Notional Mission Assurance Perspective

Preliminary draft community paper for discussion, on common MA definitions, major factors & proposed strategy

Purpose – Propose a community / talking points position on Mission Assurance (MA), distilling the key factors / elements to focus our SYSCOM technical efforts - based on delivering ‘assured’ Information Dominance (ID).

DoD Directive 3020.40 (CIP R&R) defines Mission Assurance (MA) as “in accordance with the intended purpose or plan. It is a summation of the activities and measures taken to ensure that required capabilities and all supporting infrastructures are available to the Department of Defense to carry out the National Military Strategy. It links numerous risk management program activities and security-related functions, such as force protection; antiterrorism; critical infrastructure protection; IA; continuity of operations; chemical, biological, radiological, nuclear, and high explosive defense; readiness; and installation preparedness to create the synergy required for the Department of Defense to mobilize, deploy, support, and sustain military operations throughout the continuum of operations.”

B.L.U.F – MA is a complex, multiple variable construct that has many definitions, interdependences and communication channels between the widely distributed elements of people, process/policy and products (and some would add politics). While all the variables of any MA ‘equation’ are of course important overall, we assessed that several key MA variables that appear the most impactful in delivering affordable ID are:
1 - **Cyber Security** - encompasses both defensive (IA/CND) and offensive (CNE/A) measures (includes trusted systems & networks (TSN) as well as key management factors: enforced hygiene, effective access control, etc),
2 - **Ao/RAM** – the ability to continue key operations with affordable sustainment, (note - Ao/RAM is more survivability centric, where we also need to account for resiliency – which is more environment centric overall, and some consider it another view of MA, versus a potential variable), and
3 - **Mission criticality** - operational impact / need of the capability - in general includes NSS and MAC 1 (where the ‘crown jewels assessment (CJA) and mission essential functions (MEF) factor in more heavily).

We then add key second order effects: **governance** (R&R, priorities, seam issues), **requirements** (the “what” is needed) and **TE&C/IV&V** (testing / certification), where all are themselves complex variables made up of fuzzy / political factors.

Where depending on your CJA / MEF perspective, your variable sensitivity will vary, as the coefficients are stakeholder centric – as criticality is in the eyes of the beholder!

Enterprise MA implementation - While every environment (operational, acquisition, certification, etc) will have a different combination of key value factors (greatest potential impact), these three key variables will likely always be a major force in ensuring the organization’s vision is met. The second order effects will vary based on the specific mission success objectives metrics. The management challenge is to not let the overall MA complexity drive ‘analysis paralyses’ – but instead collectively work on the key factors first, while monitoring the other variables status and barriers therein (e.g., use the pareto principle to prioritize / manage issues / efforts).

Premise - As in most endeavors with their own unique environments, one can develop an ‘equation’ view of the capability under quantification (even if many of the items are ‘implicit’) that can be constructed to account for major variables and the sensitivity of their coefficients therein. Thus more effectively discuss the many factors, elements, and trade-offs in this complex IT/cyber/process ecosphere. MA is widely thought of differently by virtually every stakeholder, even as it is fundamentally based on risk management and is heavily based on availability / resilience and security / cyber in these digital, internet connected times. Yet if we decompose MA into two major aspects: (1) operational (duties / NTAs) and (2) technical (systems, functions capabilities), then MA is more manageable. Especially within the CHENG architecture and certification aspects,
where the operational linkages are not as well known, nor within our swim lane control. To better understand the scope and what factors have the most influence on reducing the risk posture, we propose a “MA equation” approach which allows for inclusion of all variables that might influence the outcome of an endeavor, especially prioritizing impacts / risks and subsequent mitigations. The below illustration and example equation will be expanded to cover the MA variables and coefficients.

--- BLUF. We propose the major “MA” variables - and “most probable” coefficient for each (H, M, & L) - using the illustration below and the following descriptions will clarify that approach and initial numerics.

We propose a MA equation / model to accommodate the ID capability requirements, as they are a NAVY CNO leadership priority. We also provide a notional framework for leadership to balance our collective residual risks, limited funds and to ultimately discuss key stakeholder value and tradeoffs within MA.

The notional equation is comprised of elements / variables (requirements) and their coefficients (weights / sensitivity), to facilitate more global discussions and collaboratively assess these key factors with those entities struggling with the same MA scope and best value. In brief: our collective enterprise risk management plan (RMP) should address ALL major variables – where the sensitivity of the coefficients will vary by entity and will determine the prioritization and resource allocation of each organization’s efforts. Each entity will address and aggregate their maturity factors, risk impact / RoI and complexity of variables for their unique ecosphere.

We propose the enterprise risk assessment ‘equation’ (for the best value / lowest residual risk) =

REQUIREMENTS \(a_1\) + CYBER (IA/security/CND (defense) & IO/CNE/CNA (offense)) \(a_2\) + “Ao” / RAM (Sustainability / Maintainability / DOTMLPF / Automation / Survivability) \(a_3\) + SAFETY (hazmat, etc) \(a_4\) + TE&C / IV&V \(a_5\) + QUALITY \(a_6\) + ENVIRONMENT / PESHE \(a_7\) + GOVERNANCE (management / processes) \(a_8\) + MISSION CRITICALITY (overall operations utility / need ) \(a_9\) + POLICY \(a_{10}\) + TRAINING / EDUCATION \(a_{11}\) + OTHER \(a_{12}\) …

(reader note – we understand that the weighted sum equation approach is likely not the ultimate method to use, on the assumption the system is linear regarding performance, which clearly doesn't hold in this setting, as the rest of the paper demonstrates. In some aspects of the system, performance (MA) is governed by the “weakest link”, in other aspects, there is redundancy and/or capability to reconfigure or compensate for degraded capabilities, so MA is governed by the “best link.” In still other aspects, MA will be governed by conditional relationships between elements; there are also feedback relationships that create dynamics in time (downward spirals, over-shoot, under-shoot) – thus weighted sum equation cannot deal with any of these non-linear or dynamic effects – BUT we start there to at least get general concurrence on the key variables with MEF / CJA.)

Once the major variables are agreed to, the effort becomes getting all stakeholder concurrence on the relative value/weight/sensitivity of each coefficient since resources are scare and decreasing, so we must have a “best value” / highest ROI approach to MA. Collectively knowing that mission success is all about RISK, which is elusive, subjective, as well as in the eyes of the beholder” – thus the equation approach allows organizations to distill key capabilities to prioritize and resource. Value-added risk management demands that we balance “consequences” from limitations / restrictions with the greatest issue threat vectors based on key mission areas.
Even as MA is a complex function, we must be specific in variable impacts for the total big Navy picture – and get past ‘it depends’ but **deliver an effective MA process and capability to the 95% level that ID needs initially.** The intent of this MA community paper is to ensure all major variables are accounted for (where there is no wrong answer, but we want to have minimal categories that accommodate similar factors), and then propose estimated, notional values to initially quantify each variable’s sensitivity / impact value to then seed the ID prioritization of MA efforts – e.g., what matters! That is, this MA strategy paper’s first pass review / discussion is intended for an initial variable concurrence (the WHAT), then seed the discussion on a value estimate of the utility of that variable (H, M, & L), to the overall “MA eco-sphere.” From there, we develop our MA POA&M.

We need to take an overall lifecycle approach to designing in, building, integrating and certifying MA – ending with the IV&V of the T&E results demonstrating that the MA capabilities were indeed delivered. As well as work as designed and advertised, with any limitations clearly noted - as the following illustration shows from the ‘systems engineering “V”’ perspective.

