

NASA OSMA's Emerging "Digital" Objectives-Hierarchy / Assurance Case Framework

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 Denny. "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"

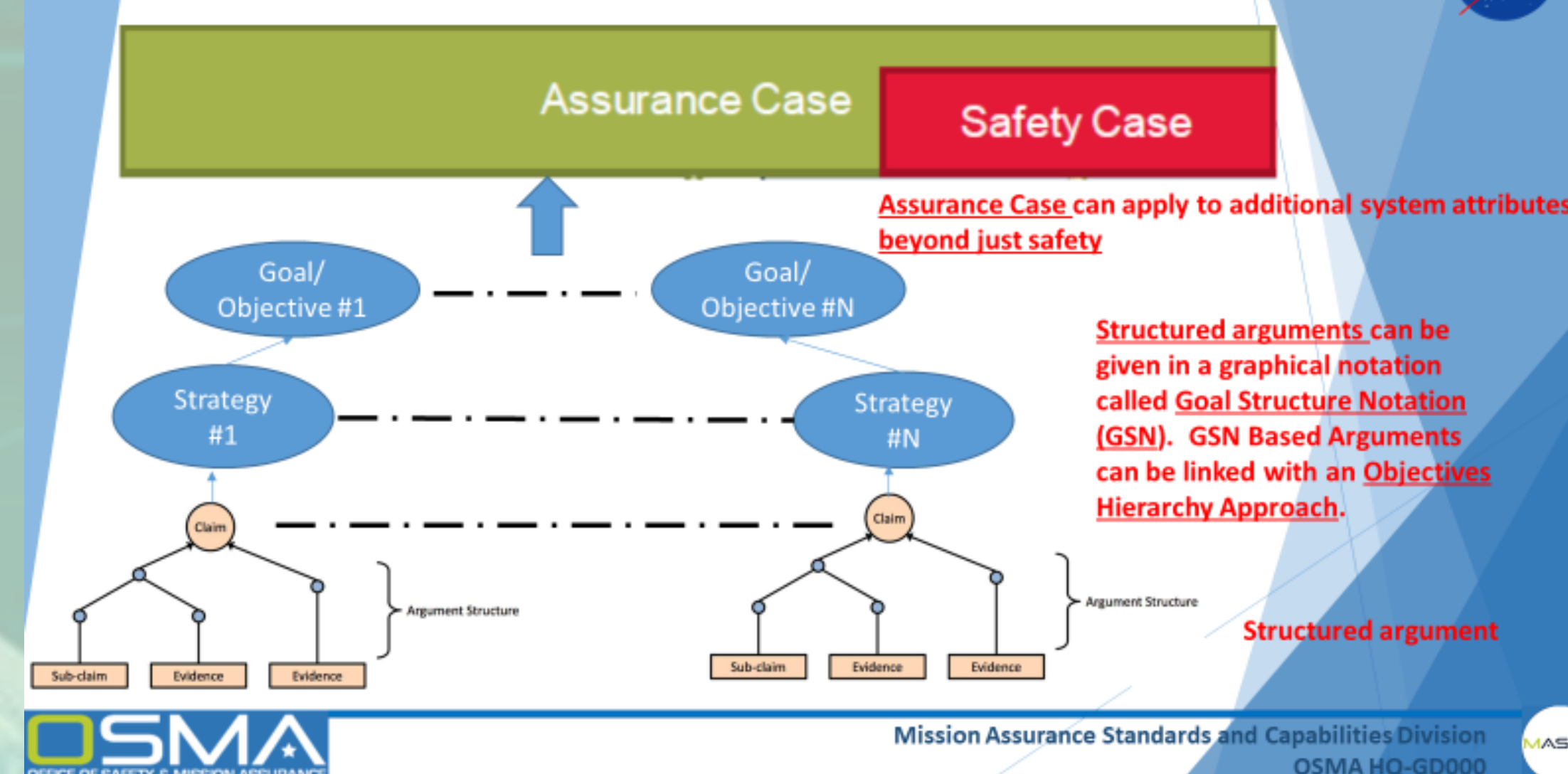
"The structured arguments are given in a graphical notation called Goal Structuring Notation (GSN) which has elements for capturing claims, reasoning strategies, evidence and contextual information. GSN-based arguments have close connections to the objective hierarchy's approach promulgated by NASA's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



