THE AEROSPACE CORPORATION

The Aerospace Corporation
Civil Systems Group (CSG)

Framework for Trusted Operations of Autonomous Systems

Ronald J. Birk, Stephen R. Marley
Civil Systems Group (CSG)

February 26, 2019

Approved Material Release: OTR201900411

Framework for Trusted Operations of Autonomous Systems

An Intelligent Ecosystem Perspective

- U.S. aerospace agencies and companies employ complex systems-of-systems comprised of hardware, software, networks, and human-machine interfaces, with an increasing use of intelligent agents, artificial intelligence, and machine learning.
- Complex systems-of-systems are continually evolving as “intelligent ecosystems” to meet new operational demands and the environments they operate in are subject to dynamic external influences.
- Ensuring effective and safe operations of autonomous systems affecting lives and property **requires a framework for verification and validation** of system state-of-health and end-to-end enterprise effectiveness.
- By integrating continual state-of-health monitoring, learned system behavior, and modeling impacts of the range of potential intelligent system changes coupled with the system’s evolving operational environment, it is possible to detect anomalous behavior, predict impacts and plan for fail-safes.

Intelligent Ecosystem: distributed, adaptive, scalable, system of systems with properties of self-organization, self-sustainment, and self-evolution.

Key Areas for Trusted Space Ground Systems

All areas require verification and validation to establish trust

- **Space Operations:** Effective detection and response of anomalies must evolve with the systems, operational environments, and actors involved.
- **Mission Tasking and Resource Management:** Adaptive, efficient, and time-responsive space constellation resource tasking drive needs for intelligent systems and machine learning.
- **Mission Data Processing:** Decision-able information for space system operations involves processing extremely large volumes of dynamic data enabled by intelligent mining and multi-INT fusion.
- **Space Enterprise Management:** Governance of the enterprise, comprised of producers and consumers, of space systems benefits from intelligent systems, artificial intelligence, and machine learning. These technologies are applied as
  - *Artificial Intelligence for Mission Assurance – artificial intelligence and machine learning are applied to conduct verification and validation of space systems*
  - *Mission Assurance for Artificial Intelligence – mission assurance verification and validation are applied to establish trusted smart AI and autonomous systems*

