11th ICCRTS
Coalition Command and Control in the Networked Era

Security and Privacy within an Intelligent Sensor Grid

Somalia,Strong Resolve (Norway), Adventure Exchange (Spain), Roving Sands (USA), Determined Effort (Yugoslawia), Battle Griffin (Norway), IFOR, SFOR, KFOR, Central Enterprise, Enduring Freedom, ISAF

Topics:

Information Assurance
C2 Architecture
Cognitive Domain Issues

Author:

Margarete Donovang-Kuhlisch

IBM Deutschland GmbH
Public Sector Defense
Godesberger Allee 115
D-53175 Bonn
+49-228-881-435 / fax: -301
mdk@de.ibm.com

- this page left blank by intent -

Content

1. CONCEPTUAL APPROACH TO EFFECTS-BASED PLANNING & OPERATION 4

2. ARCHITECTURE APPROACH FOR AN ISG 6

3. SECURITY AND PRIVACY IN AN ISG 7

3.1 RUNNING IT AS A BUSINESS 8
3.2 MANAGING DIFFERENT LAYER IN THE SOA STACK 9
3.3 FEDERATED IDENTITY MANAGEMENT & PRIVACY 10
3.4 PERVASIVE SECURITY 12

4. IT IS ALL ABOUT SEMANTICS 12

4.1 GLOBAL INFORMATION GRID 12
4.2 ADVANCED INFORMATION MINING 13
4.3 INTELLIGENT SOFTWARE AGENTS 14
4.3 MODEL-DRIVEN ARCHITECTURE & NCO 15

5. SUMMARY 16

A. APPENDICES 16

A.1. REFERENCES 16
A.2. ABBREVIATIONS 16
A.3. ABOUT THE AUTHOR 18

Figures

Figure 1: Effects-Based Operation 4
Figure 2: Knowledge-Based Development 4
Figure 3: partial automation of the OODA cycle 5
Figure 4: model-driven architecture for mission-specific decision support 5
Figure 5: sense & response operation – terms and characteristics 6
Figure 6: Core Enterprise Services 6
Figure 7: Secure Enterprise Service Bus 7
Figure 8: NCO Capability Transformation (Source: NNEC Feasibility Study, 2005) 7
Figure 9: security management disciplines 8
Figure 10: best practices IT infrastructure library 8
Figure 11: ITIL resource management 9
Figure 12: ITIL component management 9
Figure 13: ITIL service management 9
Figure 14: ITIL process management 10
Figure 15: ITIL security management 10
Figure 16: federated identity management (FIM) 10
Figure 17: enterprise privacy architecture (EPA) 11
Figure 18: regulatory modelling 11
Figure 19: policy-based PKI 12
Figure 20: information grid – evolving standards 13
Figure 21: unstructured information management infrastructure (UIMA) 13
Figure 22: knowledge management framework with UIMA 14
Figure 23: mobile software agents within simulation and decision support 14
Figure 24: application generation within MDA 15
Figure 25: LCIM – DEVS/HLA – MDA framework comparison 15

1. Conceptual Approach to Effects-Based Planning & Operation

The worldwide market trends globalization, integration and innovation do not miss the military and defense domains. Security organizations therefore are undergoing a process of transformation with the goal to enable effects-based planning and operation (EBO). Within this concept, intelligent information management on the semantic level provides a common relevant operational picture (CROP), which leads to shared situational awareness (SSA) and eases decision making and the achievement desired effects on the base of command and control superiority.

Such a transformation process is generally considered to be iterative and thriving for the development of an overall decision supporting knowledge database to assist both in operation planning and during operation execution.