Mission Assurance Standards and Capabilities Division
OSMA HQ-GD000



Conceptual Illustration



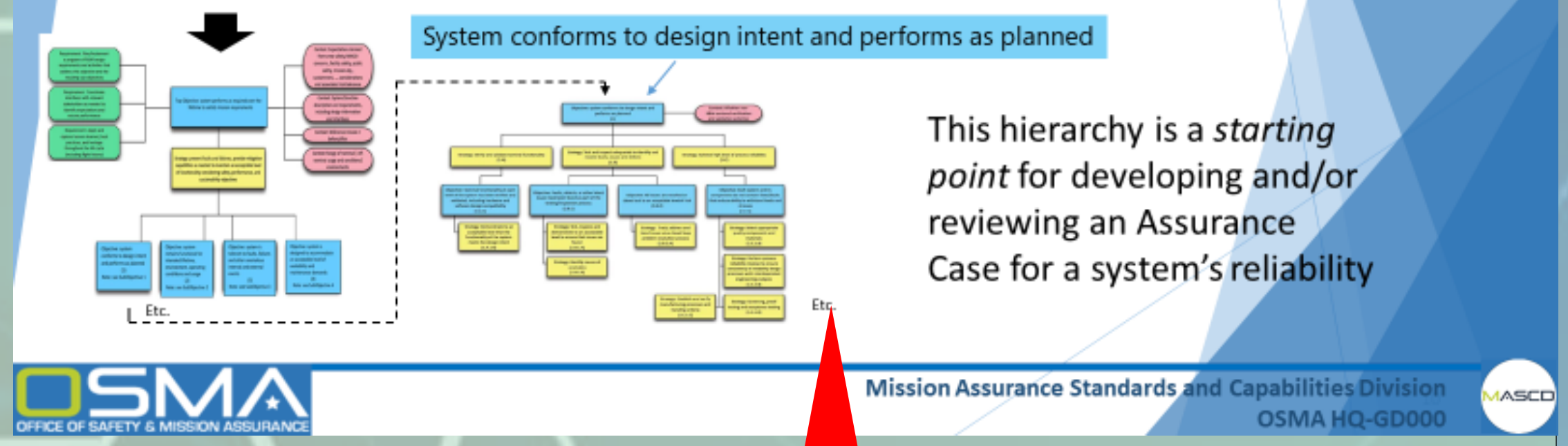
Mission Assurance Standards and Capabilities Division
OSMA HQ-GD000



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)

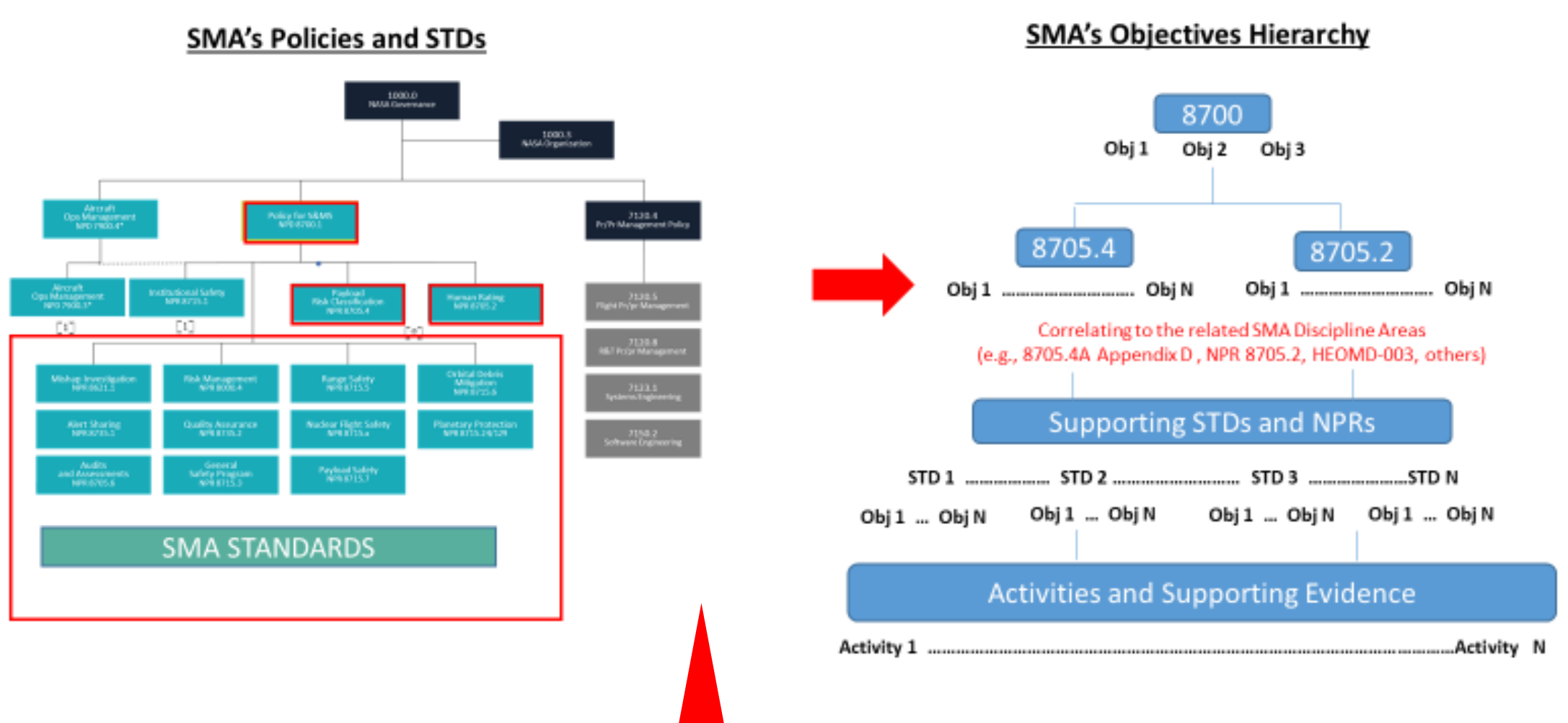
NASA-STD-8729.1A provides a Reliability and Maintainability GSN/Objectives Hierarchy showing the top-level concerns while systematically providing more specifics that a project will need to address to assure reliability is designed and built into systems