**SoS Testing and Evaluation (T&E) & Capability / Interoperability Certification**

*** **We propose / estimate the end state MA ‘key’ variables as** (assessed / described in the next section):

1. **cyber security** - both defensive (IA/CND) and offensive (CNA/E – in authorized hands),
2. **Ao/RAM** – ability to continue operations, affordable sustainment, and
3. **Mission criticality** - operational impact / need - in general includes NSS and MAC 1 capabilities.

We then add **governance** (R&R, priorities, seam issues), **requirements** (the “what” is needed) and **TE&C/IV&V** (testing / certification) as key second order effects.

Recommendations: SYSCOM initiate a MA directorate WG/IPT and update this paper as a collaborative way to determine the key MA strategy aspects to focus our directorate TE&C efforts / resources on:

* Supplement / follow the DoD MA strategy objectives (and resolve the MA vs resiliency overlap / duplicity).
* Quantify the key technical capabilities for the ID vision / three operational vectors (assured command and control, battlespace (situational) awareness, and integrated fires (responses, both kinetic and digital).
* Collectively define and prioritize the key / most impactful variables for MA (MEF & CJA), including metrics.
* Synchronize the various risk management plans / frameworks for the enterprise – an integrated “RMF”
* Align MA/Cert directorate resources / processes to support the key ID needs – influence where we can.
* Align all MA activities / processes into supporting the IT Technical Authority (TA) objectives.
* Incorporate SoS/I&I SysEngr aspects into all applicable variables, to include following standards in an enterprise architecture, life-cycle / end-to-end perspectives, minimize costs: TOC / CAIV / etc.
MA Discussion
(note – the appendix has additional rationale / support details)

1 - Methodology (and limitations)

Methodology overview – How we assess MA is important, where process, methods and intentions matter in any outcome assessment endeavor. MA is an all-encompassing construct with numerous perspectives and definitions – from every angle and stakeholders view and objectives. Thus getting a consensus on what the key attributes and issues are is problematic at best. Weighting the variable coefficients sensitivity from their user outcome impact, maturity and complexity, then allows stakeholders to more easily prioritize resources for those factors that have the most risk reduction “RoI” in their specific environment. Additionally, the equation can change to accommodate other factors and rebalance the coefficients sensitivity as needed. Thus the MA quantification and support processes can be standardized, where, even as the major influences can morph with technology and threats, the discussions and mitigations can move forward while management decides in parallel the best value tasks at each major variable’s inflection points.

MITRE (see appendix for more details) - a principal responsibility of a commander is to assure mission execution in a timely manner. The Mission Essential Function (MEF) they define relates to operational scenarios and NTAs therein (Navy Task Activities); this is an excellent method to use / complement the ‘crown jewels” assessment (CJA) methodology to view variables and coefficients. MA includes the disciplined application of system engineering, risk management, quality, and management principles to achieve success of a design, development, testing, deployment, and operations process. MA reaches across the enterprise, supply base, business partners, and customer base to enable customer success.

2 - What sorts of variables / factors should we consider? How do we support MA for customer capability delivery and also in a SysEngr approach too? We consider the operational and technical aspects as major top-level categories under MA, principally because they are managed by different entities and are assessed differently – to a large degree, heuristically for the former and capabilities centric for the latter.

“…When we engineer for mission assurance, what essential attribute(s) are we seeking to “engineer in?” Is it robustness, resilience, dependability, risk management, security, agility, flexibility, or adaptability? Is it one of them, some of them, or all of them? What are the tradeoffs and how are they determined? Who is the decision maker—the operator, the producer, or the accreditor and what role should each play in the decision-making process? What does “systems engineering for mission assurance” look like? The reality is that we don’t yet have a complete answer.” This equation approach will allow better understanding and practice of MA and when taken together, the various dimensions of mission assurance pose some of the most difficult challenges in engineering systems today.

“…The working definition of “systems engineering for mission assurance” is rooted in the insight that operational users of military systems are almost always willing to accept some level of risk in accomplishing their missions. It is in the nature of their profession, but to do that, they need the tools to understand the risks they are accepting and the ability to assess and balance available options and alternatives. This suggests that “systems engineering for mission assurance” is the art of engineering systems with options and alternatives to accomplish a mission under different circumstances and the capability to assess, understand, and balance the associated risks. Options and alternatives will likely take the form of a blend of technical and operational elements, which requires systems engineer to have an intimate understanding of the technical details and limitations of the system, the doctrine and operations of the user, and the environmental conditions and threats that will or may be encountered….”

The equation approach helps focus key operational risks into better systems understanding of the more complex and dynamic “I&I” aspects of the environment.

Michael.h.davis@navy.mil
Two initial sources providing suggested factors to consider for MA variables are:

(1) JPL MA disciplines (example items to include, taken from several JPL sources):
Reliability engineering, problem/failure/trouble reports, environmental engineering, parts / components engineering, materials & processes, contamination / hazardous material control, quality assurance, software assurance, system safety, configuration management, environment protections, planning and management process, regulatory / statutory compliance, mission operations (C2) assurance…

(2) NASA Policy for Safety and Mission Assurance - Typical SMA Items from those who know MA very well.
Industry / regulatory awareness - Advisories / Alerts (Government-Industry Data Exchange Program)
Emergency preparedness (Worker Health and Safety aspects) Mishap reporting and investigating

Quality - assessment, assurance audits engineering management, parts, product identification and traceability, reviews, software, surveillance, workmanship, Reliability engineering, human management, software. Reliability-centered maintenance, Risk assessment and management…
Safety - management engineering, aviation, confined spaces, cryogenic, electrical, explosives, propellants, and pyrotechnics, mobile device activity, facility, fire, hazardous materials, hazardous operations, explosive / oxygen other gasses, ionizing and non-ionizing radiation, delivered products, systems container vessel, software, system test operations, survivability, training…

3 – Mission assurance perspective as an integration, aggregation from systems assurance?
How do we both accommodate and all work collaboratively towards one MA end state – assured information dominance, based on key operational missions – which must be aggregated into a site / platform view.

- Mission Assurance:
  - Process to ensure that assigned tasks or duties can be performed in accordance with the intended purpose or plan

- System Assurance:
  - Justified confidence that the system functions as intended and is free of exploitable vulnerabilities
  - Either intentionally or unintentionally designed or inserted as part of the system
  - at any time during the life cycle

- System Assurance Activities:
  - Planned, systematic set of multi-disciplinary activities
  - to achieve the acceptable measures of system assurance and
  - manage the risk of exploitable vulnerabilities.

One MA view can be approached in the same general way as ‘open architecture (OA)” methods and processes are accomplished…integrating the major MA equation variables using standard modules, interface controls and common processes --- while using a couple of standard systems engineering methods:
(1) a DON enterprise architecture, (2) common standards (and profiles therein) and (3) specifications for key modules / elements / capabilities... and even processes. One key MA objective is to **minimize complexity** – reduce the numbers of variables and standardize those that remain - aka, drive them all to a "commodity" state! 

*Especially as Network and Systems Risks Impact Mission Objectives*, as illustrated directly below and as we've found in our platform / SoS certifications, using the mission impact and aggregation model in the “MFOM” program to aggregate operational impacts - where it's all about the DATA (re: 2 following figures).

Systems reliability and assured data flows are then also key aspects in MA execution of operational tasks by mission. These can both be well accounted for in the “MFOM” program and model that the fleet uses for their Maintenance Figure Of Merit (MFOM) calculations of reliability – supporting the overall ship’s readiness posture (re: MFOM operational impact results feeds Status of Resources and Training System (SORTS), as well as the Defense Readiness Reporting System (DRRS), etc). The complexity of numerous capabilities interoperating and shared data aspects of our multi-mission platforms must be accounted for in our MA processes, supporting the key operational missions.

