G2OPS®
Smarter Intelligence.®

Model-Based Systems Engineering (MBSE)

Model-Based Systems Engineering (MBSE) is radically changing how systems are developed and modernized, enabling greater visibility of distributed technology infrastructure and predictions of risk, performance and cost. A digital twin created by MBSE is a powerful tool for architecting or remediating systems-of-systems where complex interdependencies exacerbate the challenges of identifying risk levels and establishing viable project plans and budgets.

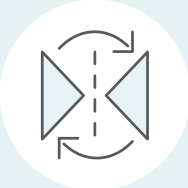
Digital Twin Technology

The MBSE approach is centered on the creation of a digital twin proxy of your system components, data, network, interfaces, requirements and operations. The digital twin provides a validated model you can count on to streamline your engineering processes from change management through installation, test and troubleshooting for your fielded complex system.

MBSE Advanced Analytics

G2 Ops provides consulting, training and digital twin creation services, with engagements ranging from introductory training and opportunity workshops to turnkey digital twin model creation and tuning. Typical deliverables include:

- **Performance Modeling and Simulation.** Provides a model of a mission's Key Performance Parameters (KPP) to map system and interface requirements and use simulation tools to predict KPP performance and optimize to their requirements.
- **Baseline/Change Management.** Models Life Cycle Inventories (LCI) of infrastructure to automate Engineering Change Request (ECR) processes to reduce administrative labor and accurately predict cost, schedule and performance of changes from the design baseline.
- **Interface-Based Integration Risk Management.** Automates interface management through architecture-managed interface requirements. Key LCI processes are supported by auto-producing interface management plans (IMP).
- **Thread Optimization.** Models tactical thread reliability, analyzing for single point of failure and assessing thread-level mission performance in response to primary, secondary and tertiary system failures.
- **Acquisition Requirements Development.** Generates contractor specifications which, when coupled with operational and architecture information, improve understanding of requirements to improve cost and schedule performance.
- **Test Automation.** Models system states, allowing for parameter variances for more complete test coverage, auto generates test matrices based on interface risk, models KPP requirements and auto generates technical data packages.



The creation and use of the digital twin typically includes the following steps.

1. Baseline definition and capture. *G2 Ops helps define an organization's IT and cyber architecture including the physical (comms, mechanical & electrical), logical (software & data) and operational (requirements & processes) aspects.*

2. Baseline management. *Our processes include setting up configuration controls, developing baseline documentation, managing interfaces and providing lifecycle support to manage platform variations over time.*

3. Impact assessments. *Starting from the established baseline, G2 Ops provides Unified Risk Management services and can analyze accurate simulations of system performance.*

4. Model change impacts. *Actual or planned changes to the baseline can be accurately modeled to evaluate modernization options, conduct tradeoff analyses, simulate per-formance of future designs and assess the strength of cybersecurity measures.*

- **Automated Technical Certification Package Generation.** Creates a complete technical certification package from the MBSE model, ready for weapons, safety and mission certification.

- **Automated Sustainment Support.** A full set of digital twin documentation is created for maintenance, training, provisioning and logistics.

- **Secure Distributed Access.** Ensures secure access to the MBSE model throughout an enterprise, including model checkout/check-in, advanced analytics hosting and data security.

Unified Cyber Risk Management

G2 Ops uses MBSE to enhance system integrity and cybersecurity by overlaying vulnerabilities against mission and operational context. This guides prioritizations for mitigations based on operational impact and criticality to mission, including the ability to:

1. Score mission-based risk impact to proactively prioritize risk mitigations prior to any mission impact. For example, our models recognized WannaCry's impact in March 2017 when the vulnerability was first published with high risk ratings, well before the exploit was generally deployed in May 2017.

2. Generate attack graphs and calculate exploit likelihood. Calculate risk based on architectural context, or threat surface, providing a sophisticated vulnerability analysis capability that predicts the likelihood cyber vulnerabilities will reduce mission effectiveness.

3. Increase impact visibility for critical components, attributing risks and vulnerabilities to multiple critical mission threads or dataflows. This capability equips leaders with mission-based prioritization for modernization planning linked to operational value.

4. Identify obsolescence exposure and supply chain risk. Systematically evaluate vendor and supplier risks in terms of individual or overall mission to enable remediation prioritization based on mission support requirements.

5. Integrate discovery scan outputs and other risk assessment data with mission threads. Take ACAS and other RMF-related vulnerability and risk assessment output and overlay mission priorities to improve comprehension and awareness of impact and modernization priorities.