

SowellEAC



**National-Louis
University**
Center for Continuing Education

The Black Belt Enterprise Architect Certification Program



Don Zugby, Principal Instructor

Custom Enterprise Solutions, LLC

www.sowelleac.com

(703) 620-0639

The **Sowell/EAC** Black Belt EA Certification Program

- **Approach**
 - Continues the philosophy of the **Sowell/EAC** Basic EA Certification Program
 - Exploits the core EA products and their interrelationships by applying proven analytical techniques to flesh out issues, improvement opportunities, and pragmatic transition strategies
- **Method of Delivery**
 - A mix of lecture, demonstrations, case examples, and class participation, assignments, and examinations
 - Mr. Zugby and Ms Sowell are present throughout all sessions to ensure consistent tie-ins to the core EA products
- **Program Duration**
 - Five + one full classroom days
 - Because of the breadth and depth of material covered, advisably spread over a two-week period to allow time for students to “digest and rest” between sessions, and to complete assignments
 - 10 half-day training sessions, plus ...
 - One full day for final exam and student presentations of projects
- **Formal Recognition**
 - Certification as a Black Belt Enterprise Architect, and Continuing Education Units (CEUs) conferred by National-Louis University

What is the **Sowell/EAC** Black Belt Enterprise Architect Certification Program?

- Picks up from where basic EA certification programs leave off
- Teaches students how to assess architectures systematically
- Sharpens students' analytical awareness and insights
- Exposes students to unique and proven analytical constructs and methods developed and applied by Mr. Zugby to bridge architectures effectively to Enterprise strategic planning and systems engineering activities in Government and Industry
- Enables students to transform “static” architectures into definitive, defensible, and actionable assessments and transition strategies that are presentable to executives and engineers alike

Is the *only* available and established formal certification program that provides in-depth coverage of the **Functions**, **Knowledge**, and **Skills** identified in the **OSD NII Proposed Requirements for Architecture Analysts**

Coverage of the OSD NII Proposed Requirements for Architecture Analysts

OSD NII-identified *Functions (F), Knowledge (K), & Skills (S)*

- (F) Ensure that the development of architectures supports federation*
- (K) Architecture federation*
- (K) Mission thread analysis*

EA analysis case examples are discussed which demonstrate segmented architectures of mission threads and selected operational scenarios.

- (F) Perform analyses to identify gaps, redundancies, areas of improvement*
- (S) Gap & redundancy analysis*
- (S) Process improvement analysis*

Students are taught in the use of capability progression models (CPMs) of IT-related processes, EA services, and EA infrastructure to assess gaps and issues. Students use CPMs, interoperability frameworks, and threat mitigation matrices to determine specific types and levels of capability needed for EA improvement.

- (F) Develop as-is to to-be architecture transition & sequencing plans*

Students use applicable CPMs and other analytical aids to derive capability-driven EA transition stages.

Coverage of the OSD NII Proposed Requirements for Architecture Analysts [continued]

OSD NII-identified *Functions (F), Knowledge (K), & Skills (S)*

- (F) Perform architecture analyses to identify cost-benefits, performance issues, & risk*
- (S) Cost-benefit analysis*
- (S) Performance analysis*
- (S) Risk analysis*

Students use detailed capability models and model drill-downs to determine benefits versus implied cost trade-offs, including potential schedule risk.

Students are given case examples and guidance to apply to EA process and systems performance analysis.

- (F) Ensure that the development of architectures is compliant with overarching policies and guidance*
- (K) Overarching policies and guidance (e.g., FEA, EAMNF, GIG policies, DARS policies, net-centric strategies, etc.)*

The analytical techniques and guidance given during the program are fully compatible with prevailing DoD and Federal EA frameworks, and are presented in that context.

Direct linkages to the DoDAF, FEA reference models, and GIG/NCES strategies are incorporated into the course material.

Coverage of the OSD NII Proposed Requirements for Architecture Analysts [continued]

OSD NII-identified *Functions (F), Knowledge (K), & Skills (S)*

- (F) Ensure that the development of architectures supports the key decision processes of the organization*
- (K) Architecture elements of key decision processes (e.g., JCIDS, DAS, PPBE, ...)*

Students are given insights into the decision processes and process interrelationships that are pertinent to EA analysis, and are taught where specific enterprise policies and standards are tied to capability improvements.

- (F) Provide interoperability solutions to clients/customers*
- (K) Interoperability standards*

Students are tutored in the structured and systematic analysis of systems interoperability, using of the LISI reference model and various analytical techniques and net-centric extensions.

- (K) IT investment management*

Investment management is one of the processes that is examined early in the program, especially as it is affected by EA analysis.

The CPM drill-downs show the students how to map related community programs to progressive capability levels, thus providing investment management with viable leveraging options.

Coverage of the OSD NII Proposed Requirements for Architecture Analysts [concluded]

OSD NII-identified *Functions (F), Knowledge (K), & Skills (S)*

- (K) Various tools and tool suites*

Students are given significant exposure to capability progression models and their use in EA analysis as vehicles for assessing gaps and shortfalls, and for identifying incremental capability improvements.

Students are exposed to LISI as a comprehensive vehicle for assessing systems interoperability.

- (F) Deliver and present architectural analyses results and supporting architecture products to clients/customers and senior-level decision makers*

Students are presented with numerous case examples of a variety of ways for packaging and presenting EA analysis findings across a range of clients and their interests.

More than one segment of the program is purposely focused on the roll-up of architecture findings for presentation to senior-level decision makers.



Who is the Instructor of our Advanced Black Belt EA Certification Program?