---

As “data/information” flow and use is a major factor in the decision superiority aspect of “ID” – and knowing we must securely transport data and then use other applications and programs to facilitate transforming that...
Mission assurance requires mapping Mission Essential Functions (MEFs) onto their cyber assets to identify mission dependence on cyberspace capabilities – ideally using the “cyber security kill chain.” This mapping assumes a contested cyber environment where an adversary seeks to exploit or attack a mission through cyberspace. (excerpts from USAF ARL)

Mission assurance follows a four-step process:

1. Prioritization of mission essential functions
2. Mapping critical cyber assets
3. Vulnerability assessment of mission essential functions
4. Mitigation of vulnerabilities and risks

**Prioritization:** The first step is to create a detailed outline of the mission essential functions. Subject Matter Experts (SME) prioritize the MEFs according to their effect on the outcome of the mission. The outline must include the level of granularity with which this mission requires visibility into the basic cyber components. Each MEF breaks down into smaller cyber elements. However, depending on their importance in the overall mission prioritization, they may require more or less decomposition.

**Mission Mapping:** During this next step, a mission separates into lower level mission essential functions. The mission essential functions break down further into basic components. The cyber components includes USAF owned assets, DoD owned assets and commercial assets used during the mission. The SMEs narrow the focus to those assets that are most critical for the success of the mission. Essential to understanding and striving toward mission assurance is defining the connection between cyber components in relation to the mission.

**Vulnerability Assessment:** Throughout the stages of the mission, cyber assets have varying impact on the overall measure of mission assurance. The impact ranges from no effect, mission degradation requiring fight through capabilities, to mission failure. A formal examination of the cyber assets previously mapped out allow for a complete vulnerability assessment.
Mitigation: After identification of the potential vulnerabilities, current research, TTPs and mitigation strategies reduce the exposure of the mission. The challenges not solved pave the way for future research and breakthroughs.

For one current example of the complexity of MA with the various variables / inputs / priorities, we summarize the current efforts within the NIST CIP cyber security framework initiative, being led by the Whitehouse, with several public conferences this year alone. The important reference point for MA is what they think is important and to realize that those factors are pervasive in our IT / network / cyber ecosphere, including the ‘internet of things.’ As of Sep 2013, 4 of 5 NIST CIP conferences were held to date – major progress made, but questions remain on such key issues as: implementation, privacy protections and coordination with existing programs and standards. Also, according to a discussion draft prepared for the Dallas workshop, the gaps still include: authentication, data analytics, privacy and supply chain. Many participants also said that more guidance was needed on what to do first. "I wouldn't know where to begin," said one participant who has conducted audits of major financial institutions. (see URL for more details [http://www.nist.gov/itl/cyberframework.cfm](http://www.nist.gov/itl/cyberframework.cfm))

DHS started a working group for voluntary program participation with incentives designed to spur companies to adopt the framework. One of the incentives expected in the framework is cyber-insurance; it's seen as a way for infrastructure owners to mitigate risk. Also, see the US Chamber of commerce proposals to increase participation: extending liability protection, eliminating some cybersecurity regulations, leveraging federal procurement (NIAP), and making R&D tax credit permanent. The cybersecurity framework advises critical infrastructure companies to:

- Inventory and track physical devices, systems and software applications and platforms within the organization.
- Protect remote access to organizational networks to include telework guidance, mobile devices access restrictions and cloud computing policies and procedures.
- Reduce potential for abuse of authorized privileges by eliminating unnecessary assets, separation of duties procedures and least privilege requirements.
- Integrate cybersecurity practices and procedures with human resources management, such as personnel screenings, departures and transfers.
- Perform personnel and system monitoring activities over external service providers.

NIST initially issued a FRI for the framework and received over 200 companies responses. NIST developed a summary of all the responses, plus statistic, etc. The summary of that summary of issues is listed below – where MOST are directly related to MA as well as cyber:

- Leverage the NERC CIP standards (note - V5 may not apply the same to other 18 sectors)
- PII/privacy (need a global nature - where the EU is stricter)
- Follow the data - DLP and big data analytics
- Need a cyber reference architecture (and use APLs...)
- Resiliency is major of course (BCM / COOP)
- "one size does not fit all in cyber" (some also say almost 90-95% security is the SAME regardless!)
- Focus on risk management (many suggest using RMF) (then again, don't chase the threat, which is elusive, but use 'consequence based' risk mgmt as well!!)
- Need to agree on the KEY impact areas (crown jewels) = MEF – mission essential functions
- NIST SP800-82 is good (Guide to ICS), but need an implementing / tailoring process.
- Need a scalable CIP foundation... (like COBIT, or the "top 20 SANS controls")
- Business risks must be addressed in cyber protections approach... including COMMON METRICS
- Global education is needed...target SMEs / IA folks who build stuff..
Need a Cyber CMM... a standard model to assess / map too (aka, CVE, NVD, CVSS, etc)

Need common, effective Cyber tools.


The key to the “MA equation” is in the calculation of the sensitivity of the variable coefficients, as while are variables are important to consider, the actual mission impact and “ROI” of added resources varies widely for each factor. A key tenet of this weighted / sensitivity approach is that, while most variables are essential to MA, many have low ROI / value in added efforts, as they are: (1) under mature management (the state is known and executed effectively) and (2) adequately resourced in the current state. That is, they are essentially at the upper end of the ‘law of diminishing returns’ curve and good enough in the aggregate, knowing resources are constrained and other critical factors need more support. The leadership challenge is then to acknowledge many essential factors are ‘good enough’ in the present state yet not diminish their overall value / utility to MA. Where the MEF/CJA focus needs to be on those variables that need the support to raise their effectiveness for the enterprise. These higher weighted, more sensitive variables factors are then used to prioritize risk reduction efforts based on utility of effort, accommodating both the law of diminishing returns and economies of scale.

We propose that the coefficient weights (which reflect the RISK to them) are derived from three main factors: impact, maturity and complexity – which are described in the coefficient section of the paper. Where the weight / risk level = impact (10 – 1) x maturity (10 – 1) x complexity (10 – 1) ; where the scales of 10-1 are explained later, (e.g., max weight = 1000 and min = 1).

- **Impact** is based on: a relative (and generally somewhat subjective) assessment of the potential damage caused by a reduction in the provided capability – heavily related to the “MAC” level (mission assurance category) used in IA security level determinations (re: level I causes ‘severe damage’). For example, given our defense in depth / breadth architecture, and the typical / standard C4ISR capabilities and methods – how much would the operational mission risk be increased if this capability was significantly diminished with no workarounds or alternatives.

- **Maturity** is based on an assessment of the state of the capability. This factor predicts how well the capability / function is developed, managed and provided for now; that is, where is the program / process on the ‘law of diminishing returns curve’ (using common rubrics like the Gartner hype cycle) and would additional resources make any reduction in risk. As an example, products with low TRL (Technology Readiness Levels) are more immature (that is, less than 6 is considered less mature) and add more risk. Maturity is a significant factor for each variable, as a high value means the likelihood of an impact is enhanced, thus the risk is higher– e.g., not well accounted for in the capability set. Thus in the extreme the overall MA risk is reduced where a high impact occurrence is greatly mitigated by a mature variable (an inverse relationship)

- **Complexity** is based on a notional value to quantify the added risk of the unknowns, like creating covert channels, where added SoS / I&I factors / connections add to the likelihood of new vulnerabilities. For example a capability with many interfaces, dependencies and data flows is considered more complex, where a commodity item with simpler connections is considered less complex. This factor is a general weight to account for the potential added risks from more: communications / channels, data paths, etc – most unknown.