Needs for Trusted Operations affect all aspects of Space Systems

Intelligent Ecosystems - Global Exploration Roadmap

Evolving Space Ecosystems anticipate increasing Autonomy

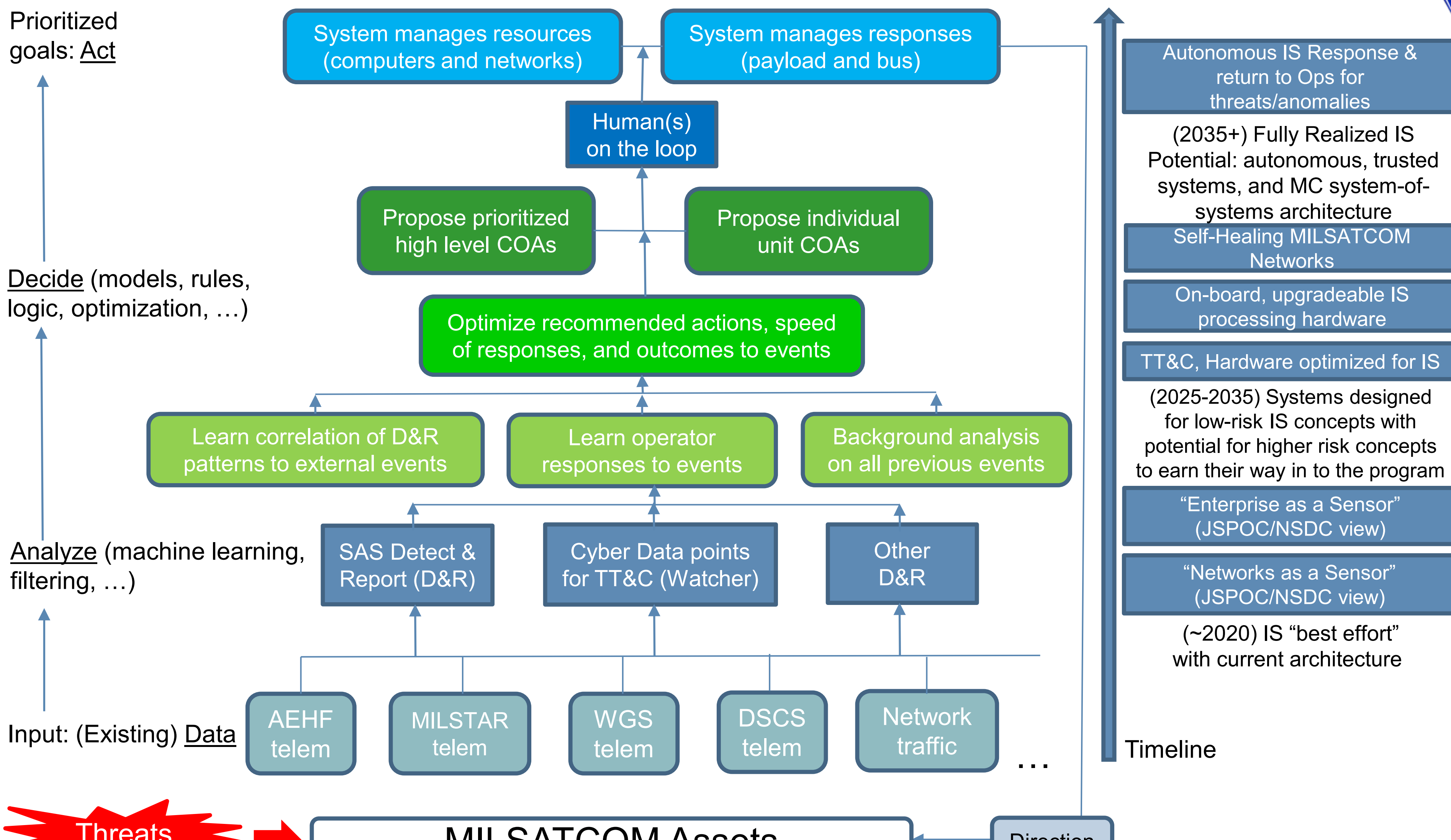
Global Exploration Roadmap Critical Technologies (Summary Table)	Today ISS & Spaceflight Heritage	Near-Future Moon Vicinity/Surface	Future Mars Vicinity/Surface
Propulsion, Landing, Return			
In-Space Cryogenic Acquisition & Propellant Storage	Spacecraft: CPST/eCryo demo	u-G vapor free liquid tank to propulsion transfer, Efficient low-power LOx & H_2 storage >1 Yr (Mars)	
Liquid Oxygen/Methane Cryogenic Propulsion		Throttleable Regen Cooled Engine for Landing (Lunar Scale)	Throttleable Regen Cooled Engine for Landing (Mars Scale)
Mars Entry, Descent, and Landing (EDL)	Spacecraft: MSL class (~900 kg)	Demonstration of advanced technology in deep space environment	Large Robotics >1000 kg; Human ~40,000 kg
Precision Landing & Hazard Avoidance	Spacecraft: Lunar & Mars Landers State-of-the-Art	~100 m accuracy, 10's cm hazard recognition, Support all lighting conditions	
Robust Ablative Heat Shield Thermal Protection	Spacecraft: Orion Heatshield test flight (EFT-1)	~1000 W/cm2 under 1.0 atmospheric pressure	~2,500 W/cm2 under 0.8 atmospheric pressure
Electric Propulsion & Power Processing	Spacecraft: 2.5 kW thruster (Dawn)	~10 kW per thruster, High Isp (2000 s) (for some mission options)	~30-50 kW per thruster (for some mission options)
Mid & High Class Solar Arrays	ISS: 7.5 kW/Panel	High Strength/Stiffness Deployable, 10-100 kW Class (for some mission options)	Autonomously Deployable, 300+kW Class (for some mission options)
Autonomous Systems			
Autonomous Vehicle System Management	ISS: Limited On-Board Mgmt functions, < 5 s comm delay	On-Board Systems Mgmt functions (handles > 5 s comm delay)	On-Board Systems Mgmt functions (handles > 40 min comm delay)
AR&D, Proximity Operations, Target Relative Navigation	ISS: Autonomous docking	High-reliability, All-lighting conditions, Loiter w/ zero relative velocity	
Beyond-LEO Crew Autonomy	ISS: Limited Autonomy	Automate 90% of nominal ops Tools for crew real-time off-nom decisions	
Life Support			
Enhanced Reliability Life Support	ISS: MTBF <10 E-6, Monitored/operated by GC	More robust & reliable components (eliminate dependence on Earth supply logistics) Increased systems autonomy, failure detection capabilities, and in-flight repairability	
Closed-Loop Life Support	ISS: 42% O_2 Recovery from CO_2, 90% H_2O Recovery	Demonstration of advanced technology in deep space environment	O_2/CO_2 Loop closure; H_2O Recovery further closure; Solid Waste, reduce volume/storage
In-Flight Environmental Monitoring	ISS: Samples to Earth	On-Board Analysis for Air, Water, Contaminants	

