AEROSPACE

APPROVED FOR PUBLIC RELEASE

GETTING IT RIGHT

COLLABORATING FOR MISSION SUCCESS

VOLUME 10 | ISSUE 4 | JUNE 2020

OPPORTUNITIES IN DATA EXPLOITATION

By CHRISTIAN WALLISCH
The Aerospace Corporation

The Ground System Architectures Workshop (GSAW) provides a forum for the world's space-related ground system experts to collaborate with other ground system users, developers, and researchers through tutorials, presentations, working groups, panel discussions, and technical exhibits.

Over 600 members from 130 organizations in the ground system community registered for the four-day March event to discuss this year's theme of "Opportunities in Data Exploitation."

continued on page 2

Brig Gen Donna Shipton delivered the GSAW opening keynote address.

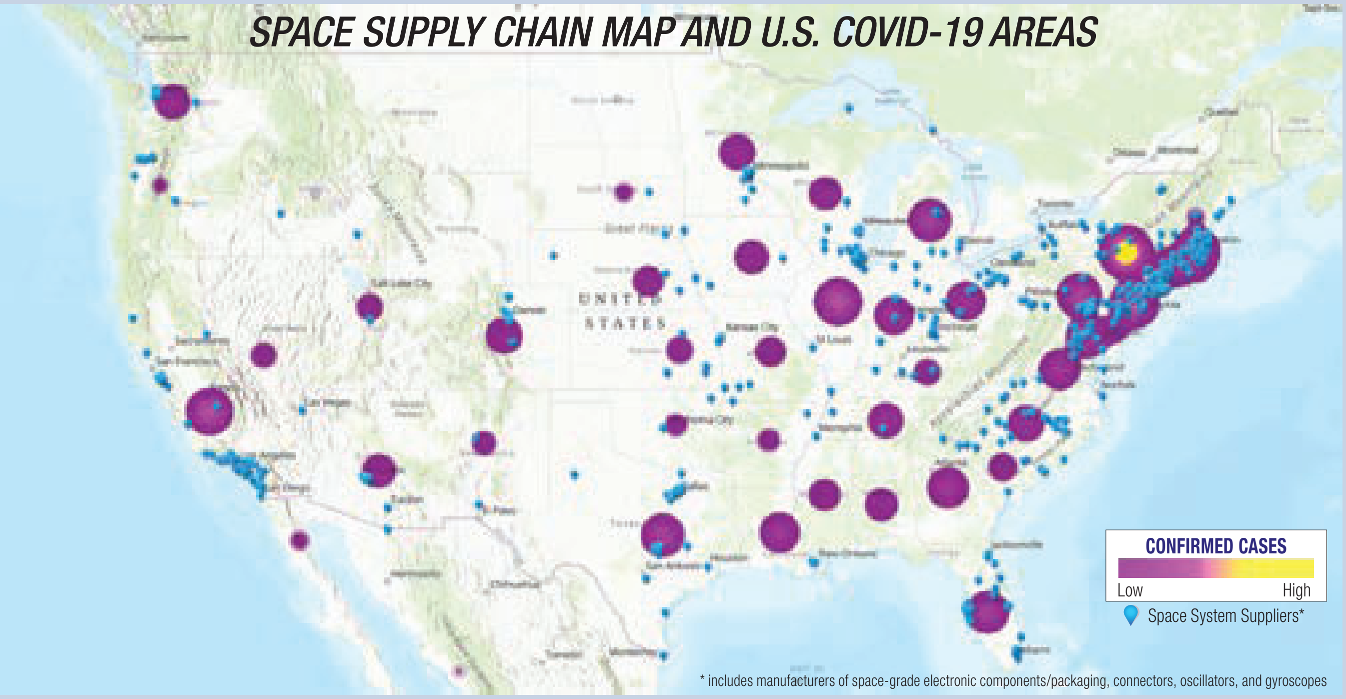
COVID-19 AND THE SPACE INDUSTRIAL BASE

By GAIL JOHNSON-ROTH,
JOE CHENG, and ELAINE LIM
The Aerospace Corporation

The world is different now as COVID-19 is impacting government, business, and public behavior. The Department of Defense has taken multiple actions to shield the defense industrial base during the COVID-19 pandemic. The health of the space and defense industrial base is influenced by the health of the workforce and the broader economy.