Of course, we also need to agree on which risk management framework and model to use. There are many models to consider: NISTs risk management framework (RMF), NSA’s Mission Oriented Risk and Design Analysis (MORDA), Aspect-Oriented Risk Driven Development (AORDD) Framework, Common Vulnerability Scoring System (CVSS), Mitre’s Threat Assessment & Remediation Analysis (TARA), etc., etc. (note, usually MORDA process is implemented according to the Security Optimization Countermeasure Risk and Threat Evaluation System (SOCRATES)) – then again, there are newer game-based methods of risk assessment to consider as well.
4 - Variable discussion:
+ for each variable we propose definitions / scope - major elements (ideally, eventually MOEs / MOPs too)

+ REQUIREMENTS - (a1) - This is the most basic of all variables that every endeavor must quantify in depth up front – assess if we have scoped and defined WHAT “MA” is / or is not - for all variables / factors and then who approved them? Typically requirements are developed first from an operational perspective that then needs to be translated into technical requirements which further quantity measures of effectiveness (MOEs) / measure of performance (MOPs) to gage the success metrics associated with providing “MA.” Any metrics determination will be problematic, given the wide variety of definitions and variables MA currently has. In general MA has numerous categories to accommodate – as illustrated by the typical reliability input data available (e.g., FMECA, hazard analyses, etc) and MA design priorities. For example, some common MA design priorities are: 1. Safety critical, 2. Mission critical, 3. Reliability critical, 4. Maintenance critical, and 5. Monitoring critical. Additionally, synonymous with organizational mission assurance capability is an organizational reliability capability, which is defined by IEEE Standard 1624-2008 as the ability of an organization’s reliability practices to ensure that product reliability meets or exceeds its customers’ requirements. In general, the requirements should be quantified at a level commensurate with the product/capability criticality, SysEngr life-cycle phase, and ultimate value of the effort. Additionally, the technical requirements need to accommodate Modular Open Systems Approach (MOSA) following a common, accepted enterprise architecture. Then of course, we need to use the standards that apply to MA - ISO/IEC 27000 series, DoD Instruction 3020.39, ISO/PAS 22399-1, NFPA 1600 and NIST FIPS200 (and others), etc..

+ CYBER - (a2) - Covers IA/security/CND (defense) & IO/CNE/CNA (offense) & threat / vulnerabilities. Of all the MA variables, this is definitely the ‘wild card’ in that it too is defined differently by most users and the ability to accurately assess security risk and then aggregate many functions / levels is relatively non-existent, or marginal at best. Even then, no two experts can agree. Add in to that uncertainty that our inability to gauge just how well “inheritance” actually works and the deterrence effectiveness of computer network exploitations / attacks (CNE/A) and the security protections variable is fuzzy at best. This variable is intended to capture ‘most things in cyber security” even as the various sub-functions therein are themselves fuzzy on how effective they are (education, etc). When we describe the cyber ‘coefficient’ below we will take into account the huge potential impacts of rare but catastrophic events and the proven capability to inflict kinetic losses through digital means. So how do we assess cyber risks with what methods – like: the System/Acquisition Mission Assurance Engineering (SAMAE), or Decision Analysis to Counter Cyber Attacks (DACCA) or others? Like Microsoft’s DREAD? (“note - The DREAD model is used, and promoted, by Microsoft as a means to prioritize risks associated with exploitable vulnerabilities, and to do so with a greater granularity than is possible with a simple numerical or red-yellow-green type rating system. “DREAD” is an acronym made up of the first letters of five attributes that threat modeling uses to “measure” each vulnerability in the system being assessed—
- Damage potential—How much damage will result if the vulnerability is exploited?
- Reproducibility—How easy would it be reproduce the exploit?
- Exploitability—How easy is it to exploit the vulnerability?
- Affected users—How many users (rough percentage) would be affected by the exploit if it were successful?
- Discoverability—How easy is it to find the vulnerability?)

+ “Ao” / RAM (a3) - consists of Sustainability / Maintainability / DOTMPLF / Automation / Survivability / etc. Besides defining these factors in a common, global manner, we also need to agree on the failure mode severity and probability of occurrence numerics / algorithms. For example, reliability definitions are different than those used in safety, etc and with definitions for reliability / safety top impact severity ranges varying from; (1) complete loss of primary mission capability / Catastrophic (death, system loss, or sever environmental damage)... all the way down to the lowest level (5) insignificant / none/ insignificant. We then need a common...
risk matrix transition between various risk guides, for example the NIST RMF versus mil-std-882d versus the one in NWSCP (interoperability certifications) – for just a couple of those being used.

+ **SAFETY** (hazmat, etc) - (a4) - Safety is the state of being "safe", the condition of being protected against physical, social, spiritual, financial, political, emotional, occupational, psychological, educational or other types or consequences of failure, damage, error, accidents, harm or any other event which could be considered non-desirable. In general, entities producing capabilities need to follow ESOH. Safety is the condition of a “steady state” of an organization or place doing what it is supposed to do. “What it is supposed to do” is defined in terms of public codes and standards, associated architectural and engineering designs, corporate vision and mission statements, and operational plans and personnel policies. For any organization, place, or function, large or small, safety is a normative concept. It complies with situation-specific definitions of what is expected and acceptable. Safety can also be defined to be the control of recognized hazards to achieve an acceptable level of risk – this is the perspective we take in the MA equation. Since ‘safety’ is a relative state, eliminating all risk, if even possible, would be extremely difficult and very expensive. Thus a ‘safe situation’ is one where risks of injury or property damage are minimal and manageable.

+ **TE&C / IV&V** - (a5) - We’ll need a representative ‘use case’ by which to accurately IV&V. TE&C results (Test, Evaluation and Certification - supported by Independent Verification and Validation methods) supports assessing and quantifying that the capability / process actually provides what the requirements state. This too is a broad area in and of itself, as most of the variables are, and can be more or less critical, depending on how well the design is built - including using open architecture methods, minimize coupling, reducing dependencies, etc. The value of TE&C is assessing the final state in the intended environment; thus increased confidence levels that the capability works as intended for the user, and the risks are minimized and well known.

+ **QUALITY** (a6) - this is a fairly subjective variable that is interrelated with many others as well. Quality of design tends to be the most important factor in this variable, as within that construct fault tolerance can be incorporated to minimize the need for high quality components to get an adequate quality result. IAW DoD/DAU program manager's guide "The quality of products or services is determined by the extent they meet (or exceed) requirements and satisfy the customer(s), at an affordable cost - as built according to specification. . Quality is a composite of material attributes, including performance and product/service features and characteristics that satisfy a customer's requirement. A key to success is to incorporate systems engineer/design quality into the product by defining the product or service quality requirements from the beginning and then providing the contractor with the maximum degree of flexibility to meet these requirements". Quality needs to be defined first in terms of measurable parameters or characteristics, which vary from product to product. For example, for a mechanical or electronic product these are performance, reliability, safety and appearance.

+ **ENVIRONMENT / PESHE** - (a7) - This variable accounts for the overall site / platform effects in MA, both digitally / virtually as well as true natural and physical aspects. Are there backup capabilities, can other places / processes easily take over, is the location unique or a choke point, are there huge disaster / cleanup costs (e.g., 'toxic super fund')

+ **GOVERNANCE** - (a8) - This accounts for the required management of processes, people, products and priorities (among others). Given delivery of any capability, the organizational level of effort needs to be quantified and documented (and then of course followed / enforced), especially the communication plans / methods (which get more complex as the numbers of entities / personnel grows).

In the Seventies organizations used IT/networks to reinforce departmental or functional specialization (including the matrix organization). Starting in the Eighties the tide began to reverse and managers began to think in terms of value chains and processes. In the Nineties IT gurus joined in with Business Process Reengineering.  

Michael.h.davis@navy.mil
Workflow, and, more recently BPM Systems and Six Sigma. Today we are witnessing a shift from management based on departments to management based on processes. Still, any every organization, commercial of government, can benefit by adopting best practices in business process management – focused on user satisfaction in mission accomplishment.