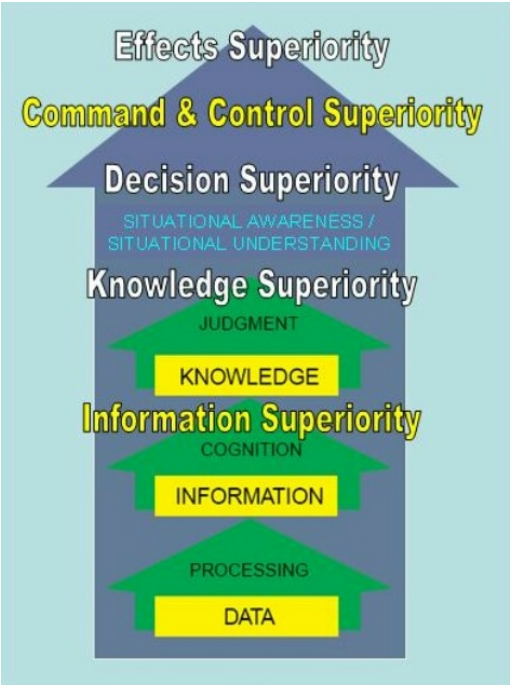


Figure 1: Effects-Based Operation

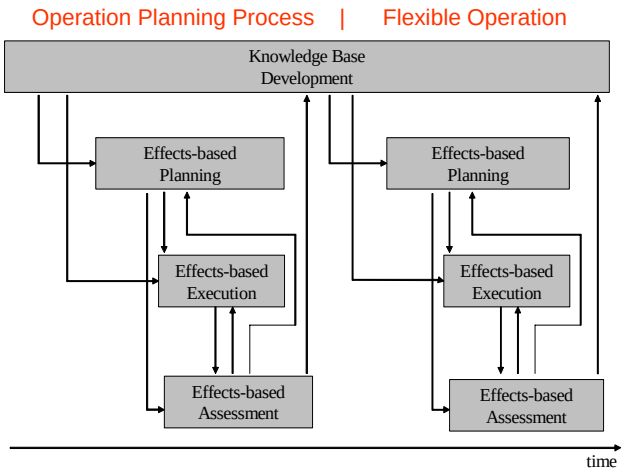


Figure 2: Knowledge-Based Development

Both planning and execution phases undergo the steps planning/modeling, execution/simulation and assessment within a system-of-systems analysis (SoSA), leading to proposed adjustment in future engagements (lessons learned). Knowledge-base development has been rudimentarily exercised with in various national and multinational experiments – both apart from any real systems and processes as well as concentrating on tool evaluation rather than doctrin verification.

Despite from that is the concept of KBD widely adopted and the only valid base for the envisioned partial automation of the command and control cycle:

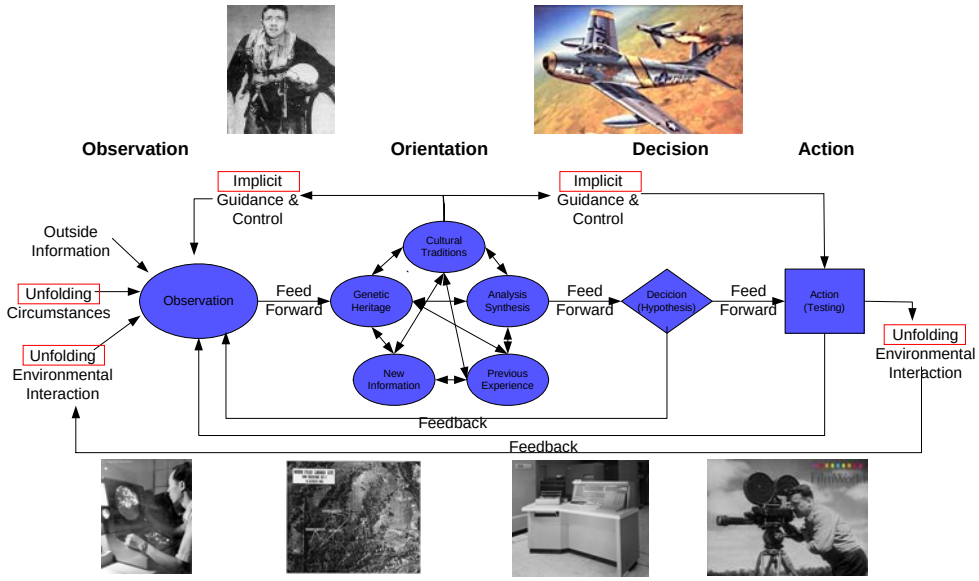


Figure 3: partial automation of the OODA cycle

There is nothing new in the C2 approach of observe-orient-decide-act (OODA), but performing it within a networked world bears new possibilities. The evolving knowledge base can be used to unfold implicit information by the means of both stochastic and agent-based modeling and simulation. Despite the fact, that the process of model building for reference scenarios (like evacuation, peace enforcement, stabilization operation) is very much at its beginning and that the fund of analyzable (digitally available) experience is still small, the methods and tools for this special type of business intelligence for network centric operations, which can be viewed as an intelligent sensor grid, are plenty and manifold.