Supply chains involve thousands of organizations subject to a shifting array of technical, business, market, and security risks that may disrupt or deny the timely provisioning of affordable products and services as required for mission success. The Aerospace Corporation (Aerospace) is leading data collection and analysis

continued on page 4



* includes manufacturers of space-grade electronic components/packaging, connectors, oscillators, and gyroscopes

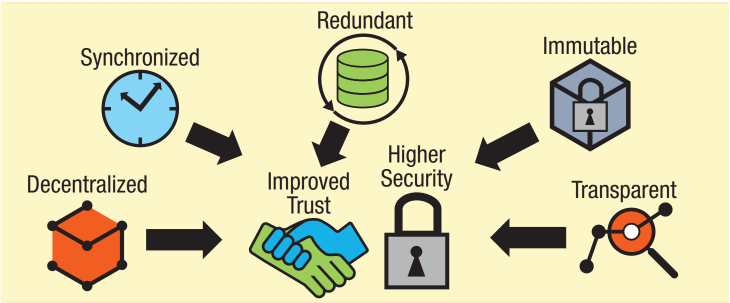
COVID-19 data taken from Johns Hopkins University, May 29, 2020.

IMPROVING TRUST IN A ZERO TRUST ARCHITECTURE (ZTA)

By ROHIT MITAL
KBR Inc.

Trust in a security environment is used in lieu of absolute certainty. Trust is needed to extend or access capabilities that otherwise would not be possible, and it's an indication of the relative strength of the assurance of the belief. The level of trust is dynamic and changes over time; access to capabilities must be adapted accordingly.

Zero trust architecture (ZTA) is a security concept centered on the belief that organizations should not automatically trust anything inside or outside its perimeters. In ZTA there is no implied trust. The trust level is explicitly and dynamically calculated based on context. The concept draws on technologies such as multifactor authentication; encryption; file system permissions; and information about users, their locations, and applications they seek access to for calculating trust.



Blockchain features that support ZTA

Amazon Web Services Blockchain, a distributed ledger technology (DLT), was employed representing multiple participants engaged in file sharing.

DLT dynamically builds trust using transaction information about the data files by creating a digital passport for each of the files. This technology offers a decentralized, democratized, transparent, universally acceptable governance mechanism for managing file exchanges. DLT assures immutability of transactions and eliminates single-point-of-failure issues while providing redundancy and availability.

With some limitations, DLT can provide an effective technical solution to addressing zero trust when acquiring data from nonfederal data sources on a global network of data providers.

For more information, contact Rohit Mital, 719.201.6996, rmital@sgt-inc.com.

OPPORTUNITIES IN DATA EXPLOITATION

continued from page 1

Brig Gen Donna D. Shipton, Vice Commander of the United States Air Force Space and Missile Systems Center, addressed challenges in the ground system field of making data meaningful and giving the right data to the right user at the speed of need.

There were key opportunities that came out of the plenary sessions:

- Machine learning—Based on addressing an objective function, such as accuracy prediction, an option that is not as smart as humans, but faster and cheaper
- Artificial intelligence (AI)—The realization that only an estimated 13% of AI projects make it to production. Lack of definitions to discover, deploy, manage, and secure models introduces inertia and distrust
- The minimum viable process—Practical tool for winnowing legacy systems engineering practices to an optimized, scaled, agile systems development approach
- Cloud-based satellite operations—Lift-and-shift legacy programs, transporting digitized RF waveform to a data center where demodulation can take place, instantiating capabilities on demand
- Learned from 1 billion ground system log messages—"The messages scroll so fast we can't read them—but if they stop scrolling, we have a big problem" (it was suggested to seek help from an intern)
- Learned how to prepare mission data for future analysis—Advances in "big data" mining techniques help monitor and highlight interesting changes with minimal effort

To end with a quote from the meeting (originally from philosopher Jean Baudrillard), we may already be living "in a world where there is more and more information and less and less meaning."

News and proceedings are available on the event website at http://gsaw.aero.org.

For more information, contact M Christian C Wallisch, 240.293.9008, mchristian.wallisch@aero.org.

Rohit Mital, right, of KBR Inc. receives the GSAW 2020 Best Presentation Award from GSAW 2020 Chair Rick Johnson. The winning presentation was titled "Using Distributed Ledger for Managing Trust Among Data Exchanges."