**MISSION CRITICALITY** *(overall operations utility / need)* - Mission critical refers to any factor of a system (equipment, process, procedure, software, etc.) whose failure will result in the failure of business operations. That is, it is critical to the organization's mission. Also, if a business operation cannot be interrupted under any circumstance without hurting production, then this operation is considered business mission critical because it is indispensable. Also, from DAU, Mission-critical functions are those functions of the system being acquired that, if corrupted or disabled, would likely lead to mission failure or degradation. Mission-critical components are primarily the elements of the system (hardware, software, and firmware). In addition, the system components which implement protections of those inherently critical components, and other components with unmediated access to those inherently critical components, may themselves be mission-critical. Mission-critical functions and components are equal in importance to Critical Program Information (CPI) with respect to their inclusion in comprehensive program protection. There are four generally accepted protection failure criticality levels:

- **Level I** – Total Mission Failure --- Program protection failure that results in total compromise of mission capability
- **Level II** – Significant/Unacceptable Degradation --- Program protection failure that results in unacceptable compromise of mission capability or significant mission degradation
- **Level III** – Partial/Acceptable --- Program protection failure that results in partial compromise of mission capability or partial mission degradation
- **Level IV** – Negligible --- Program protection failure that results in little or no compromise of mission capability

**KEY NOTE** - Additionally, there are three "MAC" levels, described later, that instinctively, though still at a high level, define a common level of mission criticality (e.g., critical, essential and support). Finally, for an example of "what matters most" - when it comes to "IT / cyber", for such a commonly used IT industry term, mission critical computing is a surprisingly difficult label to clearly define and classify. For many IT strategists, definitions of mission critical computing are often rooted in the realities of IT from past decades. Put simply, mission critical computing refers to any application, workload or system that is deemed essential to the core function of the organization.

This variable tries to accommodate the criticality of all levels of capabilities and processes and interactions between individuals, units and strategic management. This variable is much more the people aspect of MA versus the more technical aspect we can influence with systems engineering. It's meant to convey the utility of the entity in the enterprise within a more global roles / responsibilities (R&R) and Navy Task Analysis (NTA), for a couple of examples, where together they indicate the priority and criticality of the element in assessment - principally as they effect the operational risk assessments based on key mission areas.

**POLICY** - Policies (and execution procedures to support them) are the strategic link between an organization’s Vision / Mission and its day-to-day operations. But why is that so important? It's because well written policies & procedures allow employees to understand their roles and responsibilities within predefined limits. Basically, policies & procedures allow management to guide operations without constant management intervention. As well as have consistent execution of processes with definitive metrics to make decisions on and manage expected behavior. Policies and procedures connect a company's vision and goals to internal operations. These internal controls are key to accountability within the company structure. Policies are general and define the important issues within the company, while procedures include step-by-step directions that ensure consistent behavior. Taken together, policies and procedures provide a road map for a company's workforce to
follow. They provide guidelines, promote consistency, guide disciplinary / enforcement actions, assist with statutory / regulatory requirements.

+ **TRAINING / EDUCATION - (a11)** – Training presents an opportunity to expand the knowledge base of all employees, and training and development provides both the organization as a whole and the individual employees with benefits that should enhance the ‘value proposition for all stakeholders. Training addresses weaknesses, leads to improved performance, provides consistency in knowledge, and leads to higher employee satisfaction. All of which improves the bottom line - consistent execution of processes, tools, and equipment - as well as better designed and built capabilities. Education and training are key agents for transformation. They are complementary activities which reinforce each other. Education focuses on the function of explaining concepts, doctrines and practices and teaching procedures, for instance English language classes and history. Training focuses on practicing and applying that knowledge, which helps to assimilate the subject matter completely. Education / training comes in several levels: awareness, productivity / skills increase, vocational (apprenticeship, etc), professional, and targeted levels for specific product / service development (among others). Thus education comes in many forms, but the precept is that these forms are relatively well known for the industries they support, where the execution process and efficiency of skills absorbed may be lacking.

+ **OTHER - (a12)** - definitions / scope - major elements

*note - this is a placeholder to add other variables, with a corresponding coefficient proposed in the following section*

**5 - Coefficient discussion:**

The weights of the coefficients are a critical aspect to making the “MA equation” work within a wide community of interest and varying perspectives / objectives. We described the three main factors earlier and now broadly quantify the implementation perspectives / numerics with the intent to assess the RISK associated with that factor. For this initial discussion version, we will use notional values to represent $H = 9$, $M = 5$ and $L = 2$, and we’ll eventually iterate all variable’s coefficient with each capability owner / community of interest (COI) leads, who can adjudicate their specific values. The collective coefficient risk value then is $I \times M \times C = a$ straight multiplicative numeric, where 1000 is the highest risk and 1 is the least. Thus the high variable coefficients then signify a potential for severe damage - with an immature capability / process containing a high degree of complexity – these factors help weight damage aspect of impact. Where the intent of developing the variable coefficients is to work on the highest values first, determine where we can exercise influence directly or engage the principle owners to assist them. This includes managing / adjusting resources to more needed variables and the trade-off analyses needed therein.

**Impact** – potential damage caused if the capability / process is reduced / removed and the ‘operational risk’ of diminished mission areas subsequently increases. High (risk) implies that the loss of the variable will cause severe damage. We will use the established damage levels quantified in the “MAC” levels as our definition.

- **MAC I** - the loss of data would cause severe damage to the successful completion of a DoD mission.
- **MAC II** - the loss of systems could have a significant negative impact on the success of the mission or operational readiness.
- **MAC III** - the loss of MAC III data would not have an immediate impact on the effectiveness of a mission or operational readiness.

**Maturity** - the risk associated with how well is the variable managed / resourced. High (risk) then is a weakly managed, supported or otherwise relatively adhoc state of the capability / process. Low (risk) is a well-integrated, adequately funded effort with few known critical risks / issues (also associated with a ‘commodity’ state). (note, this is an inverse relationship of sort, where the negative aspects of a variable are captured as high risk that then implies a low variable capability state, where the risk is greater of not performing the mission)

**Complexity** – the general state of the inter-relationships of the variable where the more types and versions of the variable generally adds risk. High (risk) infers a highly interdependent, tightly coupled, and numerous
connections / communications channels capability / process. Low (risk) is basically a commodity state with minimal I&I aspects, which are loosely coupled.

These three proposed coefficient values are principally to initially quantify the key areas of “MA” to focus targeted engineering support on; thus a notional representation, yet only ONE view of what matters most in MA. To help start the community discussions on the ‘crown jewels assessment (CJA)’ of MA and the critical choke or inflection points – which we know are dependent on the view of the stakeholder and the ownership therein. We propose ‘starting values’ of each variable to seed the discussions on relative weight of the coefficients.

+ For each variable we list any/ limitation / assumptions / measures, where the overall value = score = numbers for I, M, & C (initially we propose using H, M, & L risk values, of 9, 5 and 2 to gain an approximate score for discussion). (An arbitrary threshold of 200 was used to call out the more impactful variables – bolded below, with a potential high ‘2nd order’ effect those at/above 125 in risk value)

+ (a1) - Requirements – 125 = M x M x M.
  
  I = M. While the “ID” specific technical requirements are not flushed out, they depend mostly on existing IT / C4ISR capabilities that are reasonably well known, even as we transition to cloud, with services, these are well established in the commercial sector. Cyber is not as well quantified, but adequate. M = M. Mostly use known technologies, thus in general relatively mature, where the translation to common capabilities is weak (using APLs, etc to reduce complexity). C = M. DoN is working towards a global common enterprise ID architecture (IDEA), but there are still multiple EAs, with no enforcement of common standards, etc nor common V&V/ certification methods (iso IT TA).