Mission Assurance Standards and Capabilities Division
OSMA HQ-GD000



Policy Enabled - Integrated Objectives Hierarchy On-Ramp for SMA Discipline Integration and Interoperability



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.

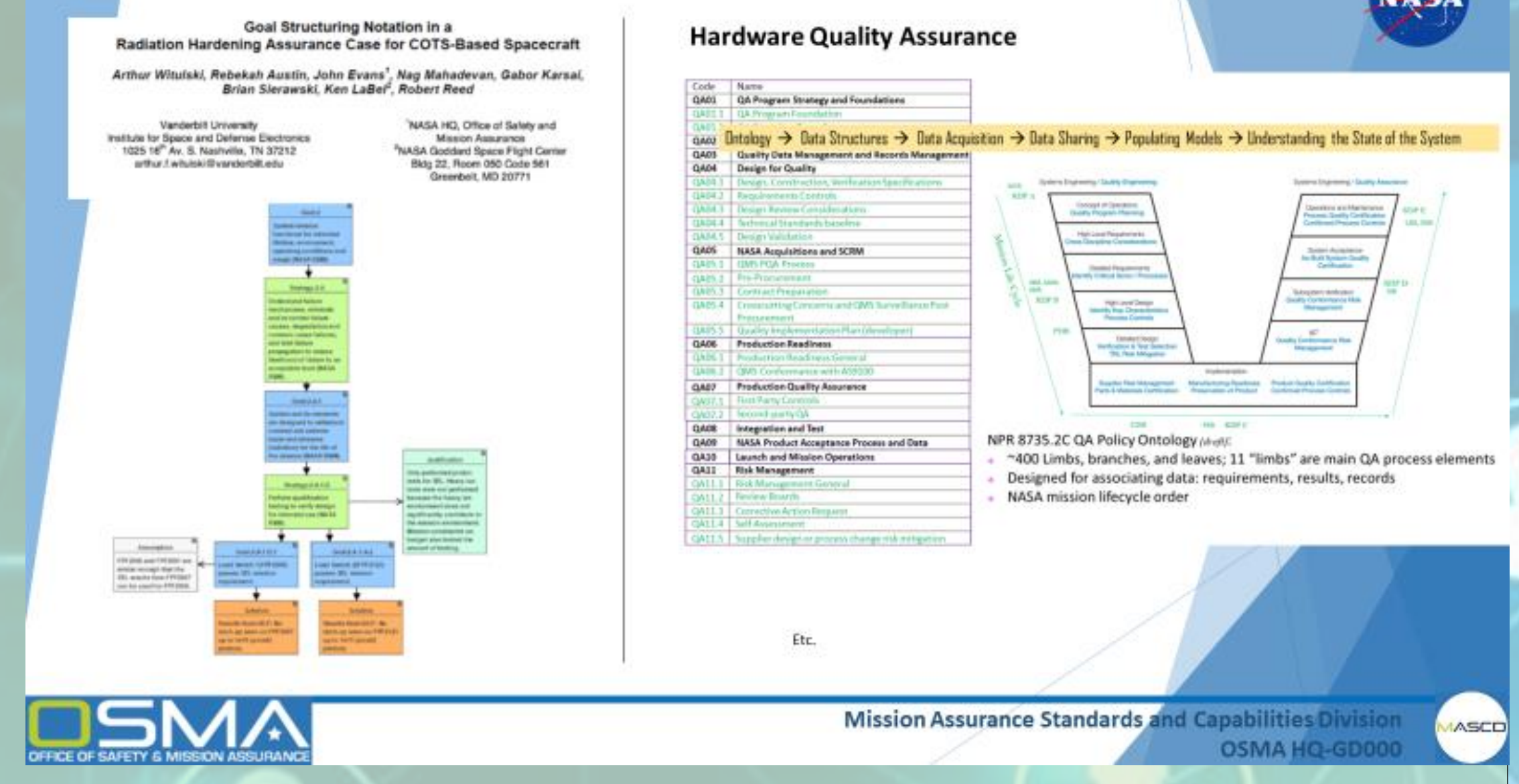
NASA SMA Disciplines			
Aviation Safety	Institutional Safety	NASA Activities and GSDP	Range Flight Safety
Construction Safety	Lifting Devices and Equipment	Reliability and Maintainability	Reliability and Maintainability
EEE Parts	Mechanical Systems	Nondestructive Evaluation	Risk Management
Electrical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