RECENT GUIDANCE AND RELATED MEDIA

Supply Chain Risk Management Assessment Framework for Data Center Infrastructure by K.T. Wilson; TOR-2020-01307; USGC

Space Crypto Options for Small Satellites by V.I. Lang; TOR-2020-01099; DOD

Software Technology Maturity: A Framework for Measuring Software Development Products and Processes by L.H Perry; TOR-2019-02498; USGC

SMC-S-012 Tailoring Guide for Agile Compatibility by J.R. Starcher; TOR-2020-00895; USGC

Space Vehicle Interface Specification Survey by J.B. Juranek; TOR-2020-00935; USGC

A Case Study: Limitations and Constraints of a Fixed-Price (Incentive, Firm Target) Contract by M. Callaway; TOR-2020-00679; USGC

Launch Vehicle Mission Success by M. More; TOR-2020-00051-REV A; USGC

DOD	=	Approved for the Department of Defense and its contractors
PR	=	Approved for public release
USGC	=	Approved for release to U.S. government agencies and their contractors

For reprints of these documents, except as noted, please contact library.mailbox@aero.org.

DETECTING ANOMALIES IN SPACECRAFT TELEMETRY

By VALENTINO CONSTANTINOU
NASA Jet Propulsion Laboratory
California Institute of Technology

Spacecraft anomaly detection systems typically target only a subset of anomaly types and often require costly expert knowledge to develop and maintain. Tiered alarm systems indicate when values stray out of predefined limits. The volume of data returned by spacecrafts continues to increase with missions such as the NASA-Indian Space Research Organization Synthetic Aperture Radar that will generate about 85 terabytes of data per day. Improving the accuracy and scalability of anomaly detection systems requires allocating necessary but limited engineering resources.

Deep learning and neural network architectures advancements have led to performance breakthroughs in a wide variety of applied tasks and problems in computer vision, speech recognition and translation, and time-series modeling—the latter is similar to anomalies identification problems aboard spacecrafts. Spacecraft telemetry is inherently time-series data, and many anomaly detection approaches which exist today lend themselves well to this type of data.

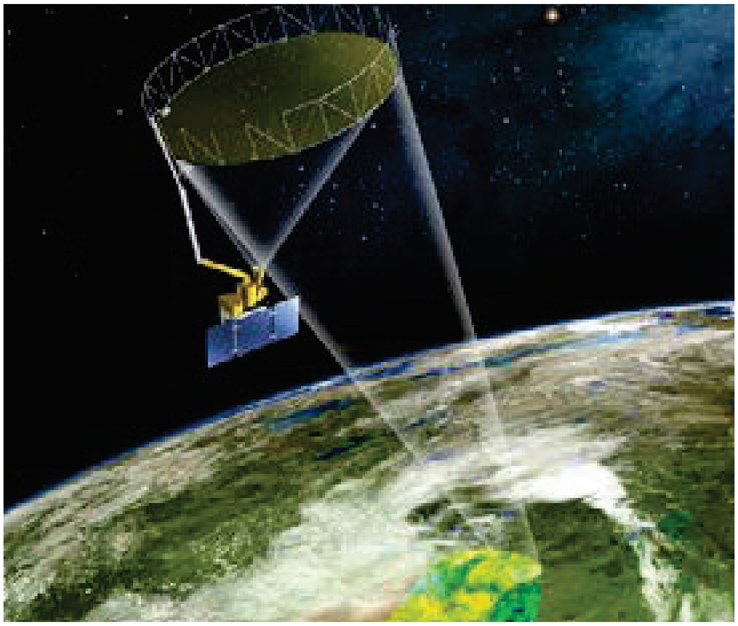


Image credit: NASA

SMAP satellite LSTM experiments result in successful anomaly detection.

Long Short-Term Memory (LSTM) deep neural networks have shown success through natural language processing, speech recognition, and text classification prediction problems by capturing important temporal information: the order of words in a sentence, the tones in one's voice, a string of characters. LSTM can identify a diverse set of anomaly types.

LSTM networks can be trained using nominal operational data. One strategy is to select telemetry and command sequences from past orbital periods with normal operations. The trained networks can then predict and compare the telemetry to the actual value received from the spacecraft. The resulting value—the residual, or error—is then tracked to flag suspected anomalous periods using thresholding algorithms.

Experiments have proved these methods work well in detecting different types of anomalies. Successful anomaly detection systems can be implemented for routine and highly automated (a "lights out" operation) missions such as the Soil Moisture Active Passive (SMAP) satellite—a 95% recall score. Challenges still exist for spacecraft with highly dynamic external conditions and operations such as the Mars Science Laboratory rover Curiosity—a 79% recall score.

