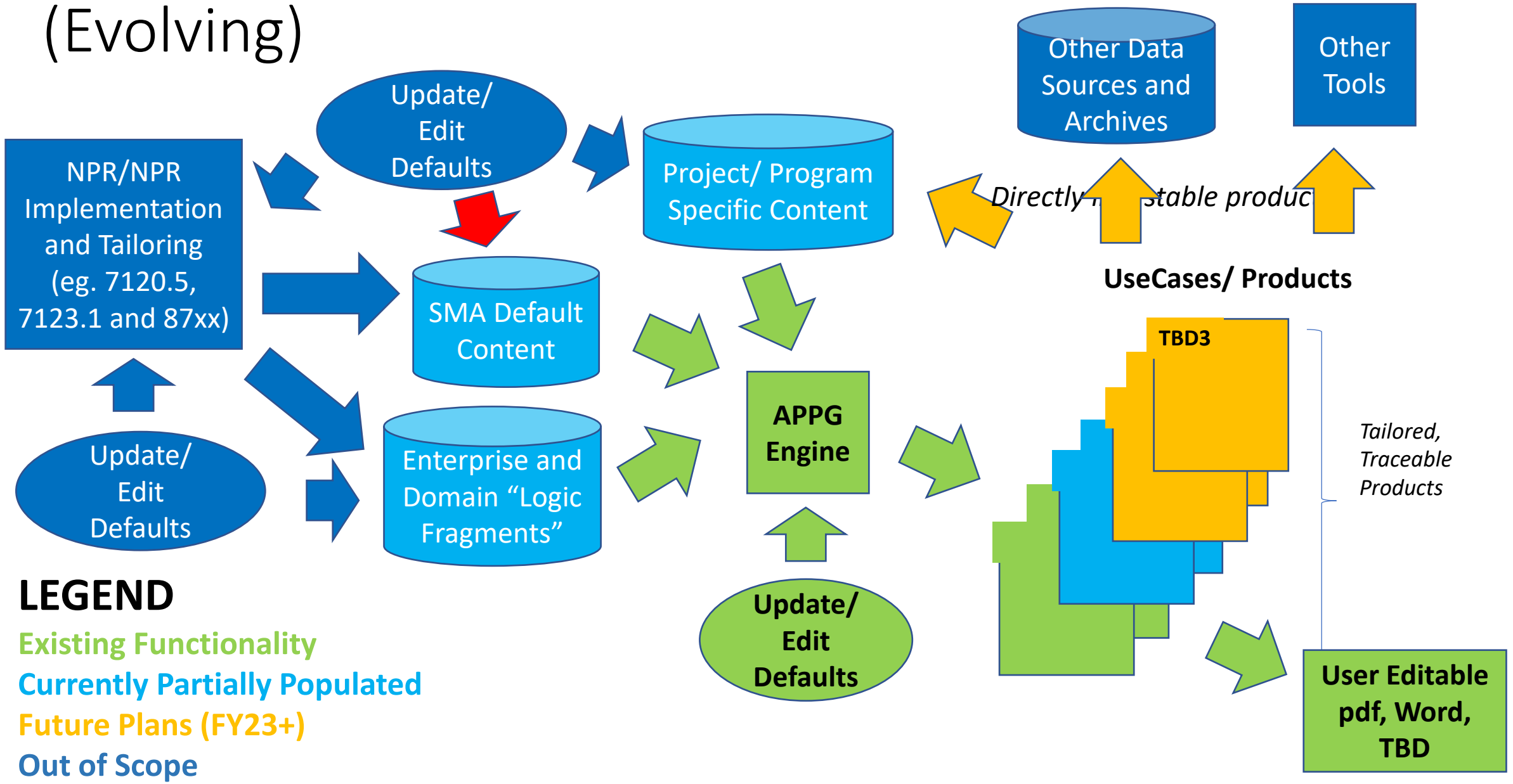


Back-end analysis of data sets for improvements, trends, risk awareness

Data architecture can be expanded over time: attach templates, related policy statement*, etc.

Content held as a data set. Can be related to other data sets and support analytics.