Donald E. Zugby

- Director of Advanced EA Programs, Custom Enterprise Solutions, LLC
- Formerly Department Head and Senior Principal Engineer for the MITRE Corporation
- Developer of *Capability Progression Modeling*™ discipline and comprehensive IT-related models and drill-downs
- Initial Developer of the *Levels of Information Systems Interoperability*® (LISI) Reference Model and analytical process
- 30+ years of systems engineering and applied expertise in Enterprise Architecture development, analysis, and acquisition

Supporting Instructor: **P. Kathie Sowell**

On-call Experts (Current MITRE Program Managers):

Bruce Thompson, Program Management, Interoperability & LISI Guru

Dave Robbins, EA Development, Analysis, & EA Presentation Techniques

Black Belt Students are Taught EA Analysis Systematically

- Often, an EA or an EA segment is developed and/or scrutinized with a specific analytical purpose; e.g.,
 - What's our vulnerability to cyber threats?*
 - How interoperable are our systems?*
 - How should we streamline our business process?*
- Other times, an EA is developed and/or analyzed with the intent of conducting a comprehensive assessment of business operations and systems support
- In these cases, a logical “pecking order” or deliberate sequence of analyses makes sense to ensure that the high ground is covered before diving into the weeds
 - For example, *you might first want to know if the car runs before your interest turns to the status of the tire treads!*
 - Or, *you might first want to know if you have connectivity with your information source before you start worrying about information formats or streaming video!*

Key EA Analyses Addressed in the SowellEAC Black Belt Program

EA Business View
 (Who, what, where, when, why)

What required vs. existing **Activities & Functional Capability Levels?**

What required vs. existing **Enterprise Services and Capability Levels?**

What **Information Exchanges & Levels of Interoperability** are required ?

What **Performance** required? **Timeliness? Accuracy?**

What **Security Domains & SCI Conditions** apply ?

What **Potential Threats & Risks** apply ?

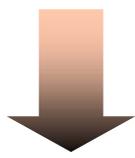


EA Systems View
 (Resources, infrastructure)

What **Enabling Systems** or **technologies** are used? What **Enterprise Service Applications** are provided? Are the current **Levels of Capability** adequate? What **levels** of what **capabilities** are provided?

What **Systems Interoperability Levels** are achievable? What **Performance** achievable? Is **Requisite Information** Accessible? **If Net-Centric operations**, can users fully interconnect and exploit?

What **Security Barriers** exist? **Resolvable? What Threat-mitigation Capabilities** exist? **Reasonable Counter-threat Assurance?**



Design Rules & Considerations

What **Technologies** and/or **Implementation Standards** might apply?

Related program to leverage? Off the shelf capability? Adaptation or Piloting needed? **R&D** required? Enterprise **Policy** changes required?

How should we systematically progress to where we need to be?

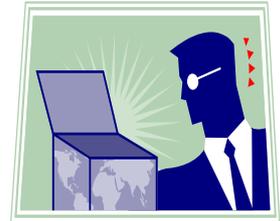
How the Black Belt Curriculum is Organized

SowellEAC Black Belt Module	Theme	Topics Covered	Half-day Program Sessions
BB 201	Setting the Stage for the Practice of EA Analysis	<ul style="list-style-type: none"> • Program objectives, content, and context • Coverage of OSD NII Requirements • Typical EA analysis sequence 	1
BB 202	Capability Progression Modeling (CPM)TM	<ul style="list-style-type: none"> • CPM context and components • CPM development & EA relationships • Example CPM models (CIO context) 	2-4
BB 203	Use of CPMs in EA Analysis	<ul style="list-style-type: none"> • Business Process & Capability Sufficiency analysis using CPMs 	5
BB 204	EA Systems Interoperability Analysis	<ul style="list-style-type: none"> • Interoperability Analysis: Dimensions & Constructs • Levels of Systems Interoperability • EA analysis using the LISI RM • LISI & EA Frameworks 	6-8
BB 205	EA Analysis Extensions & Presentation Techniques	<ul style="list-style-type: none"> • Analysis in a net-centric environment • Threats and mitigation assessments • Performance analysis • Executive-level roll-ups of analyses 	9-10
	Final Review and Presentations	<ul style="list-style-type: none"> • Class summarizations, presentations, & final examination 	Final Full Day

A Brief Intro to Some Unique Analytical Methods Covered in the Black Belt Program

- **Use of Capability Progression Modeling™ and Model Drill-downs**
- **Interoperability Analysis Using LISI**
- **Analysis of Threats & Countermeasures**

So, How Did this “CPM” Discipline Come About?



Carnegie-Mellon

Pre-CY 2000

IEEE SEI Capability Maturity Model (CMM)
 [Software development]

CY 2001

Capability Maturity Model Integration (CMMI)
 [Adaptation of CMM to IT processes & organizations]

CES Principal*

Levels of Information Systems Interoperability (LISI)
 [Systems interoperability improvement]

Pre-CY 2000

IC CIO IT Roadmap
 [Adaptation of SEI CMM to IT systems]

CY 2000

CPMs & Extensions
 [Drill-down of models for application to strategic planning, systems engineering, and program management]

CY 2003+

* While Department Head at MITRE

What is a Capability Progression Model?

- **A sound capability progression model represents increasing levels of operational capability**
 - Clear and demonstrable capability or utility thresholds
 - A script for systematic evolution
 - Applies to Enterprise processes, services, and products
- **Capability progression models provide an excellent basis for assessing the existence and sufficiency of the processes, products, and services represented in the architecture**
- **A particular capability progression level is, in itself, a discernible (*ordinal*) measure of performance or success**

What is a CPM Framework?