Source: https://www.nasa.gov/sites/default/files/atoms/files/ger_2018_small_mobile.pdf

Segment of GER critical technologies roadmap highlighting Autonomous Systems (Source ISECG)

MILSATCOM Intelligent System (IS) Vision

Increasing use of AI and ML to accelerate Decision Support



Threat Vectors for Intelligent Ecosystems

Unintended Changes in System Performance

Table 1. Threat Vectors for Intelligent Ecosystems

Threat Vectors	Description
Cyber Attacks	Malicious efforts to subvert a system through software malware or intrusion to command and control a system
Orbital Debris and Collisions	Impacts of satellite debris and micro-meteorites colliding with spacecraft
Space Weather Impacts	Energetic particles from solar flares and coronal mass ejections impinging on space systems affecting electronics
Human Error	Errant commands, programming glitches, design or manufacturing flaws
Sensor Degradation	Change in sensor monitoring characteristics and performance over time affecting measurements and resulting actions
Component Failure	Failures caused by age, excess temperature, excess current or voltage, ionizing radiation, mechanical shock, stress or impact, operating cycle, and many other causes
Radio Interference	Intentional or unintentional impact to system performance resulting from insufficient spectrum management
Unintended Intelligent System Actions	Unintended changes in system performance and actions over time resulting from artificial intelligence and/or machine-learning evolution

Threat Vector: Means of attacking or degrading system performance or quality of operations

Importance of Trust

Concepts from Discussions with Customer, Academia & Industry

- Key Themes for Trusted Systems affecting Lives and Property
  - Trust is essential for rapidly emerging Artificial Intelligence (AI) solutions to be deployed with confidence. This is more a psychological and qualitative descriptor than an established numeric or quantitative value
    - Trust through AI capabilities – AI for MA and MA for AI
    - Trust through vulnerability assessments and resilience to adversarial AI
    - Trust through test & evaluation and formal methodologies
    - Trust through modeling and simulation (e.g. game theory) of future states
  - Need for a verification and validation (V&V) test range available in some form of a facility, network, and/or environment to evaluate smart autonomous and AI systems and capabilities to establish trust
  - A near term approach is to develop and benchmark a framework for V&V of smart AI based on operational use cases

V&V is Essential to Establishing User Trust in AI/ML

Aerospace Use Cases for AI

AI applied for mission assurance at the speed of need

- Launch verification—Aerospace applies AI to assist in identifying anomalous behavior assessing increasing volumes and variety of data in run-up to launch
- Space systems operational readiness—Aerospace applies AI to assist in identifying anomalous behavior during readiness reviews for spacecraft operations
- Cybersecurity—Aerospace applies AI to handle the copious amounts of data associated with running cyber security scans in real time
- Constellations – Aerospace applies AI-based tools to conduct to detect and report anomalies for satellite communication constellations to provide decision support forecasting performance for mission assurance

Optimizing benefits of increasing volumes and variety of data for verification of operational readiness