APPG in a larger Context (Evolving)



Assurance Case Framework: Objectives Driven Requirements, Accepted STDs, and Evidence

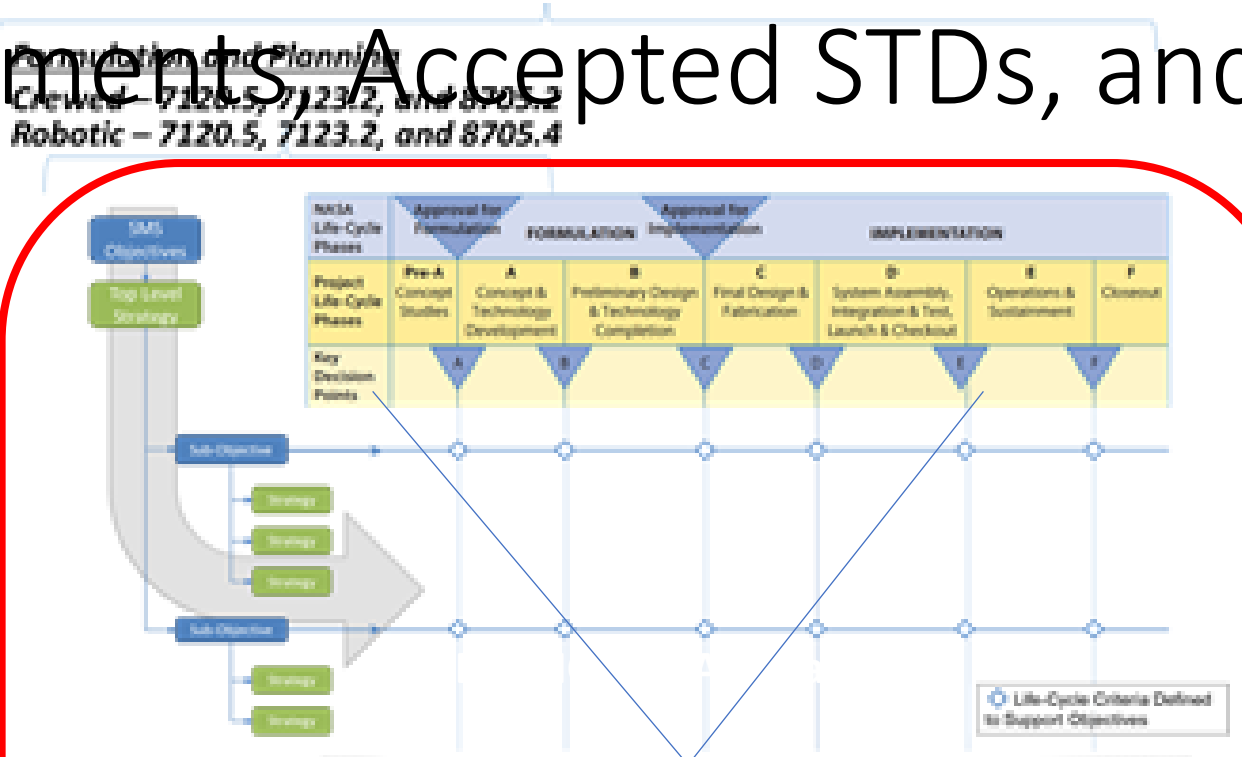
Assurance Case Framework: Objectives Driven Requirements, Accepted STDs, and Evidence

NPD 8700
Establish Top Level Objectives

NPR 8705
Establish Mid Level Objectives (AIM, SMAP)
(Mission Driven Use of Accepted STDs)

Sub NPRs / STDs
Establish Lower Level Objectives and Evidence Reqts

AIM … **xecution**



Architecting: Establish Assurance Case Framework over the entire lifecycle
(Formulation/Planning through Launch/Operations)

V&V Top Level Objectives
(vs NPD 8700)

V&V Mid Level Objectives
vs Project AIM/SMAP
(Tailored Standards Application)

Lower-level Integration and V&V
(Evidence Claims, Issues, Risks)