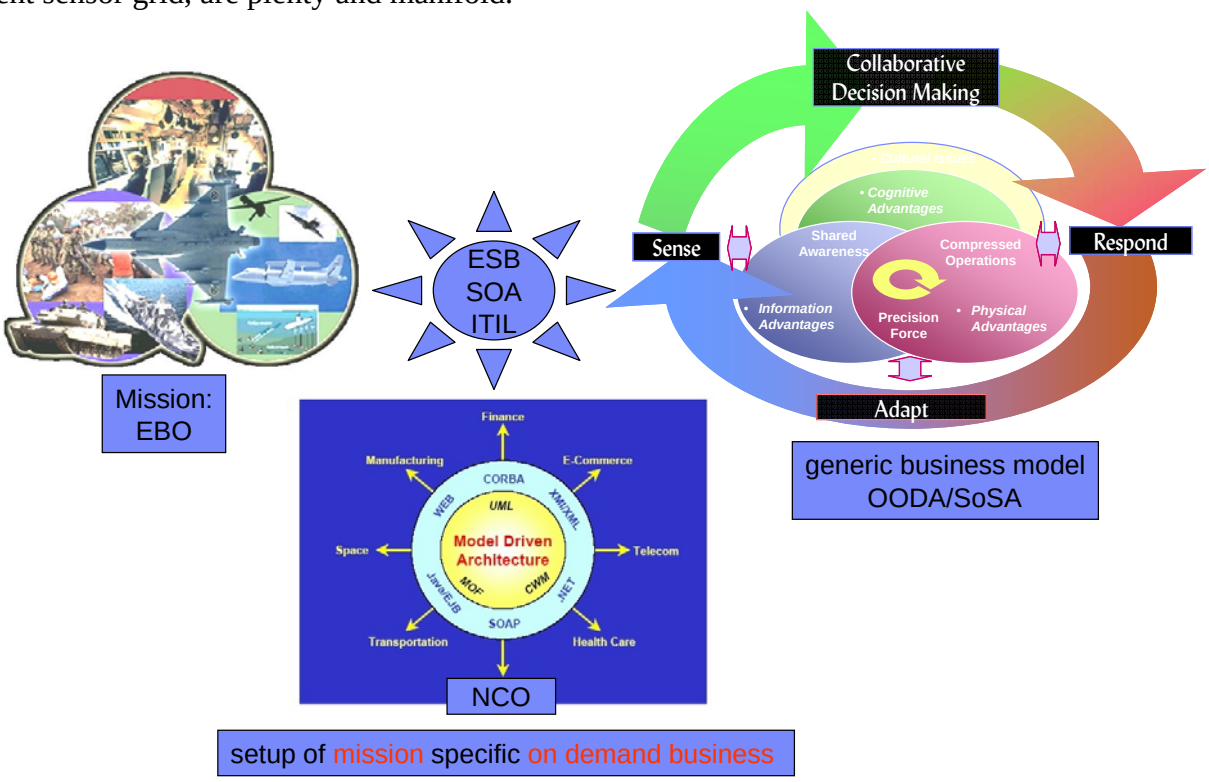


Figure 4: model-driven architecture for mission-specific decision support

EBO is characterized by the iterative KBD, which can also be interpreted as a model for sense-and-response operation of the organization, which integrates and fuses the physical domain (of sensors and effectors) with the information and cognitive domain.

Such a generic business model has to be brought to life individually for each due operation. In order to do this instantiation in a timely and effective manner, evolving standards for model-driven architecture (MDA) should be used.

Whereas the architecture building blocks for EBO are still under development, the technical enablers exist – in form of the standardized frameworks enterprise service bus (ESB), service-oriented architecture (SOA) and IT infrastructure library (ITIL) and the available implementations of these standards.

There are different definitions how this concept should be implemented and lived, not all of them by the military:

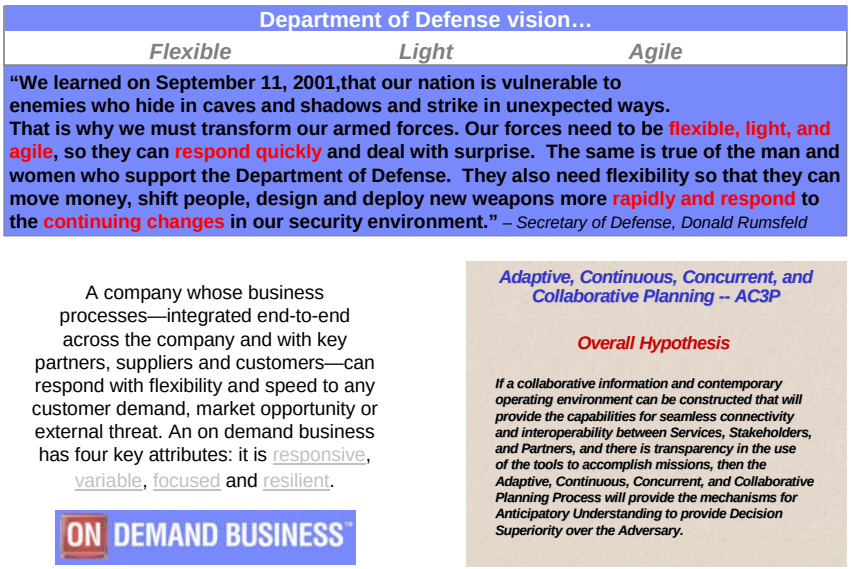


Figure 5: sense & response operation – terms and characteristics

2. Architecture Approach for an ISG

The global information grid (GIG) is thriving for shared situational awareness and understanding by providing core enterprise services (CES) to various communities of interest (COI) via a common communication backbone. Service-oriented architecture is the implementation concept for the GIG.

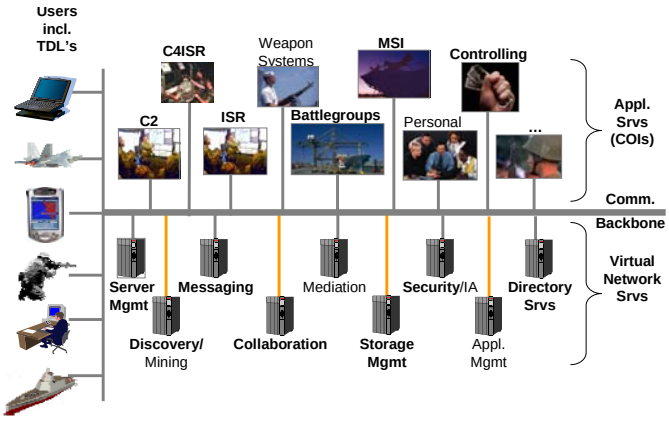


Figure 6: Core Enterprise Services

The intelligent sensor grid refers primarily, but not only to the manner, how information is entering the grid to be used within the generation of the situational picture (common relevant operational picture, CROP). An enterprise service bus (ESB) is the mean of choice for the underlying management infrastructure.

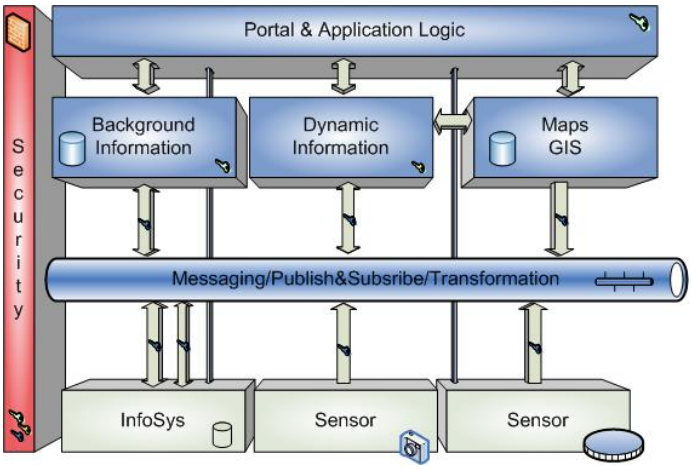


Figure 7: Secure Enterprise Service Bus

Sensors in this context can be very multi-faceted, delivering native data streams like GPS or audio/video, pre-evaluated information like tactical data links (TDL) or being autonomic information systems which publish certain data services based on a common data model. Core functionality of the ESB is the management of data flow in the grid, especially the messaging, publish/subscribe and transformation services. Role-, domain- and situation-specific application logic allows for the rendering of the CROP and its presentation in the portal. Key for the effectiveness and survivability of the ISG is the end-to-end securing of the ESB by implementing an all-encompassing private key infrastructure (PKI). Such a secure ESB is the foundation for future networked capabilities:

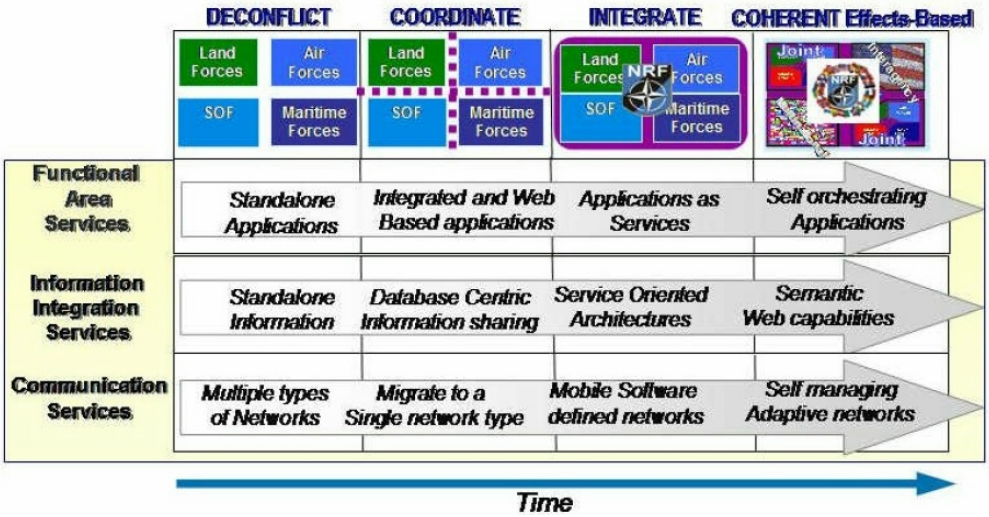


Figure 8: NCO Capability Transformation (Source: NNEC Feasibility Study, 2005)

An ESB is about integration by providing technical and procedural interoperability and therefore turns out to be the foundation for the necessary refinement of the operational architecture and the knowledgebase development.

3. Security and Privacy in an ISG

There are many aspects to security in an ISG covering the main issues of availability, confidentiality, integrity and authenticity.

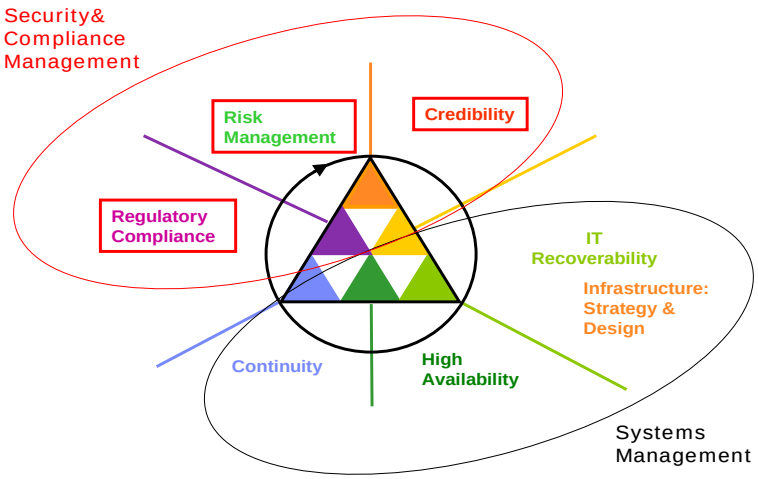


Figure 9: security management disciplines

On a coarse-grain level there are the issues of systems management on the one hand and the question of compliance to security and privacy regulations on the other. The former are rather classical for IT environments and can be addressed by a variety of techniques and COTS-products. Methods and technologies needed to ensure regulatory compliance and manageable risk in coherent effects-based operations are the subject of many research, development and standardization efforts throughout the IT world.