Framework for Verification and Validation

Ensuring innovative solutions provide reliable mission assurance

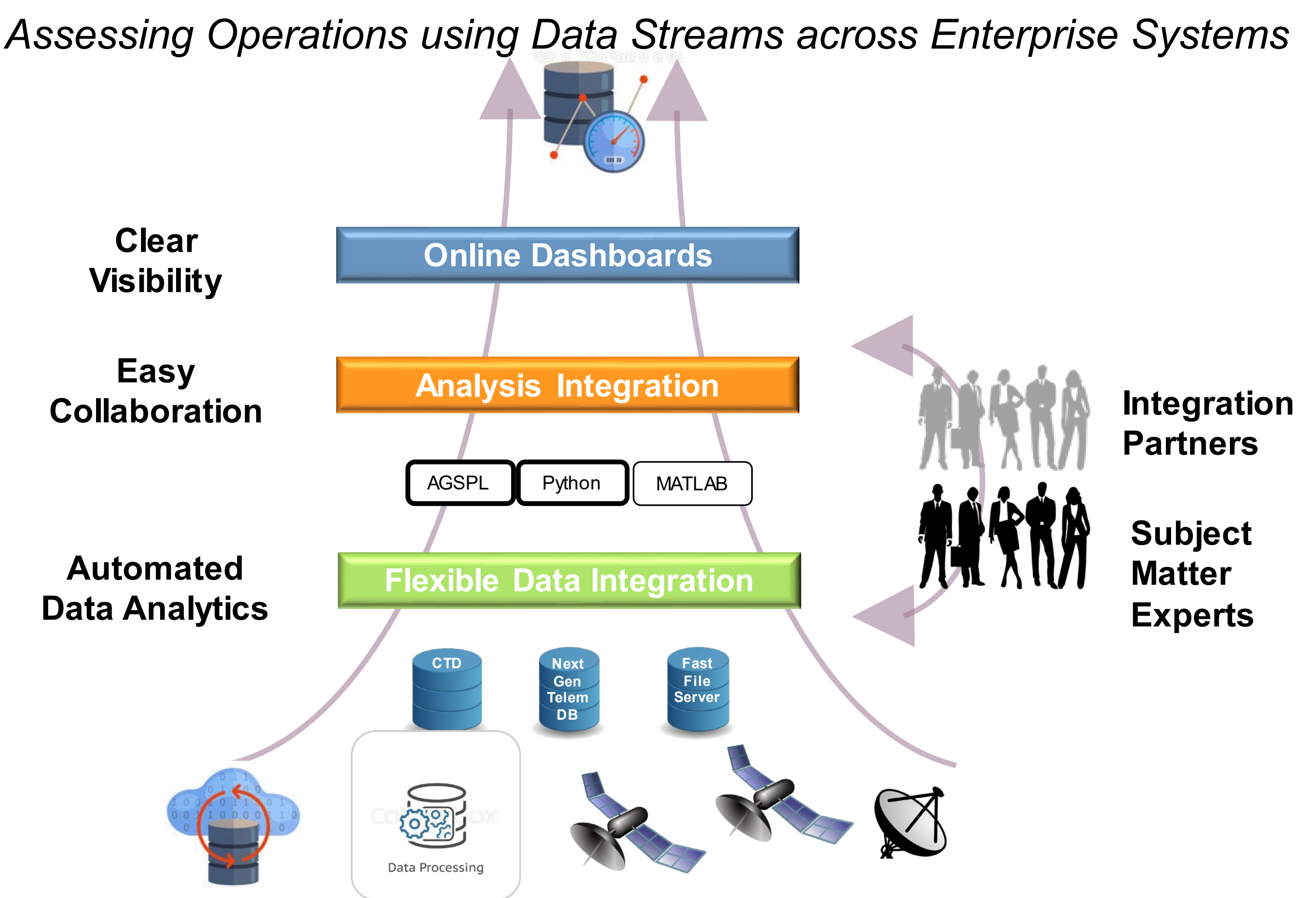
- AI/ML augments human perspective and reasoning, making it difficult to
  - *Decide what success means and hence to formulate the right requirements*
  - *Overcome unfamiliarity with the types of errors that can undermine V&V*
  - *Overcome combination of human interpretation/bias and lack of understanding of AI that can lead to particularly insidious errors*
- AI/ML may have advantages over other emerging technologies
  - *The potential of new intelligent reasoning and processing capabilities makes self-monitoring and continuous self-testing a possibility*
- Use converging evidence to build a case for trusting a new method
  - *With a repertoire of analytic methods*
  - *With domain specific a priori and operational modeling*
- Embed the new AI/ML capabilities into a robust decision process
  - *Build up a track record by following up on results with new incoming data*
  - *Use converging evidence, track record, and user reports to strengthen confidence*
- Use AI/ML only to suggest features/results that can be confirmed or refuted using traditional analytic approaches
- Employ program management strategies (e.g., monitoring, staging goals and requirements) and additional scientific research to make unknowns known

Combining AI/ML with traditional approaches to reduce risks*

*Kirstie Bellman & Chris Landauer (Kirstie.L.Bellman@aero.org)