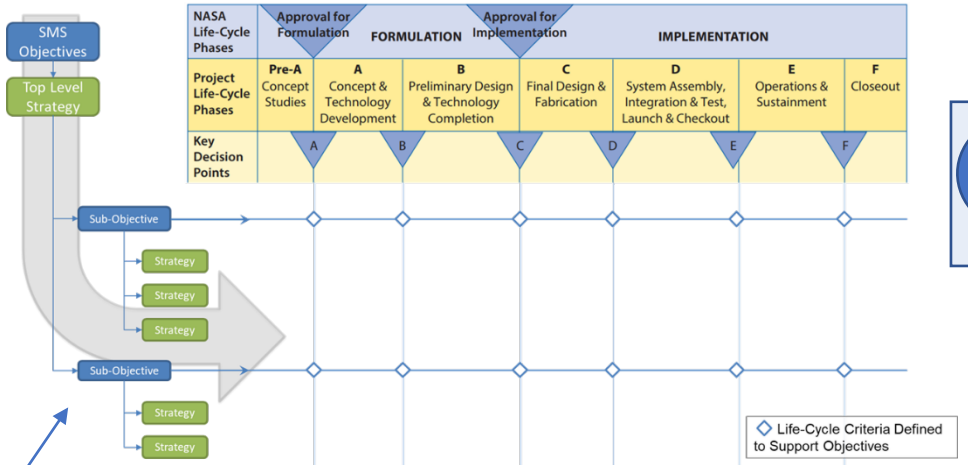
SMA's Digital Future

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

NPD 8700, NPR 8705.4, NPR 8705.2, & Accepted STDs

Objectives Driven Requirements/ Accepted STDs

Adopting SMA Directives / Standards for Greater Agility/ Effectiveness



MCR View — *CSO, IA, and LCR/KDP Reviewer Views* — FRR View

2way "Synch"!

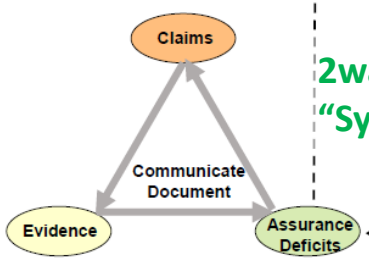
Assurance Implementation Matrix (AIM)

Project Customization Agility and Innovation

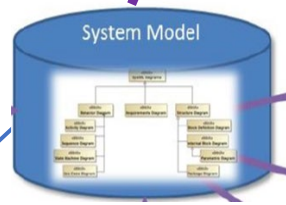
Tailorable Safety & Mission Assurance Plans (SMAP) Initial Assurance Case Argument

SMA "Assurance Case" Supported Reviews

Continuous Risk Management



2way "Synch"!



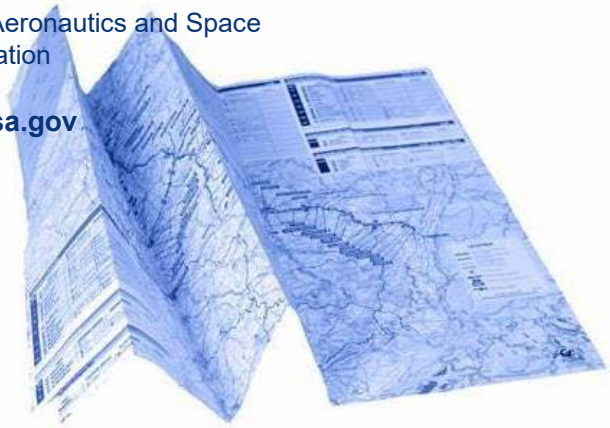
OSMA Discipline Management and Tracking Views