3.1 Running IT as a Business

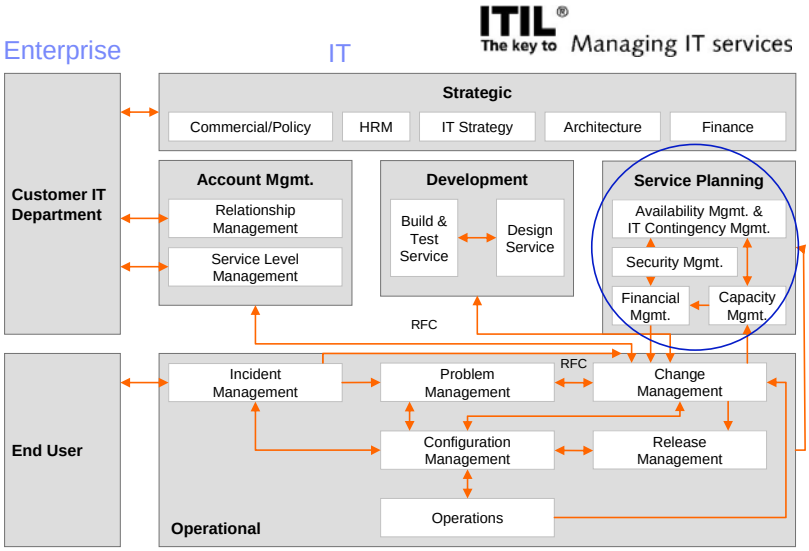


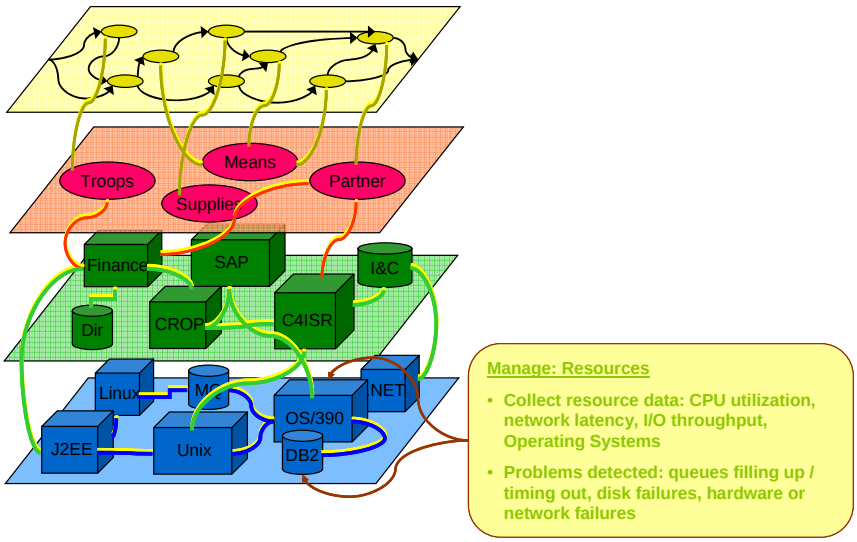
Figure 10: best practices IT infrastructure library

On the dawn of service oriented architectures (SOA) there is a growing need for chief information officers (CIOs) to run IT departments as businesses in themselve. This is supported by best practices for service processes which build on widely adopted, open standards based services and are listed in the IT infrastructure library (ITIL) architecture diagram.

Note, that the service planning process does not principally differ from an operation planning process and will also be based on an underlying knowledgebase, keeping reference models about f.e. service consumer patterns, user interest profiles and analysis and simulation tools to f.e. develope predictive capacity growth plans in order not the endanger the securing of service level agreements (SLAs) in the future.

3.2 Managing Different Layer in the SOA Stack

The management of IT services has to take place on different levels. The physical characteristics of each level are being virtualized for all the others.



The lowest level is the one of the single IT-resources – both hardware and software. Proper infrastructure design can lead to autonomy on this level. Technology and products are plentiful and mature.

Figure 11: ITIL resource management

On the next higher level the physical components of the application services have to be monitored and managed. Two major architecture frameworks for components exist and are state-of-the art: J2EE (Java) and WebServices (XML).

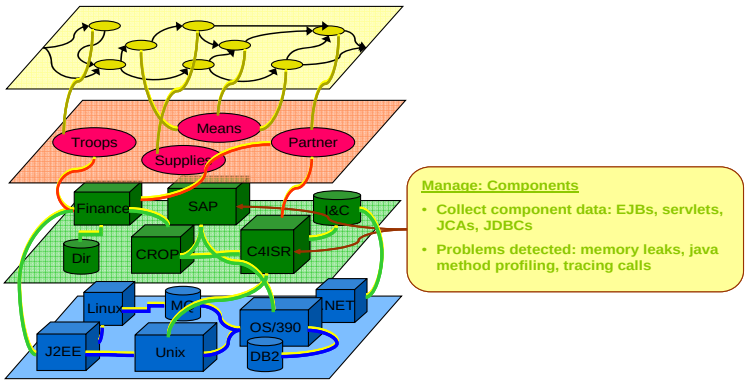
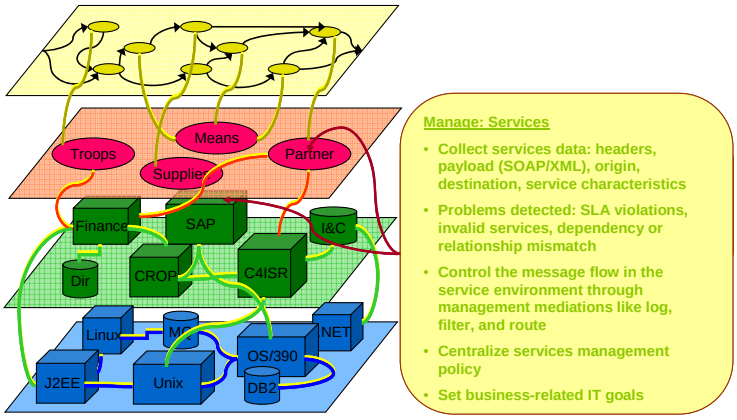