+ (a2) – Cyber – 405 = H x H x M
  
  I = H. Lack of cyber protections in even one area can cascade and cause total loss of the major mission areas, and there are multiple threat vectors. M = H. IA/CND capabilities are generally adequate, but lack of security CM / hygiene and effective access control of the IT / cyber environment greatly increases the risk from all aspects. Inability to quantify / aggregate the many sources / impacts of risk. C = M. There are standard cyber capabilities to use (APLs, NIAP, etc), and there is a general defense in depth approach (with DFIA improving that), but there is little enforcement of APLs or using monitoring tools (e.g., SCM, SIEM, IPS, etc).

+ (a3) - “Ao” / RAM / resiliency - 225 = H x M x M
  
  I = H. Depending on criticality of capability (single point of failure, mission essential programs especially), the loss can cause total mission failure. M = M. Overall reliability factors are relatively well known, yet the complexity of SoS / I&I environments lowers the overall confidence level, from the unknown interfaces / data flows. C=M. The complexity of aggregating the overall Ao impact of various systems iso their mission impacts, where some capabilities are more important than others (the ‘crown jewels’) and the correlation of multiple data sources is fuzzy at best, causes at least a M risk level. (note – we think the “MFOM” model mentioned earlier is a great tool / method to assess / aggregate platform risks)

+ (a4) - Safety (hazmat, etc) – 36 = H x L x L.
  
  I = H. Inadequate levels can cause substantial loss of resources and loss of life, potential mission degradations. M = L. Safety is a well-known / practiced discipline, though weak in some areas, it has strong oversight. C = L. The program / system level of safety practice is well known, but the potential complexity of SoS systems, dependencies and aggregating safety issues is less clear.

+ (a5) - TE&C / IV&V – 125 = M x M x M
  
  I = M. Verification that capabilities work as required is a critical aspect of MA. TE&C processes are well established for the most part, but SoS aspects are still weak; thus the enterprise impacts of ineffective TE&C
could be significant on complex missions. M = M. The TE&C community understands the processes well, a mature process overall. Some areas like SoS, SW reliability / assurance, enterprise interface management, etc are weak – especially to aggregate to aggregate risks by platform / site. C = M. The TE&C / V&V process are well established, with significant leadership oversight, but the SoS / cyber aspects raise this is a "M"

+ (a6) – Quality – 20 = M x L x L
I=M. Poor quality can affect Ao / Cyber / I&I effects / etc. - especially wrt costing more in accounting for potential intermittent capability loss and increased sustainment costs. M = L. Well known processes, program requirements / assessments accounted for within ‘acquisition rigor.” C = L. Product QA processes are well known, implemented, but the SoS roll-up aspects are unclear, which could cause a “M” risk level.

+ (a7) - Environment / PESHE – 50 = M x L x M
I=M. Generally minimal direct mission impact, though clean up costs can be huge (re: nuclear power, hazardous metals in electronics). M = L. Well known processes, required part of acquisition rules. C = M. Individual program processes well established, unclear SoS aspects ads to potential complexity.

+ (a8) - Governance - (management / processes) – 125 = M x M x M
I = M. Many to many relationships, multiple regulations & statues, etc can cause delays and added costs, which could impact missions operational effectiveness. M = M. Enterprise R&R / swim lanes, agreement on critical priorities, etc… weak at best. Best practices are generally known, especially commercially, but not common nor enforced. C = M. Many ‘authoritative” entities in charge (federally and DoD), numerous overlapping (conflicting?) statutes, unsynchronized objectives (do more in security, but gain IT efficiencies too, etc).

+ (a9) - Mission criticality (overall operations utility / need) - 225 = H x M x M
The additive capability to key primary missions areas and the R&R / NTAs they include. The mission criticality variable should be directly related to the MEF / CJA of what capabilities matter most. I = H. Clearly a high mission critical capability must factor heavily into overall MA success, as the lack of it implies a higher risk. M=M. The platform primary (and secondary) mission areas are well known and fairly mature. Still in work is how they collectively relate to and support ID (the premise is that they do) and the I&I complexities of the IT/C4ISR suite. C=M. While individual program capabilities importance is relatively well know (MAC levels, etc), the aggregation risk of the many missions based on many intertwined capabilities is not well known. While there is always the system Ao/RaM aspect, there is also the “assured data” aspect that must be preserved to provide the decision superiority that ID mandates. The need to assess what data is more important, where it’s stored, the pedigree of the data, how it can be correlated with other sources, etc. make this aspect more complex.

+ (a10) – Policy – 50 = M x L x M.
I = M. Multiple policies exist for the C4ISR / IT / Cyber environment, most are high level and not ‘implementation centric” as needed – and minimal enforcement is applied. The impact to MA is generally added costs in rework after systems are developed. M = L. In general policy is well established, known overlaps, the issues are mostly in the governance arena. C = M. While the overall federal policy aspects / coverage are fairly mature, enforcement is weak, as is the SoS / I&I impacts and incorporation of new technologies (cloud / services, etc) ; thus adding to the complexity factor – as it’s unclear how changes in some policies affect others.

+ (a11) - Training / education – 90 = H x L x M
I = H. Clearly the ability / effectiveness by which operations can use and maintain essential capabilities is paramount, as improper settings can make those capabilities ineffective; thus operator / maintainer training is a critical aspect to account for, and a potential high risk. M = L. The training required is fairly well known, the WHAT to train on, especially for “commercial IT” capabilities - as this is a commodity, as well as most C4ISR
systems with many years of operation. Yet execution of the training and its effectiveness is weak. \( C = M \). Individual programs training methods are known, accommodated, but the training for I&I / SoS aspects of IT / C4ISR is weak at best, and typically few entities offer any sort of complex enterprise environment training.

6 – Recommendations

*We all need to collectively harmonize with the four main DoD MA principles first:*

* Prioritize missions, functions and supporting assets, and capabilities
  
  Mission critical assets – defense facilities, equipment, networks, information systems, and supporting infrastructure = Defense Critical Industry Program (DCIP) = crown jewels

* Develop and implement a comprehensive and integrated risk management framework
  
  Use common criteria for risk assessment and analysis with commonly accepted criteria for linking vulnerability and consequence information horizontally across components, installations, and programs and vertically from the tactical to strategic levels = RMF

* Use risk-informed decision making to optimize mitigation solutions
  
  MA advocacy framework that brings together those responsible for executing mission essential functions and those for the security and resilience of critical assets and systems

* Partner to reduce risk
  
  with other government organizations, foreign governments, and the private sector to share threat and vulnerability information and risk mitigation efforts = CIP

So we propose the SYSCOM / organization’s next steps are:

* Quantify the key technical capabilities iso ID vision / three operational vectors.. and then distill that into an enterprise ‘crown jewels’ assessment – CJA - what really matters to mission execution (as not all capabilities have critical mission impacts, acknowledging that starting with the mission essential / MAC one programs- especially the ‘single point of mission failure’ aspects – as the likely focal points in the CJA

* Collectively define, then prioritize the key / most impactful variables for MA, align them to the ID key factors – all integrated into a value proposition for MA

* Synchronize the various risk management plans / approaches for the enterprise – focus on items that have the highest risk reduction for the most affordable costs (RoI / value)

* Align MA/Cert directorate resources / processes to support the key ID needs – ensure they are harmonized to maximize capability delivery effects, while minimizing resources. DO this within the SYSCOM claimancy and cross-SYSCOM ‘platform wholeness’ efforts.

* Align all MA activities / processes into direct IT TA support objectives (within a POA&M and integrated WBS). Additionally, ensure the SoS / I&I aspects are covered in all TE&C / Cyber activities, as well as reducing resources and gaining efficiencies throughout the C4ISR suite life-cycle.