Safety View1

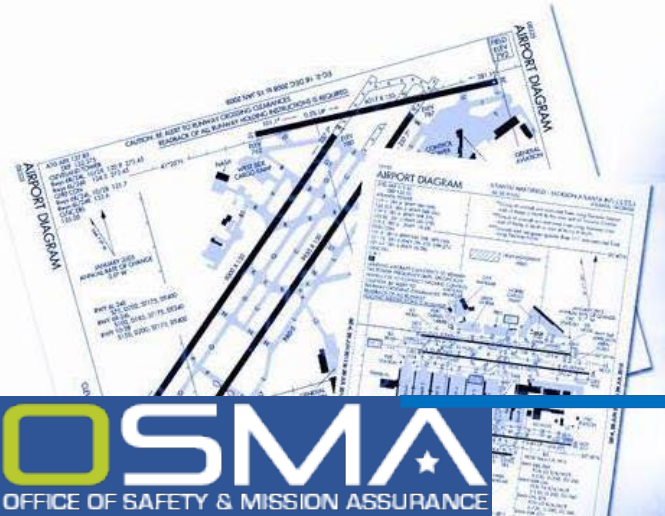
R&M View1

National Aeronautics and Space Administration

www.nasa.gov

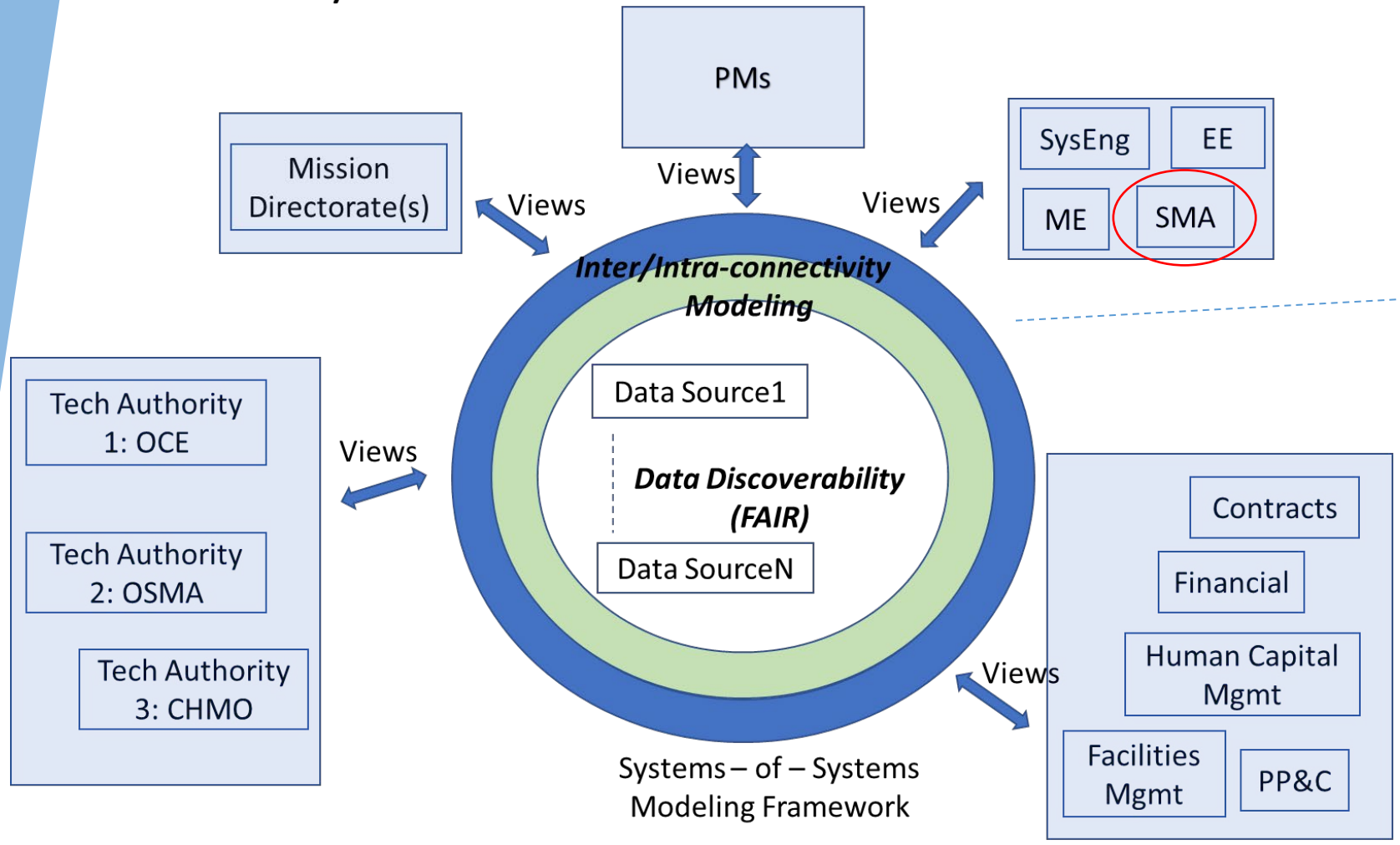


Back-Up



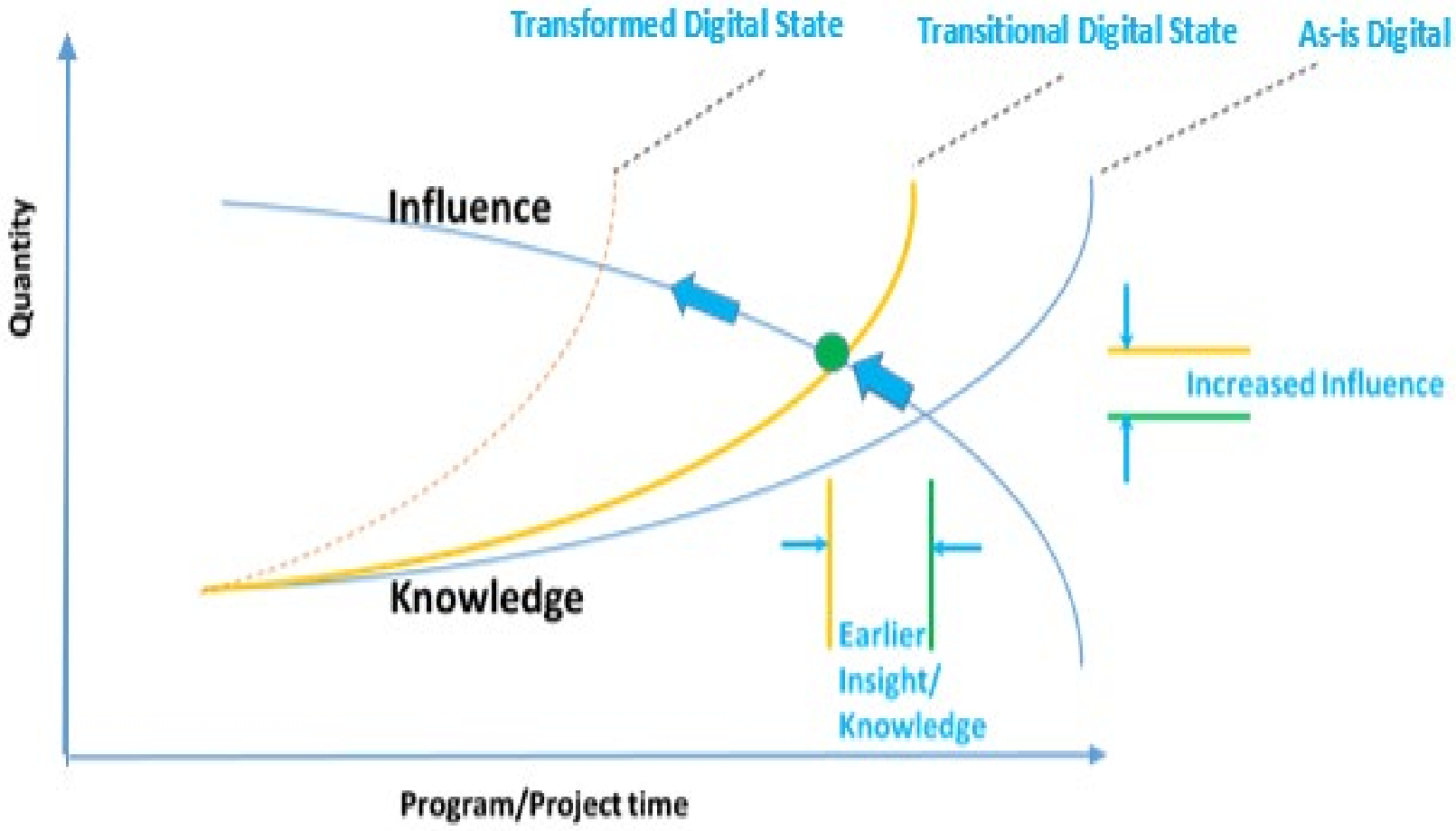
Interoperability