Prototyping Use Cases to evolve V&V Framework

Elements and Flow for Test Configurations



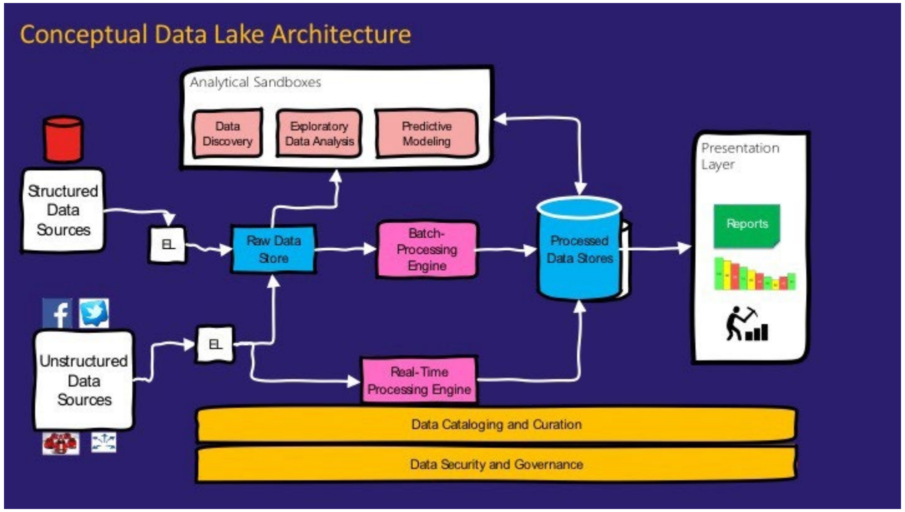
Assess Operations using Data Streams across Enterprise Systems

Approved Material Release: OTR201900411

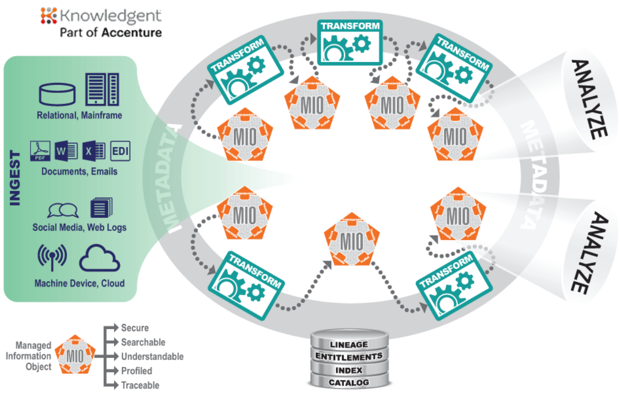
Data Centric Architecture

Verifying and validating authoritative data sources

- Load first – Understand Later
- Retain all data in its raw format
- Supports all kinds of data
- Supports all kinds of users
- Readily adapts to changing requirements
- Active cataloging of raw & transformed data



Pradeep Menon – Alibaba Cloud
https://medium.com/@rpradeepmenon/demystifying-data-lake-architecture-30cf4ac8aa07