7 - References / Bibliographies

- DoD MA strategy guide (2012)
- DoD 8500-series of policies has three defined mission assurance categories that form the basis for availability and integrity requirements. A Mission Assurance Category (MAC) is assigned to all DoD systems (1 – 3) (related to ‘crown jewels’ assessment – key systems)
Homeland Security Presidential Directive 20 (HSPD 20), DCIP, etc.
DoD Strategy for homeland defense and defense of civil authorities (2012-2020)
NASA's Process Based Mission Assurance Knowledge Based System

- DISA MA (likely the JIE effort syncs to this approach )
http://www.disa.mil/About/Our-Organization-Structure/PEO-MA
- SEI / CMU "Mission Assurance Analysis Protocol (MAAP): Assessing Risk in Complex Environments"
http://www.sei.cmu.edu/reports/05tn032.pdf
- The Science of Mission Assurance
- Mission Assurance: Issues and Challenges
- Systems Assurance – Delivering Mission Success in the Face of Developing Threats
An Integrative Framework for Secure and Resilient Mission Assurance
Cyber Mission Assurance

Other references / perspectives:
http://en.wikipedia.org/wiki/Mission_assurance
http://www.aero.org/publications/crosslink/fall2007/03.html
Achieving Mission Assurance: The migration of technology to software-intensive system implementations
Mission Assurance Standards
An article on the "Mission Assurance Moves to the Fore in Cyberspace" By Linton Wells II (Deputy SecDef)
http://www.afeea.org/signal/articles/templates/Signal_Article_Template.asp?articleid=2416&zoneid=200
http://www.prtm.com/uploadedFiles/Strategic_Viewpoint/Articles/Article_Content/PRTM_The_Need.pdf
A great whitepaper on how SW assurance = MA overall using the stuxnet virus as an example....
SANDIA Labs 'Using a Risk Based Approach for Mission Assurance' http://energy.sandia.gov/?page_id=4008

Cyber and MA... Cybersecurity must start with mission assurance
IA categories = "MAC"= MA Category, in C&A so good to know / relate to that...
another paper on cyber MA.. as SECURITY is a major aspect of overall MA...
recent conference on MA and IA, get / use the briefs..
Cyber Resiliency Metrics
https://register.mitre.org/sr/12_2226.pdf
Mission Assurance is a full life-cycle engineering process to identify and mitigate design, production, test, and field support deficiencies of mission success. Mission Assurance includes the disciplined application of system engineering, risk management, quality, and management principles to achieve success of a design, development, testing, deployment, and operations process. Mission Assurance's ideal is achieving 100% customer success every time. Mission Assurance reaches across the enterprise, supply base, business partners, and customer base to enable customer success. The ultimate goal of Mission Assurance is to create a state of resilience that supports the continuation of an agency's critical business processes and protects its employees, assets, services, and functions. Mission Assurance addresses risks in a uniform and systematic manner across the entire enterprise. Mission Assurance is an emerging cross-functional discipline that demands its contributors (project management, governance, system architecture, design, development, integration, testing, and operations) provide and guarantee their combined performance in use.

DODI 8500.1 & .2 series (Security Requirements for Automated Information. Systems)
8500-series of policies has three defined mission assurance categories that form the basis for availability and integrity requirements. A Mission Assurance Category (MAC) is assigned to all DoD systems. It reflects the importance of an information system for the successful completion of a DoD mission. It also determines the requirements for availability and integrity.
MAC I systems handle information vital to the operational readiness or effectiveness of deployed or contingency forces. Because the loss of MAC I data would cause severe damage to the successful completion of a DoD mission, MAC I systems must maintain the highest levels of both integrity and availability and use the most rigorous measure of protection.
MAC II systems handle information important to the support of deployed and contingency forces. The loss of MAC II systems could have a significant negative impact on the success of the mission or operational readiness. The loss of integrity of MAC II data is unacceptable; therefore MAC II systems must maintain the highest level of integrity. The loss of availability of MAC II data can be tolerated only for a short period of time, so MAC II systems must maintain a medium level of availability. MAC II systems require protective measures above industry best practices to ensure adequate integrity and availability of data.
MAC III systems handle information that is necessary for day-to-day operations, but not directly related to the support of deployed or contingency forces. The loss of MAC III data would not have an immediate impact on the effectiveness of a mission or operational readiness. Since the loss of MAC III data would not have a significant impact on mission effectiveness or operational readiness in the short term, MAC III systems are required to maintain basic levels of integrity and availability. MAC III systems must be protected by measures considered as industry best practices.

MITRE - a principal responsibility of a commander is to assure mission execution in a timely manner.
Mission Assurance includes the disciplined application of system engineering, risk management, quality, and management principles to achieve success of a design, development, testing, deployment, and operations process. Mission Assurance reaches across the enterprise, supply base, business partners, and customer base to enable customer success.
http://www.mitre.org/work/systems_engineering/guide/enterprise_engineering/se_for_mission_assurance/
MITRE - Definition: Mission Assurance (MA) is the ability of operators to achieve their mission, continue critical processes, and protect people and assets in the face of internal and external attack (both physical and
cyber), unforeseen environmental or operational changes, and system malfunctions. Systems engineering for mission assurance is the art of engineering into systems: (1) the capabilities for operators to be aware of different and changing adversarial strategies as well as environmental and system conditions, (2) options and alternatives to accomplish a mission under different circumstances, (3) tools to assess and balance advantages and risks of available response options and alternatives, and (4) the ability to transition to a selected option while simultaneously continuing the mission. Systems engineering for mission assurance extends throughout the entire traditional acquisition life cycle, from concept development through deployment and beyond, to include supply chain considerations and field operations.

MITRE - Mission Not Impossible: Defending IT Systems Through Mission Assurance
http://www.mitre.org/news/digest/defense_intelligence/05_10/itdefense.html

The growing threat has led to increased focus on a strategy known as "mission assurance"—the ability to ensure that an organization's IT systems will support the mission in the face of different threats. "There are many threats to systems other than conventional hacker attacks, and so we're trying to broaden the definition," says Lou Montella, division engineer for mission assurance in MITRE's Information Security division. Indeed, the threat can come in many forms: organized crime, nation states, hackers, and other offenders. In addition to developing mission assurance techniques that will defeat these adversaries, a new area of focus is on developing techniques to provide assurance that IT systems meet mission needs, even when they have been compromised… and MORE…


Context --- The concept of engineering a system that can withstand purposeful or accidental failure or environmental changes has a long history in the discipline of designing systems for survivability. In the Cold War era, designing for survivability meant nuclear hardening of command centers, creating alternate command centers, engineering electronic countermeasures into communications and sensor systems, building redundant backup components, and engineering fallback modes of operation and switchover capabilities among them. More recently, the notion of engineering for mission assurance has been extended to ensuring the ability to effectively operate at the “tactical edge” in an environment with limited, austere, or intermittent communications, by selecting from a variety of communications options in the event that primary means become inoperable. Designing communications systems for survivability meant redundant communications links and factoring in potential adversary actions such as electronic warfare. Although all these are still needed in the Internet era, engineering systems for mission assurance has been further expanded to include engineering for information assurance and cyber security.

In recent years, cyber threats have become the predominant focus of mission assurance. Some worry that such intense focus on “all things cyber” risks losing sight of other dimensions of mission assurance. Others see a tension or conflict between mission assurance’s “get the operational job done” ideal of achieving 100 percent mission success every time and the security-focused aims of information assurance, which could at times constrain aspects of operations in order to protect data and systems. Yet others are concerned that the acquisition community does not have a sufficiently mature mission assurance culture or mindset and that we are not yet sufficiently attuned to mission assurance as an “implicit requirement” that needs to be considered for all systems, whether or not it is explicitly demanded.
So what about “SoS” and I&I”
Of course - but what are they exactly? We need to quantify them to best assess and support them in MA. We
offer a couple of pictures to consider… First what is “information dominance (ID) – where SOS/I&I are major
factors in our complex, shared IT/network environment. The following illustrations are offered to show the breadth
of the ID perspective, yet focus on the three pillars of it, translating the operational tenets therein, into
functional / technical requirements to work within MA.