A CPM Framework identifies and structures the set of capability components that capture the main thrusts of an enterprise

- **The primary services or products that the enterprise is charged to provide its clients or users**
- **The strategic and tactical processes that are focused on identifying, planning, budgeting, engineering, and implementing the services or products to be provided**
- **Any other capabilities that support or enable the primary services or products**

A CIO-Oriented CPM Framework and Components



Strategic Planning & Oversight Processes

Governance & Policy

Enterprise Architecture

Strategic Planning

Investment Planning

IT Competency

Customer Relations

IT-enabled Enterprise Capabilities

Enterprise Services

Authentication, Authorization & Audit

Subscription and Delivery

Search

Collaboration

Business Intelligence Reporting

Workflow Management

IT Service Infrastructure

Domain Networks

Directory Services

Information Storage

Enterprise Portal

Tactical Processes

Technology Evaluation

Prototyping & Piloting

Systems Engineering & Integration

Data Engineering & Integration

Certification & Acceptance Testing*

Infrastructure Management

Information Management

Each Component is Modeled IAW a Normalized Discipline in Terms of Attributes and Attribute Change States

Capability Progression Levels*	CPM Attributes				
	Policy & Outreach	Standardization & Facilitation	Oversight & Control	Performance Measurement	Capability Sophistication & Flexibility
5 Optimizing	<i>Use extended to business partners & clients</i>	<i>Enterprise influential in global standards community</i>	<i>Coordinated & dovetailed with Enterprise partners</i>	<i>Performance mapped to Enterprise-level goals</i>	<i>Enterprise capability a model of best practices globally</i>
4 Quantitatively Managed	<i>Integral part of the way of doing business</i>	<i>Standards dynamically updated to track industry trends</i>	<i>Controlled at Enterprise level</i>	<i>Integral to business intelligence reporting</i>	<i>Refined, modular, highly flexible, re-usable, and expandable</i>
3 Defined	<i>Institutionalized across Enterprise</i>	<i>Enterprise-wide standards & common tools in use</i>	<i>Coordinated across the Enterprise</i>	<i>Common measures applied across Enterprise</i>	<i>Complete and applied to complex problems at Enterprise level</i>
2 Managed	<i>Used by several interest groups</i>	<i>Uniform within interest groups</i>	<i>Controlled within interest groups</i>	<i>Unique measures applied by individual interest groups</i>	<i>Applied to fairly complex problems at local levels</i>
1 Performed	<i>Used in one area or line of business</i>	<i>No uniformity nor automated aids</i>	<i>Not controlled</i>	<i>No performance measurement</i>	<i>Rudimentary & incomplete</i>

* Consistent with the *Capability Maturity Model Integration (CMMI)®* standard developed at Carnegie-Mellon University for maturing IT-related organizations and processes

Utility of CPMs to Strategic Planning

The collective set of specific Enterprise CPMs facilitates profiling an EA's "to-be" capability priorities, tradeoffs, and strategic plan

IT Service Infrastructure
Enterprise Portal Capability Levels

5 <i>Optimizing</i> <i>f(t)</i>	FBI enterprise, partner organizations, and mission customers access common portal as a staging point for information sharing, directory services, collaboration, and launch point for investigative and analytic tools, using common look and feel and user profiles. Applications accessible by the portal within and outside of the enterprise dynamically share context providing a composite view on any topic.
4 <i>Quantitatively Managed</i>	FBI enterprise-wide users access common portal as a staging point for information sharing, directory services, knowledge management and collaboration services, and launch point for investigative and analytic tools, using common look and user profiles. Applications accessible by the portal dynamically share context providing a composite view on any topic.
3 <i>Defined</i>	FBI shared interest groups use common portals as a staging point for information sharing, directory services, knowledge management, collaboration, and launch point for investigative and analytic tools, using common look and user profiles.
2 <i>Managed</i>	several topic and mission-specific portals, with each portal using different standards, authentication, and navigation model
1 <i>Performed</i>	FBI users access applications and information through separate interfaces, each with its own look and navigation model

Knowledge Management Services
Authentication, Authorization & Audit Capability Levels

5 <i>Optimizing</i> <i>f(t)</i>	FBI's PKI is interoperable with the enterprise's mission partners' PKIs and IAM solutions. Authorization is greatly enhanced due to structuring of new data stores and information products, with need-to-know attribute tags applied to data within provisioning services, and select use of biometrics now greatly enhance the extensibility due to IAM services, robust directory services, multipurpose certificates, proxy delegation, and scalable biometrics.
4 <i>Quantitatively Managed</i>	Dynamic authorization is improved based on increased use of need-to-know, privilege management, and attribute tagging at the data level. CAC, single sign-on, provisioning services, and select use of biometrics now greatly enhance the authentication and authorization process. Automated audit capabilities are in place and integrated with Security Information Management System (SIMS).
3 <i>Defined</i>	PKI applications are extended to web services, VPNs, files transfer, e-Gov, database applications, et al. CAC deployment complete. Based on established access control policy and leveraging the power of rich directory services, clearance repositories, and IAM components automated and dynamic authorization services based on policy-defined user roles and other user attributes are in place with the enterprise information portal. Audit policy is being formulated.
2 <i>Managed</i>	An enterprise PKI is in place, with limited application to FBI interest groups and secure mail. Initial rollout of PKI Common Access Card (CAC) used to store PKI credentials and for facility access. Though enterprise access control policy has not yet been established, steps are underway to investigate dynamic authorization and user provisioning services and the potential of leveraging solutions being pursued by the community, including consideration of COTS IAM products.
1 <i>Performed</i>	Efforts are underway to investigate options for an enterprise public key infrastructure (PKI) for user I&A and facility access. Authorization is a static process, limited to hard-copy access control lists. Audit is non-existent.

Knowledge Management Services
Search Capability Levels

5 <i>Optimizing</i> <i>f(t)</i>	FBI users and applications, partners, and customers can conduct robust search and access of global, secure, multimedia, multi-lingual repositories through the agency portal which utilizes automated agents for search initiation and interpretation.
4 <i>Quantitatively Managed</i>	FBI users, with authorized applications and dynamically-determined need-to-know, can search and access via the agency portal multi-lingual, multi-lingual repositories across the enterprise utilizing automated agents for search initiation and interpretation.
3 <i>Defined</i>	FBI users with need-to-know and authorized applications can search and access all enterprise multi-media repositories via a common intranet and the "one-stop-shop" portal, and can utilize some automated aids for interpreting results.
2 <i>Managed</i>	FBI users with established need-to-know can search and access multiple textual repositories with a single text query that are on a common intranet accessible via the FBI portal.
1 <i>Performed</i>	FBI users can search and access their own individual text repositories with simple text queries provided that they are on a network and are on the ACLs.