Figure 12: ITIL component management



Although SOA is not restricted to WebServices, most implementation are based on this standard today. Keys to the management of services are performance monitoring and SLA securing.

Figure 13: ITIL service management

Foundation for the C2 process management is a process model and the definition of performance indicators – basically a scorecard for decision support. These indicators have to be monitored, event-driven alarms and actions have to be enabled.

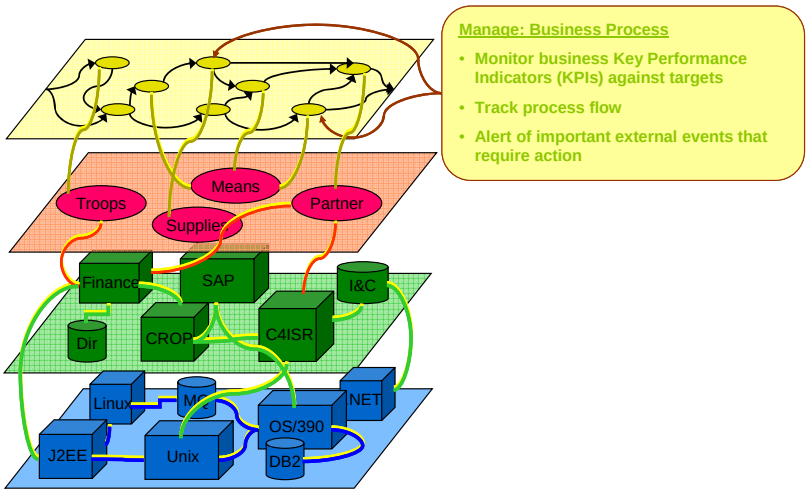


Figure 14: ITIL process management

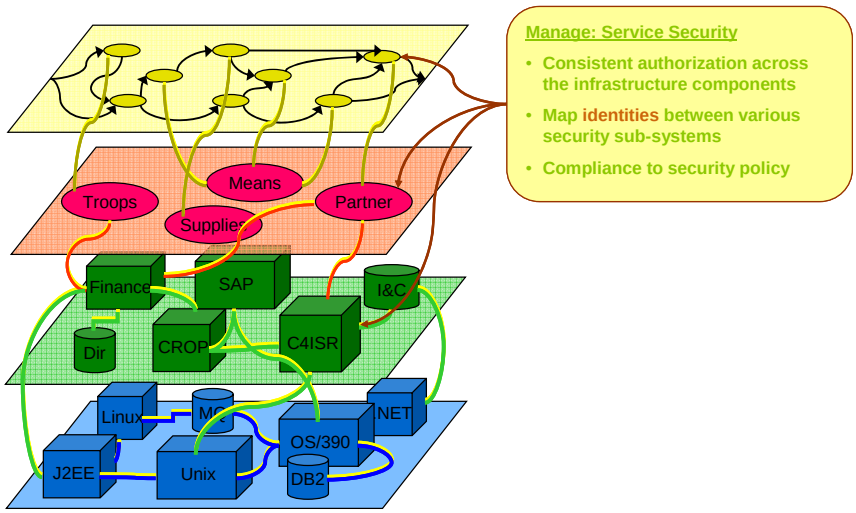


Figure 15: ITIL security management

Finally, service security has to be ensured. Again, prerequisite is a consistent authorization model, which reflects to the basic authorization rule: a service may only be used, if and only if the consumer has at least the authorization for the service's rating. Within a networked SOA the consumers identity has to be federated between various security subsystems.