Mission Assurance Standards and Capabilities Division
OSMA HQ-GD000



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

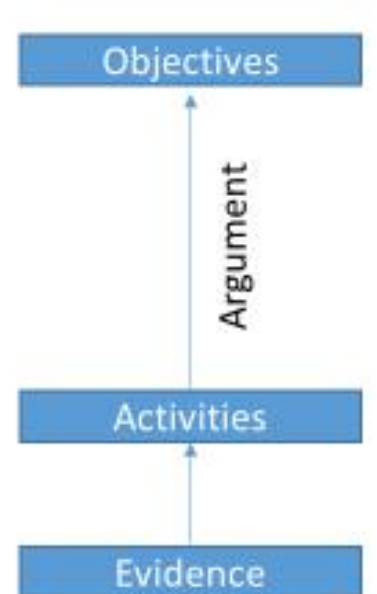


Mission Assurance Standards and Capabilities Division
OSMA HQ-GD000



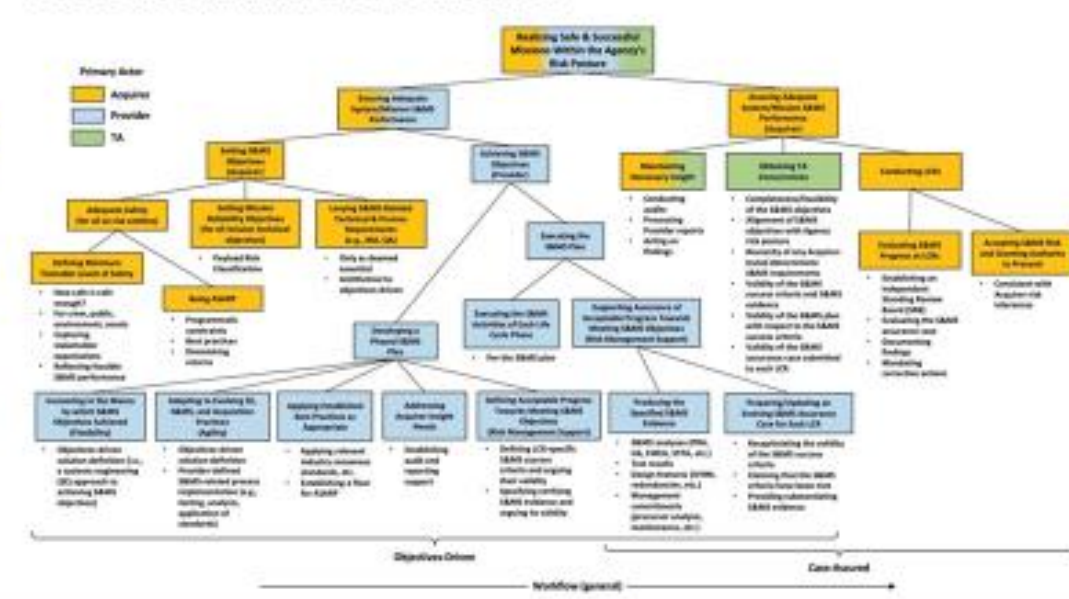
Objectives-Driven Hierarchy

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

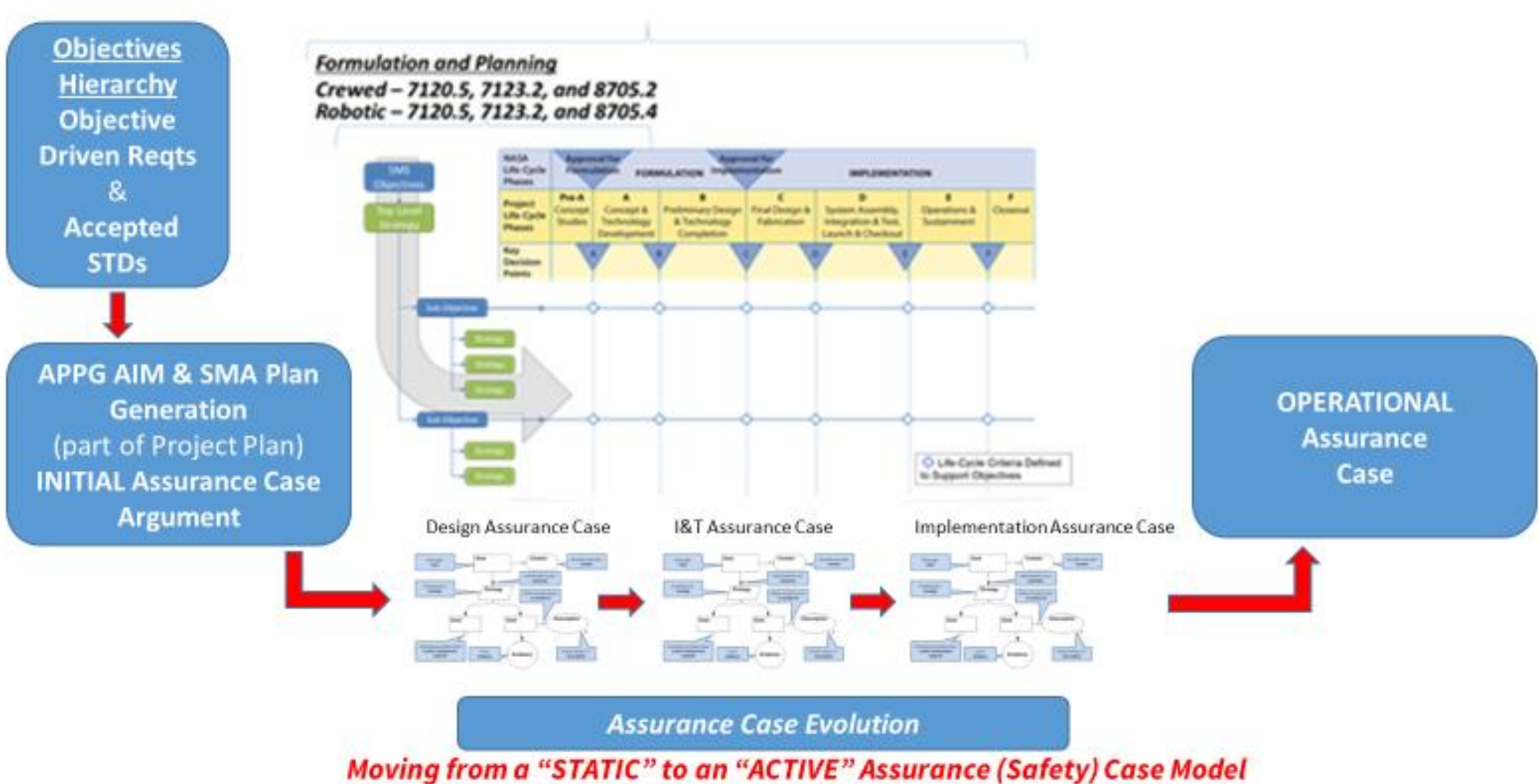
"The Nimrod Safety Case represented the best opportunity to capture the serious design flaws ... which had lain dormant for years. If the Nimrod Safety Case had been drawn up with proper skill, care, and attention, the catastrophic fire risks ..., would have been identified and dealt with, and the loss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



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

13

SMA Digital Future – Objectives Hierarchy/Assurance Case Framework



SMA's Digital Future