IT Service Infrastructure
Information Storage & Management Capability Levels

5 <i>Optimizing</i> <i>f(t)</i>	FBI enterprise and its information space able to securely and reliably interact with information resources maintained by other enterprises to agilely provide all-source information to enterprise users and mission partners
4 <i>Quantitatively Managed</i>	Enterprise-wide, secure, reliable, shared multi-media information space that facilitates agile associations and the real-time presentation of information in the context and format desired
3 <i>Defined</i>	FBI cross-interest-group secure, multi-media information repositories maintained using common standards and rules that incorporate pre-defined associations and presentation formats
2 <i>Managed</i>	Enterprise interest groups maintain multi-media information repositories using a defined interoperable set of standards, rules, and facilitators
1 <i>Performed</i>	Individual hardcopy and electronic textual information repositories maintained using a mix of non-interoperable standards, rules, and facilitators

Knowledge Management Services
Subscription & Delivery Capability Levels

5 <i>Optimizing</i> <i>f(t)</i>	FBI users, global partners, and mission partners are provided with timely, reliable, secure, adaptive, and integrated information across enterprise domains. Active profiling capabilities and need-to-know attributes are maintained for individuals as well as cross-domain interest groups or communities of interest (COIs).
4 <i>Quantitatively Managed</i>	FBI users are provided with timely, reliable, secure, adaptive, and integrated information across the enterprise based on agile, active profiling capabilities, direct requests, dynamic need-to-know correspondence between user attributes and data-release tags ("smart push"), efficient management of information provisioning, and quick response to feedback, including new information.
3 <i>Defined</i>	FBI users are provided with pertinent information across interest groups through the agency portal that responds to dynamic requests and that also delivers content based user interest profiles. Management of dissemination and collaboration techniques is executed efficiently, and timely feedback and response mechanisms are in place.
2 <i>Managed</i>	FBI users within interest groups submit requests to a portal that acts as a transparent gateway between the users and the distributed repositories. Responses to the request are fed back to the users through the portal provided that the users are on the data owners' ACLs.
1 <i>Performed</i>	Individuals within the agency submit requests to data repositories with which they are familiar and have connectivity. Responses are provided if they are on the data owners' access control lists (ACLs).

Knowledge Management Services
Business Intelligence Reporting Capability Levels

5 <i>Optimized</i> <i>f(t)</i>	BI is delivering significant business value. BI is refined to best practices based on the results of continuous improvement and benchmarking with other organizations. At the strategic level, BI is aligned with multiple mission-oriented processes through integrated performance management and analysis. At the tactical level, FBI is capable of identifying trends, anomalies, and behaviors that need management action. The enterprise data warehouse serves as a strategic enterprise resource for integrating data and supporting mission-critical applications that drive FBI's operations. A strong stewardship program is employed, and FBI deploys cascading scorecards or dashboard overlays to align every worker and business process with corporate strategy.
4 <i>Quantifiably Managed</i>	BI can be monitored and measured against compliance with procedures, and alerts regarding processes requiring action are provided. FBI departmental data marts are standardized, possibly through the creation of central data warehouses wherein logical data marts run in the same database as the data warehouse (i.e., a hub and spoke data warehouse). Users can submit queries across functional boundaries. Deployed dash-boarding applications enable improved monitoring of cross-departmental processes and enterprise value chains and provide executives with a tactical way to improve process efficiency and to empower more users with information that supports fact-based decision making.
3 <i>Defined</i>	BI procedures and processes are documented and communicated through training. End users are educated on the availability, value, and accuracy of data. FBI Divisions empower all their knowledge workers with timely information and insight through the implementation of online reporting. Though still limited in scope to single application areas, knowledge workers are provided with a shared analytic structure tailored to meet the needs of the departmental
2 <i>Managed</i>	Spreadsheets or desktop databases are in wide use within FBI Sections or lines of business and serve as surrogate data marts. These BI capabilities offer high local control, but are limited in scope and value to executive and business analyst oversight of single lines of business. Processes have developed to the stage where similar procedures are followed by different interest groups.
1 <i>Performed</i>	Business Intelligence Reporting (BIR) is localized at the department or line-of-business level within FBI. Static paper reports are generated and distributed periodically to executives and staff. Reports are preformatted, and are "hand-coded" against legacy systems or operational data stores. BIR value is limited to Units.

CPMs Help Clarify and Scope Formal Construct Relationships for a Specific EA

Enterprise Architecture

Representations and assessments of IT-related systems in context with FBI's current and objective business operations



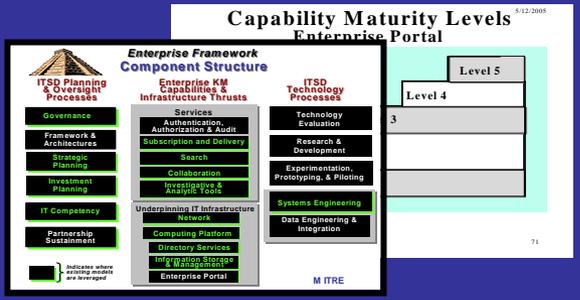
Clarifies and details IT-related deficiencies and remedies derived from EA assessments

Translates Interim & Target EA objectives into transition implementation considerations

Provides basis for reviewing & modifying Target EA based on readiness and affordability of enabling technologies

Enterprise CPMs

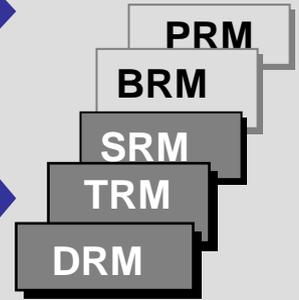
Transitional capability levels, enablers, and EA/FEA relationships associated with the IT-related services



FEA RMs
 Constructs and taxonomies of architecture elements populated with enterprise-specific "values"

Serves to harmonize the various EA products and enterprise reference models via links to a common set of capability-focused services

Identifies relevancy of the various FEA RM elements to IT-enabled services and capability levels



Enables capability-based project descriptions & business cases for OMB A300 submissions