Successful processing using these trained neural networks that can address increasing amounts of spacecraft data offer the opportunity to provide realtime operability and health information.

REFERENCES:

See the technical paper for additional details: *https://dl.acm.org/doi/10.1145/3219819.3219845*.

For experiment code, go to *https://github.com/khundman/telemanom*.

For more information, contact Valentino Constantinou, 626.864.0550, valentinos.constantinou@jpl.nasa.gov.

COMPLIANCE ≠ SECURITY

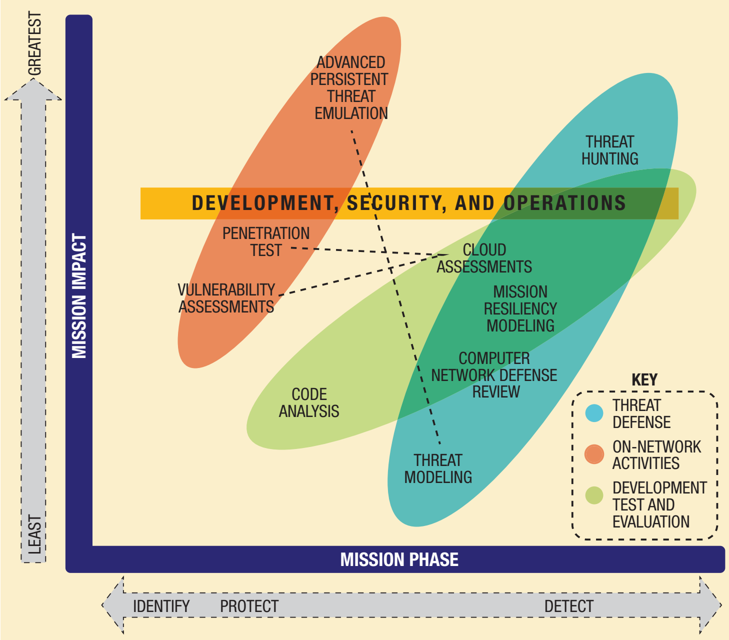
By BRANDON BAILEY
The Aerospace Corporation

Compliance-focused cyber assessments ensure that a system meets the letter of the law and the list of policy requirements by following the National Institute of Standards and Technology Risk Management Framework and/or Cybersecurity Framework. Authority to Operate is often the definition of success for these assessments but is not a guarantee of security. Attackers do not care if you are compliant!

Mission-focused cyber assessments should provide decisionmakers with prioritized, actionable ways to reduce cyber risk (i.e., mitigate vulnerabilities). A cybersecurity assessment should be a tailored evaluation based on the context of the mission, organization, architecture, and systems to determine the critical assets. Security techniques are then applied to mitigate threats and vulnerabilities to acceptable levels of risk. Cyber assessments must evaluate mission assets at each level, layer, and subsystem in addition to analyzing the architecture as an integrated whole.

Modeling the "mission thread" provides the opportunity to identify the critical assets to further assess potential points of vulnerability. The mission's adequacy can be evaluated across all phases of operations and layers throughout the architecture.

continued on page 4


GREATEST
LEAST
MISSION IMPACT
MISSION PHASE
IDENTIFY
PROTECT
DETECT
DEVELOPMENT, SECURITY, AND OPERATIONS
ADVANCED PERSISTENT THREAT EMULATION
THREAT HUNTING
PENETRATION TEST
CLOUD ASSESSMENTS
VULNERABILITY ASSESSMENTS
MISSION RESILIENCY MODELING
COMPUTER NETWORK DEFENSE REVIEW
CODE ANALYSIS
THREAT MODELING
KEY
● THREAT DEFENSE
● ON-NETWORK ACTIVITIES
● DEVELOPMENT TEST AND EVALUATION

Assessment methods evaluate mission impacts across all mission phases.

INCOSE MODEL-BASED CAPABILITIES MATRIX

By ALBERT C. HOHEB JR.
The Aerospace Corporation

Program managers and system engineering leaders are eager to apply model-based engineering to optimize their programs. The key is understanding the breadth and scope of modeling capabilities needed. Inadequate modeling capability results in system engineering goal shortfalls, and superfluous capabilities are a waste of precious resources.