Everyone has a Seat at the TABLE

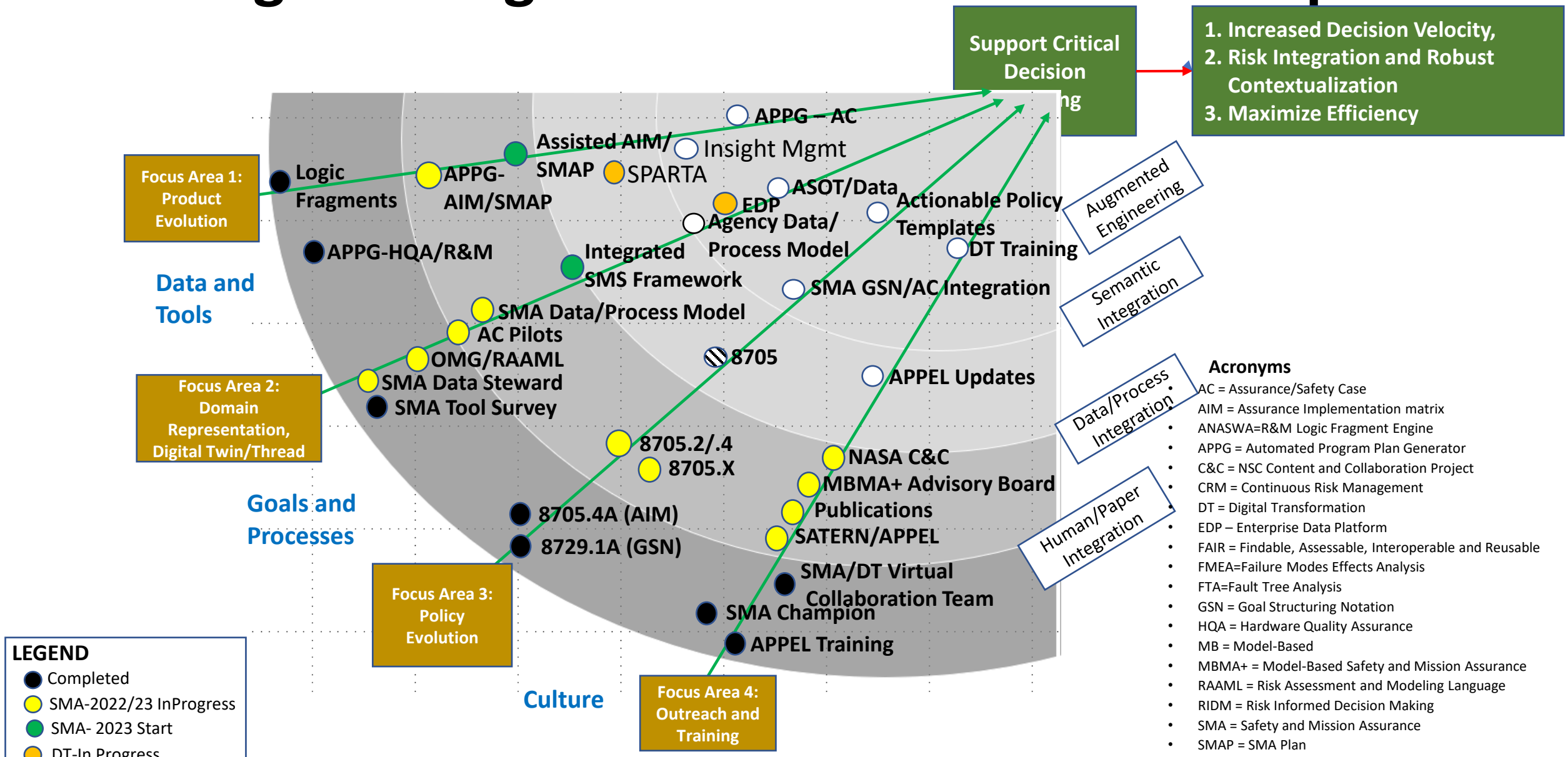


Authoritative Source of Truth

Knowledge vs Influence Curve
SMA Impact on "Critical Decision Making"



Evolving SMA Digital Transformation Roadmap



LEGEND

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

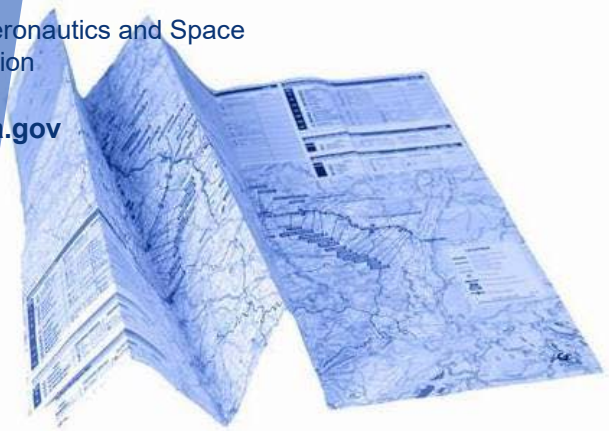
Acronyms

- 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

National Aeronautics and Space Administration

www.nasa.gov



SMA Transformational Activities and Emerging Benefits