What is ID?
(beginning with the vision, distill the requirements)

The WHAT is...
‘As WE are to move boldly:
• From Platform-Centric to Information-Centric processes
• Into Unmanned, machine autonomous technologies
• Creating a Fully-Integrated “C4ISR” - Intel, C2, Cyber & Networks Capability’

To rephrase... ID is a construct that supports ‘decision superiority’ throughout the life-cycle of key information elements (knowledge) within the warfighter triad phase of major capabilities - Sea Strike, Sea Shield and Sea Basing.

THEN all these are translated into the decision superiority “operational needs”

*** Provide the Right DATA/Info, at the Right Time, in the Right Place and to the Right entity (and only to them) = Information Environment ***

What are the specific ID requirements to accommodate?

Information Dominance - CV-1 Version 1.0
“ID” CNO ‘operational’ objectives = Assured Command and Control, Battlespace Awareness, and Integrated Fires, as sets forth the following major goals for the 2013–2017 timeframe:

- Strong and Secure Navy Command and Control;
- Persistent, Predictive Battlespace Awareness;
- Integrated Combat Information;
- Integrated Kinetic and Non-kinetic Fires;
- Information Dominance as a Warfighting Discipline.

**Assured C2.** The Navy must assure its ability to command and control forces. This requires capabilities that enable commanders to:

- Exchange orders and responses with subordinates;
- Understand the disposition of friendly forces;
- Target and conduct strikes as part of the joint force; and then
- Assess the result of those strikes.

**Battlespace Awareness.** This is the traditional mission of the Information Dominance Corps and the constituent components of meteorology, oceanography, intelligence, cryptology, communications, networks, space and electronic warfare (EW). It includes:

- Persistent surveillance of the maritime and information battlespace;
- Penetrating knowledge of the capabilities and intent of our adversaries;
- An understanding of when, where, and how our adversaries operate; and
- Expertise within the electromagnetic spectrum.

**Integrated Fires.** The Navy will use its networks, cyberspace and space capabilities to exploit and attack the vulnerabilities of its adversaries to achieve non-kinetic effects (i.e., fires). Just as importantly, we will expand options for forward-deployed Navy commanders by ensuring that non-kinetic alternatives are considered alongside with kinetic solutions.

---

### Capabilities Needed for “Information dominance”

- **Schema of maneuver** (positioning for effect)
- **Assured C2** (OPCON / INFOCON)
- **Cyber** (IA/CND protections & CNE/CNA (covert))
- **Kill / Effect Chains** (maximize left side - ISR / I&W)

**“ID” = Decision superiority**

- **“Knowledge”**
  - Quality / assured data = value, pedigree, provenance
  - Information environment
    - WAN/transport, network, cloud,
    - Infrastructure / services / apps
    - Trusted Information Systems

**“IT / network”**

Battlefield victory requires dominant position and maneuver

Which require best possible information, before the opposition can: (1) get his own information; (2) react to your movements or (3) infiltrate your environment...

**The best possible info is ID:**

- A DiD with trusted information systems providing assured / quality data, facilitating all levels of command decision superiority
CNO's Unifying Vision and Guiding Principles

(we start with the boss’ direction = ‘operational’ requirements)

**First Principles Include:**

- Every platform is a sensor
- Every sensor is networked
- Build a little; test a lot
- Spiral development/acquisition
- Plug-n-play sensor payloads
- Reduce afloat/airborne manning
- Transition to remoted, automated
- Collectors dynamically tasked

*How will MA distill these into technical regs and support them? *

---

**SoS / I&I relationships / parts**

OUR Systems of Systems (SoS) “ID” environment is all about the key interfaces and controlling parameters, that must be integrated and interoperable (I&I)

**ID ‘technical’ vision (proposed)**

“Deliver an integrated, “best value” C4ISR suite that enhances the operational ID vision, decision superiority, providing quality/assured data between trusted entities - seamlessly and with minimal impacts and maximum resiliency to all users, at a lowest TOC – leveraging COTS / common capabilities, best practices, and building in SoS/I&I methods – all securely.”

**Generalized enterprise SoS/I&I factors = COMPLEXITY!**

<table>
<thead>
<tr>
<th>Governance</th>
<th>Mission Assurance</th>
<th>Resiliency / Ao reconstitution</th>
<th>Warfighter effects</th>
</tr>
</thead>
<tbody>
<tr>
<td>SoS SysEng</td>
<td>Cyber Security</td>
<td></td>
<td>Kill / Effects chain</td>
</tr>
<tr>
<td>E2E data strategy</td>
<td>DOTMLPF / ILS Sustainment / HSI</td>
<td>TRUST TE&amp;C IV&amp;V</td>
<td>Efficiency &amp; Affordability</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Transparent coalition</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Public / private interaction</td>
</tr>
</tbody>
</table>

The **MA life-cycle must account for all of these SoS / data ‘requirements’ (variables)**
Epilogue - Other MA articles Under This Topic

The articles under this topic are focused on what we know today about SE for mission assurance. Cyber Mission Assurance structures the cyber response discussion around the notion of a system architecture that is resilient in the face of different levels of cyber threat. The article focuses on near-term actions, rooted in actual experience, to begin evolving architectures that reduce their attack surface and are more secure, resilient, understandable, agile, and manageable.

There are several elements of the mission assurance engineering (MAE) process. Crown Jewels Analysis (CJA) is a methodology that helps identify the cyber assets most critical to mission accomplishment—the “crown jewels” of a crown jewel analysis—and that begins during system development and continues through deployment. Cyber Threat Susceptibility Assessment (TSA) helps understand the threats and associated risks to those assets. Cyber Risk Remediation Analysis (RRA) is used to identify and select mitigation measures to prevent or fight through cyber-attacks.

Secure Code Review provides an overview of the specialized task of automatically or manually reviewing security-related weaknesses of an application’s source code to understand what classes of security issues are present. The goal of a secure code review is to arm the systems engineer and code developer with information to make an application’s source code more sound and secure.

Supply Chain Risk Management discusses the threats to and vulnerabilities of commercially acquired information and communications technologies that government information and weapon systems use. It discusses how to minimize the risk to systems and their components from sources that are not trusted or identifiable, or that provide inferior materials or parts.

References & Resources

Gupta, Rahul, 2006, The Need for Mission Assurance, PRTM.

A Realistic View

"Our job is to make things harder for our adversaries, but also to assume that we can't prevent every attack," Montella says. "That means we have to develop the ability to fight through an attack because we can't assume we can keep the enemy out. Mission assurance means ensuring that your systems will work in the face of a variety of different threats."

Montella is currently working with sponsors in the acquisition community to address a wider range of threats and to influence government policy at a higher level. "One thing we're discussing is how to incorporate that broader definition into the systems engineering activities we do," he says.

Foote reiterates the value of a systems engineering risk management approach. "MITRE is well known for systems engineering competencies in a wide range of technologies and engineering methodologies," he says. "If we approach mission assurance as a systems engineering set of challenges, we can bring it forward in that context. Most other organizations can't offer that."

This approach is nothing new, according to Foote. "We have a tendency to treat mission assurance as though it's a new topic or new set of challenges, when it's always been an objective of traditional systems engineering," he says. "Mission assurance is not in and of itself a deliverable."