The LSI Interoperability Maturity Model

provides a common basis for requirements definition and for incremental system improvements

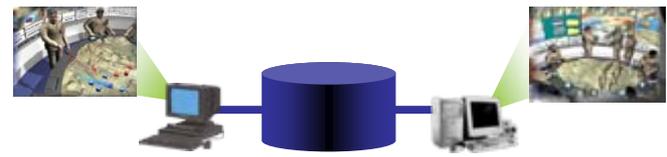
Cross-domain information & applications sharing
Advanced collaboration
(Event-triggered global database update)

4
Enterprise
Interactive manipulation
Shared data and applications



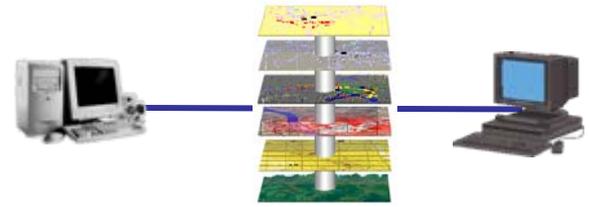
Shared databases
Sophisticated collaboration
(Common Operational Picture)

3
Domain
Shared data
“Separate” applications



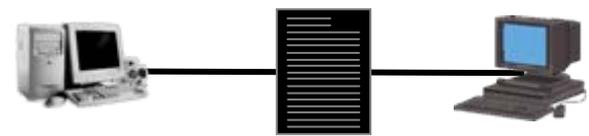
Heterogeneous product exchange
Basic collaboration
(Annotated imagery, maps w/ overlays)

2
Functional
Common functions; complex exchange
Separate data and applications



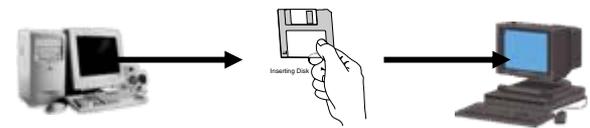
Homogeneous product exchange
(FM voice, tactical data links, text files, messages, e-mail)

1
Connected
Electronic connection
Simple file exchange



Manual Gateway
(diskette, tape, hard copy exchange)

0
Isolated
No Direct Digital Connection

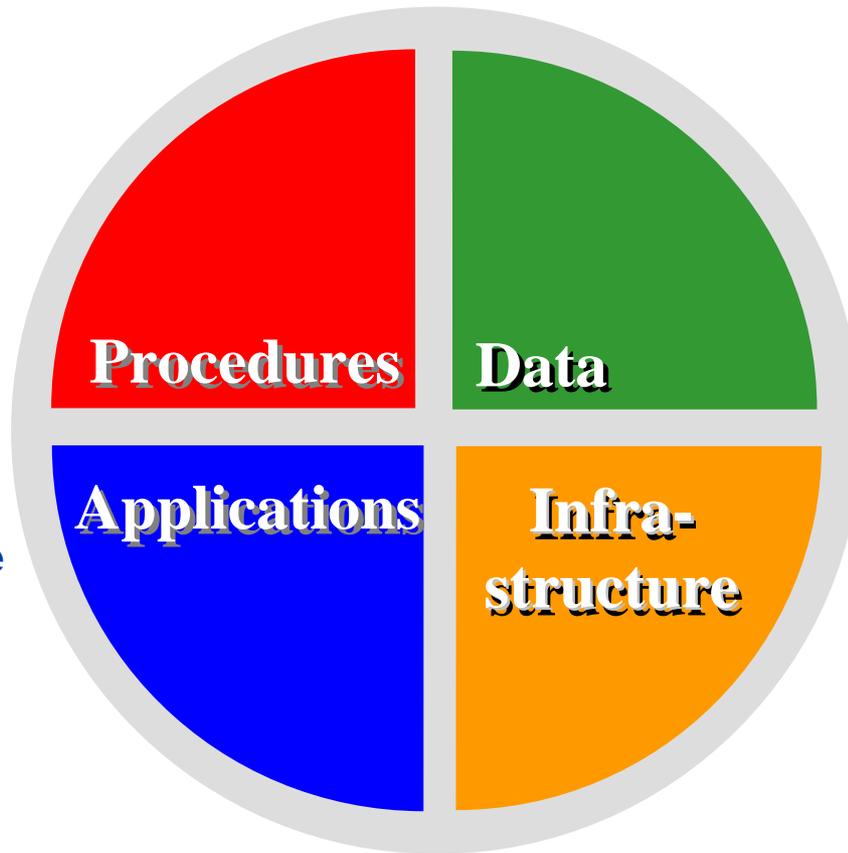


The LISI “PAID” Paradigm

defines the attributes of information systems that are the critical enablers of each level of interoperability

What policies and procedures enable systems to exchange information, capabilities, and services?

What set of applications enable information exchange, processing, or manipulation?



What information formats, data protocols, or databases enable the exchange of data and information?

What hardware, communications and networks, system services, and security features constitute the enabling infrastructure?

The LISI Capabilities Model



identifies the capabilities and implementation options available for achieving each level of interoperability

LEVEL (Environment)			LISI Capabilities Model			
			P	A	I	D
Enterprise Level (Universal)	4	c	Multi-National Enterprises	Interactive (cross applications)	Multi-Dimensional Topologies	Cross-Enterprise Models
		b	Cross Government Enterprise			Enterprise Model
		a	Govt Enterprise	Full Object Cut & Paste		
Domain Level (Integrated)	3	c	Domain Organization-wide Doctrine, Procedures, Training, etc.	Shared Data (e.g., Situation Displays, Direct DB Exchanges)	WAN	DBMS
		b		Group Collaboration (e.g., White Boards, VTC)		Domain Models
		a		Full Text Cut & Paste		
Functional Level (Distributed)	2	c	Common Operating Environment	Web Browser	LAN	Program Models & Advanced Data Formats
		b		Basic Operations (Documents, Briefings, Pictures & Maps, Spreadsheets, Databases)		
		a	Program Standard Procedures, Training, etc.	Adv. Messaging (Message Parsers, E-Mail w/Attachments)	NET	
Connected Level (Peer-to-Peer)	1	d	Standards Compliant	Basic Messaging (e.g., Unformatted Text, E-mail w/o attachments)	Two Way	Basic Data Formats
		c		Data File Transfer		
		b	Security Profile	Simple Interaction (e.g., Telemetry, Remote Access, Text Chatter, Voice, Fax)	One Way	
		a				
Isolated Level (Manual)	0	d	Media Exchange Procedures		Removable Media	Media Formats
		c	Collocated systems, Single operator	N/A	Manual Re-entry	Private Data
		b	Collocated systems, Separate operators			
		a	Non-collocated systems, Exchange via Operators			
o						
NO KNOWN INTEROPERABILITY						