The International Council on Systems Engineering (INCOSE) Model-Based Capabilities (MBCA) Matrix and User's Guide can help organizations determine their current and needed descriptive modeling capability at the enterprise, system, and program levels. The matrix assessment results provide information on needed capabilities.

Application of the matrix has proved to provide effective input into planning acquisitions, capability roadmaps, planning the evolution of capabilities, and assessing approaches during reviews.

An online assessment tool report includes an MBCA overview and a color-coded matrix for current and needed capabilities. This assessment is ideal for small projects, programs, or product managers.

A 30-minute overview of the MBCA Matrix at the 2020 January INCOSE International Workshop Town Hall is available on YouTube at https://www.youtube.com/watch?v=VRnNun2EH-o and is useful for new users to the matrix. The System Engineering Research Center—INCOSE provided benchmark survey results based on an older version of the matrix; "Benchmarking and Benefits and Current Maturity of MBSE Across the Enterprise" is accessible at https://sercuarc.org/wp-content/uploads/2020/03/SERC-SR-2020-001-Benchmarking-the-Benefits-and-Current-Maturity-of-MBSE-3-2020.pdf.

For more information, contact Al Hoheb, 310.336.0472, albert.c.hoheb@aero.org.

COVID-19 AND THE SPACE INDUSTRIAL BASE

continued from page 1

through direct engagement to assess COVID-19 impacts through existing collaborative working groups such as the Joint Mission Assurance Council and Space Industrial Base Working Group, as well as existing contractual mechanisms through program offices to identify at-risk suppliers.

Impacts exacerbated by underlying financial issues have placed significant portions of various supply chains at risk. We should anticipate long-lasting, nonlinear societal and economic effects. The foundation of the analysis starts with increased situational awareness on the industrial base health. For this effort Aerospace introduced a new capability called the Supply Chain Situation Room which allows dynamic display of supply chain intelligence to the user.

Key is understanding the impacts in relation to contractual relationships associated with suppliers to include considerations if business is mature or emerging, commercial or government, and near-term/long-term effects.

Options in terms of assistance determination can then be made on business viability, capability need, and possible application of government levers for capital/revenue enhancements and supply chain security.

Aerospace has been supporting multiple U.S. government organizations evaluating utility and options. The U.S. government is identifying issues to address in the current situation for national security space and future scenarios. Taking the right mix of sectoral and company-specific actions will support viable players providing critical capabilities for national security space.

For more information, contact Gail Johnson-Roth, 310.529.1131, gail.a.johnson-roth@aero.org or Joe Cheng, 310.336.2568, joe.k.cheng@aero.org.

COMPLIANCE ≠ SECURITY

continued from page 3

In practice, this involves working with many technologies and corresponding techniques for managing threats on critical assets such as:

- Supporting infrastructure: layer-2 and layer-3 network devices, controlled interfaces and firewalls, cybersecurity defense mechanisms, threat hunting
- Industrial control systems, operational technology
- Software: security evaluation, static, binary, and dynamic code analysis
- Mission-critical assets: identity and access management, command and control, data processing

Cyber assessments too often focus solely on compliance, rather than testing for effective security practices. Assessment methods should evaluate mission impacts across all mission phases through mission risk-focused testing to determine the cyber-based technical ground truth.

For more information, contact Thomas Axberg, 571.304.8715, thomas.axberg@aero.org or Robert J. Heald, 240.293.9025, robert.j.heald@aero.org.

2020 EVENTS

Jul 20–22 *INCOSE International Symposium (virtual)*

August 1–6 *Small Satellite Conference (virtual)*

August 24–25 *AIAA Propulsion and Energy Forum and Exposition, New Orleans, LA*

Sept 14–18 *OMG Technical Meeting (virtual)*

September 27–30 *IEEE International Joint Conference on Biometrics (IJCB), Houston, TX*

Oct 8–10 *Conference of System Engineering Research, CA*

Oct 19–22 *NDIA Systems & Mission Engineering Conference, FL*

AEROSPACE

GETTING IT RIGHT

COLLABORATING FOR MISSION SUCCESS

Getting It Right is published every three months by the Corporate Chief Engineer's Office within the Office of the Executive Vice President of The Aerospace Corporation. Direct questions and comments to gettingitright@aero.org.

Click here to subscribe.

All trademarks, service marks, and trade names are the property of their respective owners.

Cleared for public release. OTR 2020CC0634.