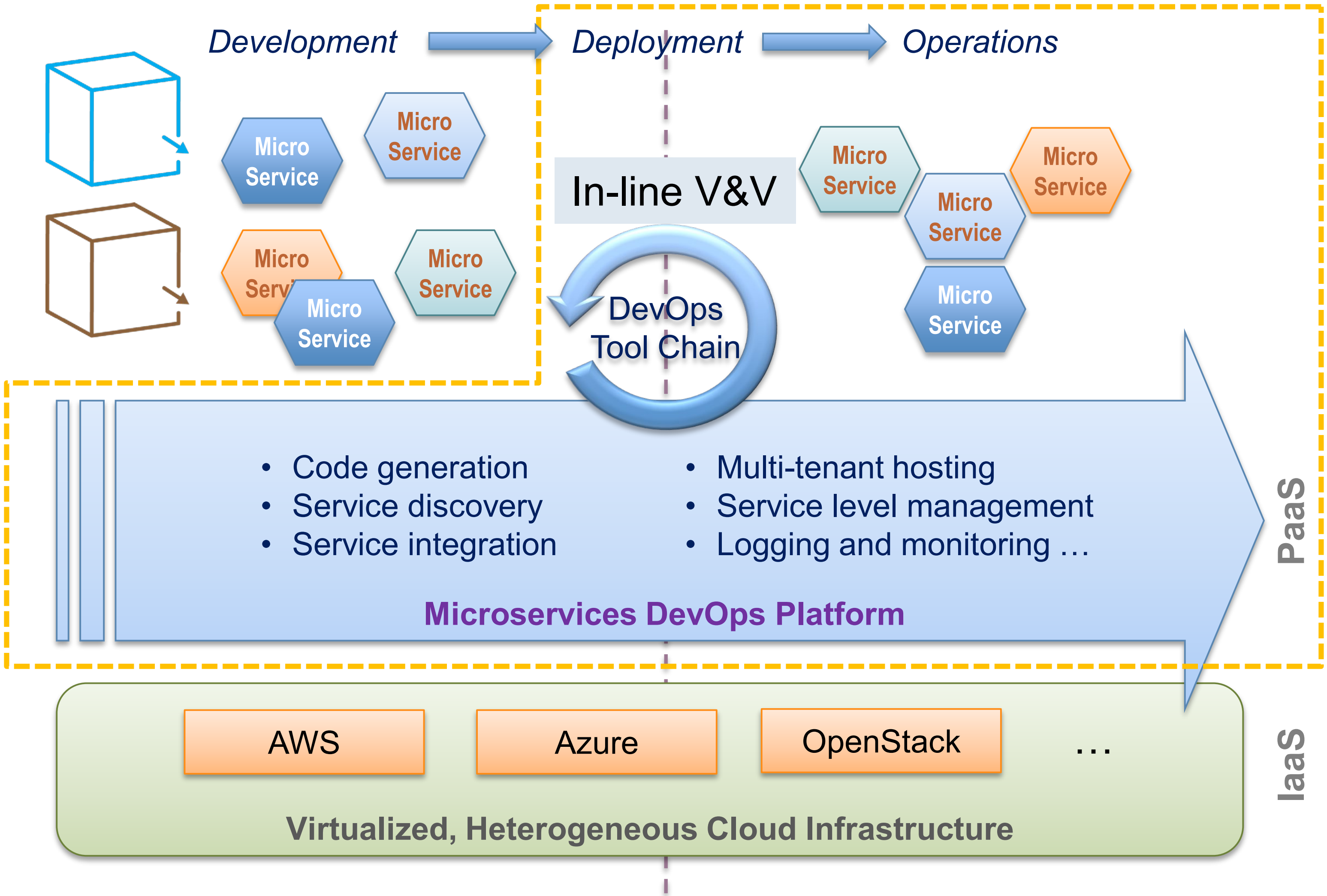
https://knowledgent.com/whitepaper/design-successful-data-lake/

- Repository for vast quantities of heterogeneous data
- Supports both batch and real-time data feeds
- Unconstrained by storage schema
- Supports Data & Analytics as a Service (DAaaS)

Moving from EDW to DL Improves Timeliness, Flexibility, Quality & Findability

Evolved Software Development Paradigm

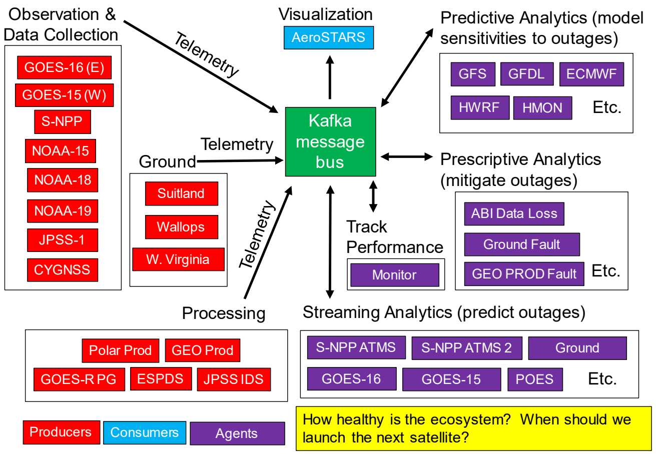
Conducting in-line verification and validation during develop ops



Governed Integration Platform for Agile Capability Deployment

Establishing AI Test Range infrastructure

- **Collect and display existing messages related to real-time diagnostic data along the data value chain using Kafka message bus**



- ***Event-driven:*** System reacts to events as they occur (as opposed to request-response or scheduled workflows).
- ***Intelligent agent:*** A goal-directed autonomous system that observes and acts on its environment.
- ***Container:*** A lightweight virtual machine.
- ***Microservices:*** Agile services (as in service-oriented architecture)

- ***Reliable:*** Failures are isolated and do not cascade. Message bus has built-in redundancy. Logic implemented in endpoints, not message bus.
- ***Scalable:*** Doubling system throughput only requires doubling the number of commodity servers (scale out, not up). New functions accommodated via loosely coupled services.
- ***Secure:*** System incorporates authentication, authorization (permissions) and encryption.

Next generation message collection and summaries of diagnostic data

Questions?