WAN
SIPRNET
JWICS
NIPRNET (Internet)
DISN LES
VSAT
DISN

Example Implementation Options

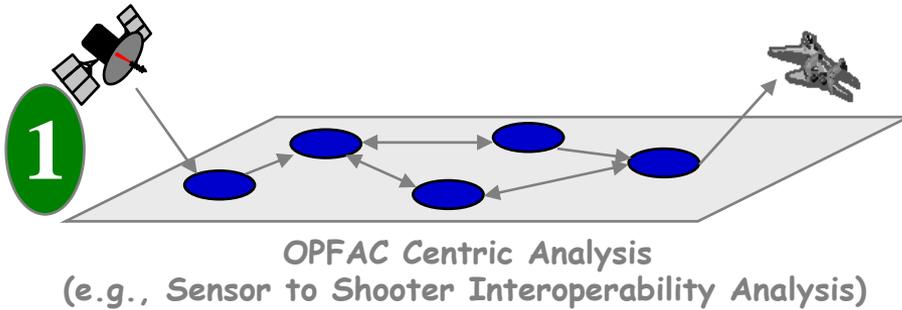
Services
Databases
Imagery
Graphics
Mapping
Spreadsheet
Clipboard
Word Processing

Mapping
Chart
ARC INFO
ARCVIEW
ATLAS
CMTK
Dew Drop
Delorme
Edge
Hipparchus
Imagine
JMTK
MPEG Viewer
MUSE
Navig. Spheroids
OILSTOCK
Open Map
Raindrop
Spatial X
QT
TEM

Document Formats
.asc .txt
.aw .doc
.lwp .pdf
.rtf .wpd
.OR2 .OR3
.nsf .htm
.sgm XML

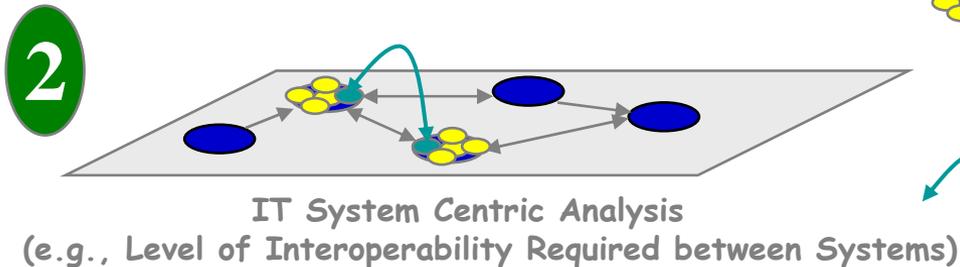
Standards
DoD JTA
IC
ANSI
ISO
IEEE

Fundamental Stages for Constructing an Architecture that Enables Adequate Addressal of Interoperability



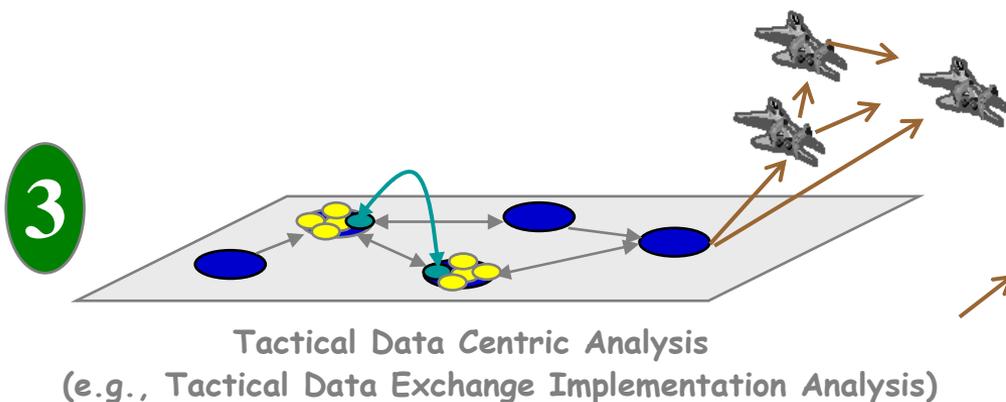
Which nodes must participate (i.e., organizations and platforms required) to conduct the mission?

What information (i.e., operational exchange needed to conduct the mission) must flow between the nodes to complete the mission? What interoperability levels?



Which IT systems (i.e., C4ISR automation technology) will be used to conduct the exchange to meet mission requirements?

Which specific system capabilities (i.e., data formats and protocols to meet IERs) are used in the exchanges between IT systems? What achievable interop levels?



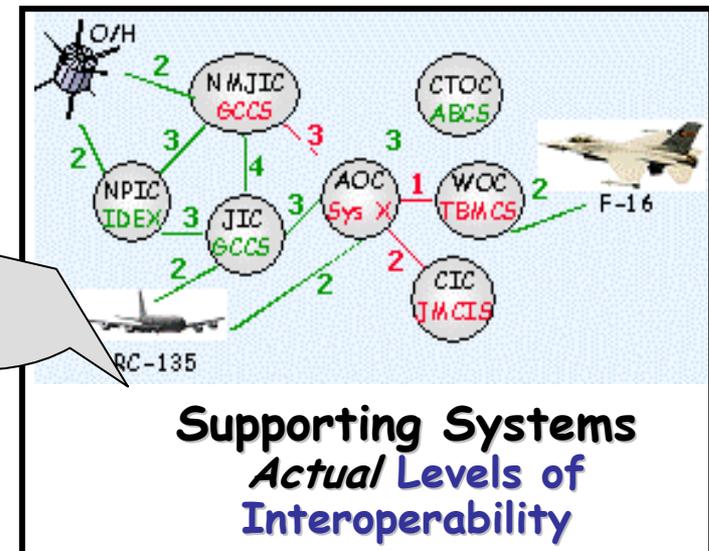
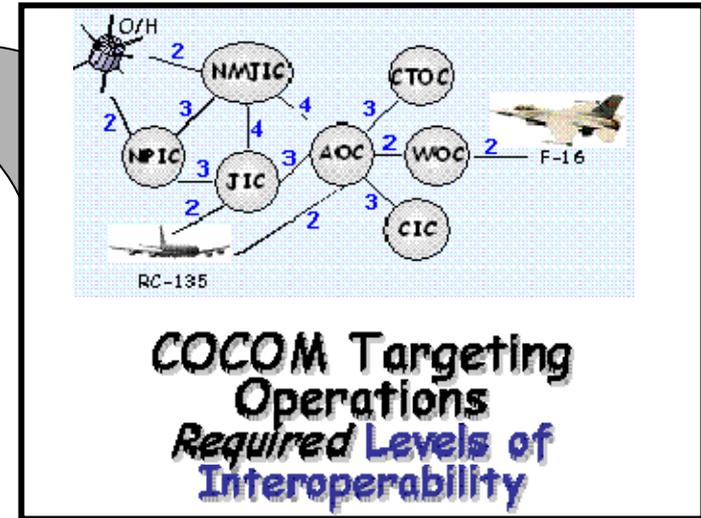
How should information be implemented by IT systems (i.e., data/mission engineering) to most effectively conduct the mission?

What standards & engineering criteria must be followed (i.e., operational criteria to meet IERs) when implementing IT systems?

EA Systems Interoperability Analysis Using LISI

LEVEL (Environment)		Interoperability Attributes			
		P	A	I	D
Enterprise Level (Universal)	4	c	Multi-National Enterprises	Interactive (cross applications)	Multi-Dimensional Topologies
		b	Cross Government Enterprise		
		a	Govt Enterprise	Full Object Cut & Paste	
Domain Level (Integrated)	3	c	Domain Organization-wide Doctrine, Procedures, Training, etc.	Shared Data (e.g., Situation Displays, Direct DB Exchanges)	WAN
		b		Group Collaboration (e.g., White Boards, VTC)	
		a		Full Text Cut & Paste	
Functional Level (Distributed)	2	c	Common Operating Environment	Web Browser	LAN
		b		Basic Operations Documents, Briefings, Pictures & Maps, Spreadsheets, Databases	
		a		Program Standard Procedures, Training, etc.	
Connected Level (Peer-to-Peer)	1	d	Standards Compliant	Basic Messaging (e.g., Uniformed Text, Email w/attachments)	Two Way
		c		Data File Transfer	
		b	Security Profile	Simple Interaction (e.g., Telemetry, Remote Access, Test Chat, Voice, Fax)	One Way
		a			
Isolated Level (Manual)	0	d	Media Exchange Procedures		Removable Media
		c	Collocated systems, Single operation	N/A	Manual Re-entry
		b	Collocated systems, Separate operation		
		a	Non-collocated systems, Exchange via Operators		
NO IN-OWN INTEROPERABILITY					

IT Systems Involved in Each Exchange





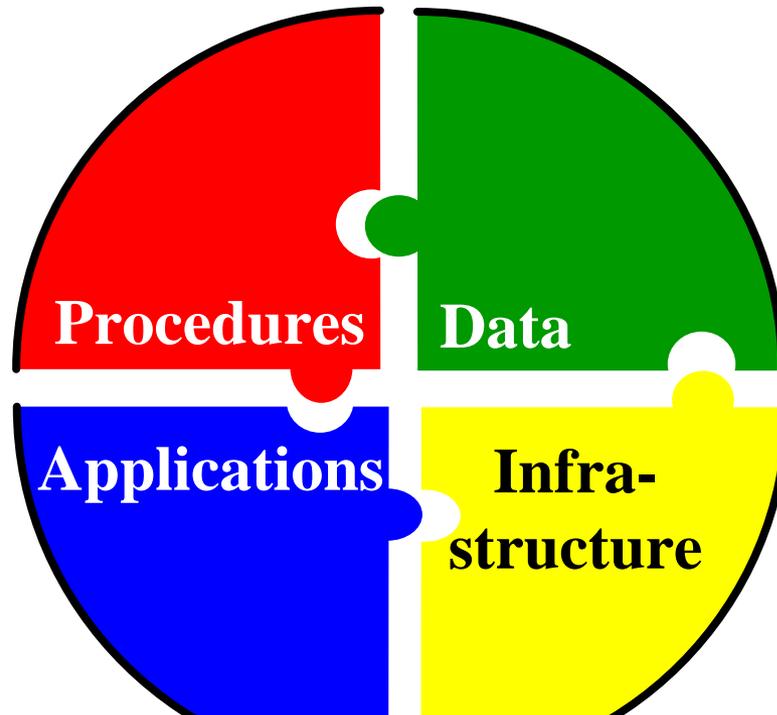
The Integration of LISI and Architectures Helps Determine the Impact of Various Interoperability Levels on Mission Effectiveness

Interoperability Maturity Levels	Enabled Business Process	Impact on Information Quality & Response					Mission Operations Supported
4 Application Sharing & COP Manipulation	Collaborative 	Content Event-responsive information; scalable perspectives; common data & shared apps across domains	Format Adaptive, event-driven & scalable views	Precision Event-focused, correlated & collaborated; de-confliction across domains	Time Minutes or Seconds	Security Fully automated cross-domain	Targeting <ul style="list-style-type: none"> • Re-locatable, mobile, & moving targets • Dynamic priorities • Essential Assisted Target Recognition (ATR) • No a priori intelligence
3 Database Sharing & Sophisticated Collaboration	Co-operative	User-adapted information; interactive cueing and filtering; shared data across organizations; full cut-and-paste	Adaptive, user-tailored views	Event-driven, correlated & collaborated; de-confliction across COIs	Hours or Minutes	Fully automated cross-COI Firewalls Guards PKI	<ul style="list-style-type: none"> • Re-locatable & mobile targets • Stable priorities • Some ATR • No a priori intelligence
2 Complex Exchange & Basic Collaboration	Co-operative	Mostly pre-set, multi-media products; automated cut-and-paste; some interactive filtering	Fixed multi-media views; user choices	Precision based on all-source fusion; limited de-confliction across organizations	Hours or Minutes	Firewalls Guards PKI	<ul style="list-style-type: none"> • Fixed targets • Some changing priorities • No ATR • Limited a priori intelligence
1 Simple Exchange	Co-operative	Pre-set, single-medium products; limited capability to filter products; user extraction	Fixed, non-integrated views	Individual source-driven; non-correlated; high risk of conflicts	Weeks or Days	Man in the loop	<ul style="list-style-type: none"> • Fixed targets • Stable priorities • No ATR • a priori intelligence
0 Manual	Isolated	Pre-set, single-medium products; user extraction of needed information					<ul style="list-style-type: none"> • Fixed targets • Stable priorities • No ATR • a priori intelligence

Black Belt Students are Taught How to Assess EA Threats & Countermeasures

Like Interoperability, Security encompasses the entire PAID paradigm!

What policies and procedures enable secure information use or exchange?



What set of applications enable secure information use or exchange?

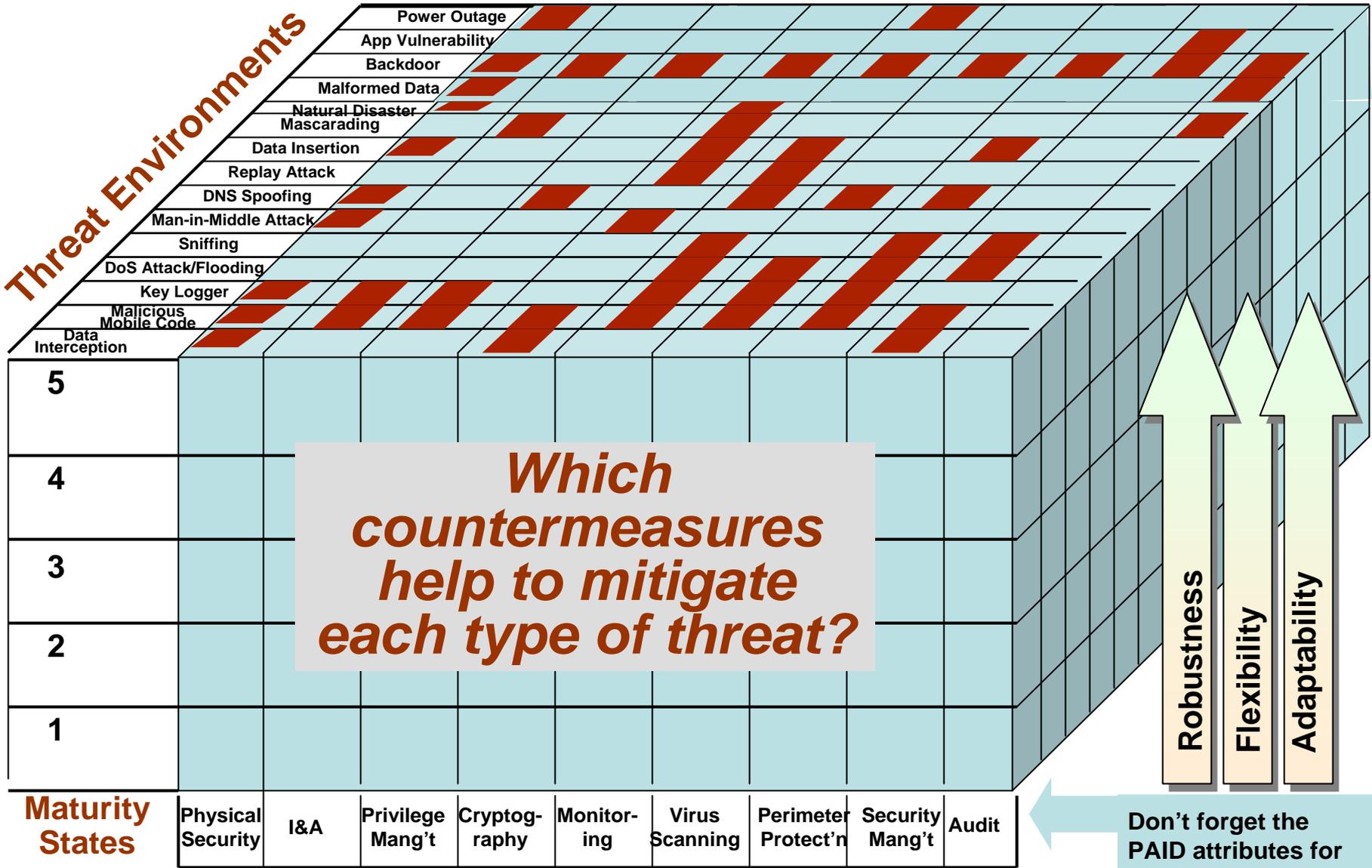
What *security conditions* must be incorporated in other applications?

What information storage mechanisms and communications protocols enable secure information use or exchange?

What hardware (computers, Servers, Network devices, etc.) enable secure information use or exchange?

The answers depend on what threats are driving the investments!

The Black Belt EA Program Exposes Students to Many Dimensions of Threats & Countermeasures



We hope you are looking forward to the challenge!

... and the rewards!