3.3 Federated Identity Management & Privacy

Integrated identity and access management (IAM) is the major enabler to secure monolithic systems as well as SOAs. For the former exists a mature toolset ready for implementation on all state-of-the-art platforms.

For SOA new challenges arise mainly within the management domain. From a scientifical point of view nothing is changing: typically a browser user requests a

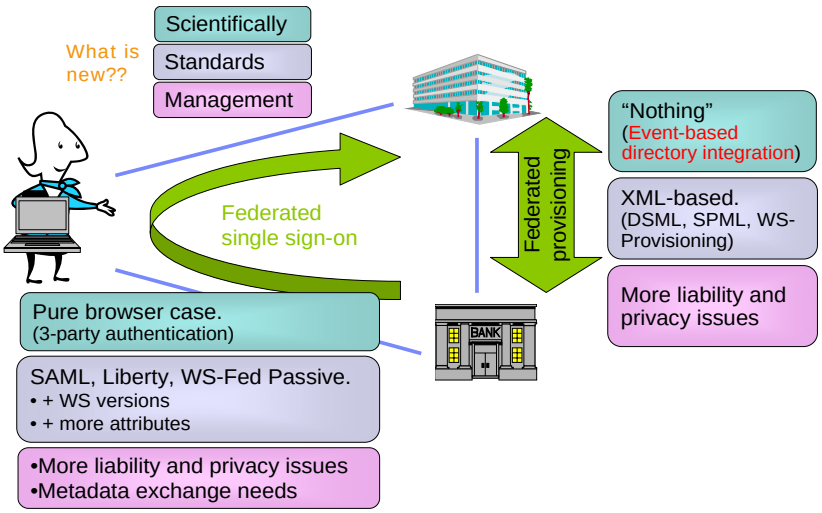


Figure 16: federated identity management (FIM)

service via a portal, thus creating the need for event-driven directory integration (on demand). Open standards for the technical enablement are evolving – mainly on basis of WebServices. On the content side new metadata exchange needs arise – while liability and privacy issues amplify.

Today, regulatory compliance especially in the financial market becomes a new driver for technology development, which can be reused in other regulated (f.e. data privacy laws) or doctrin-/policy-driven environments like NCO.

IBM has derived a sense-and-response enterprise privacy architecture (EPA), into with regulations expressed as logical models (research activity REALM) can be fed and monitored:

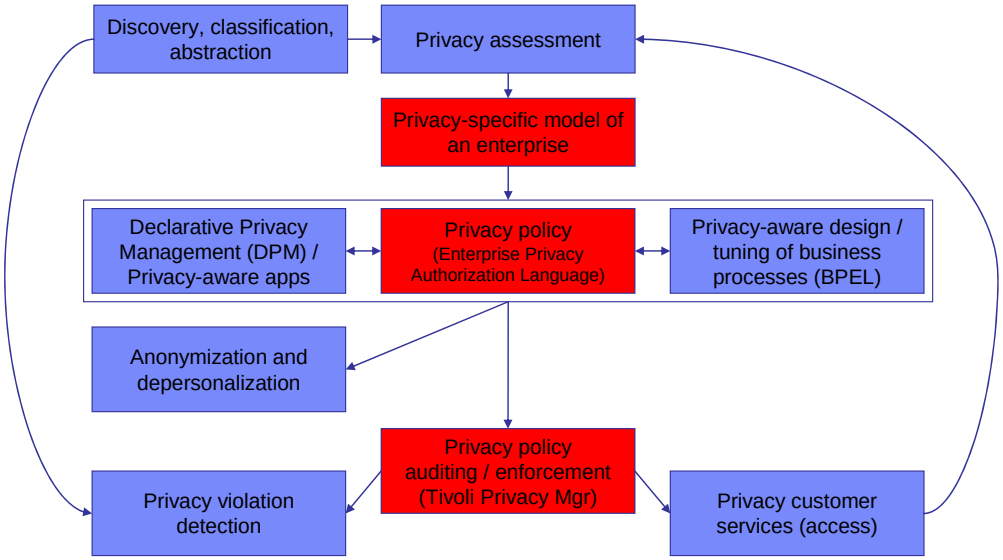


Figure 17: enterprise privacy architecture (EPA)

Whereas middleware exists (as COTS) to hosts the privacy management process, the real challenge lies in the modelling area – a very special text mining and business intelligence application within an ISG, in this case using legal or enterprise doctrin documents as data source (sensor). Innovative technology can assist, but not certify the process.

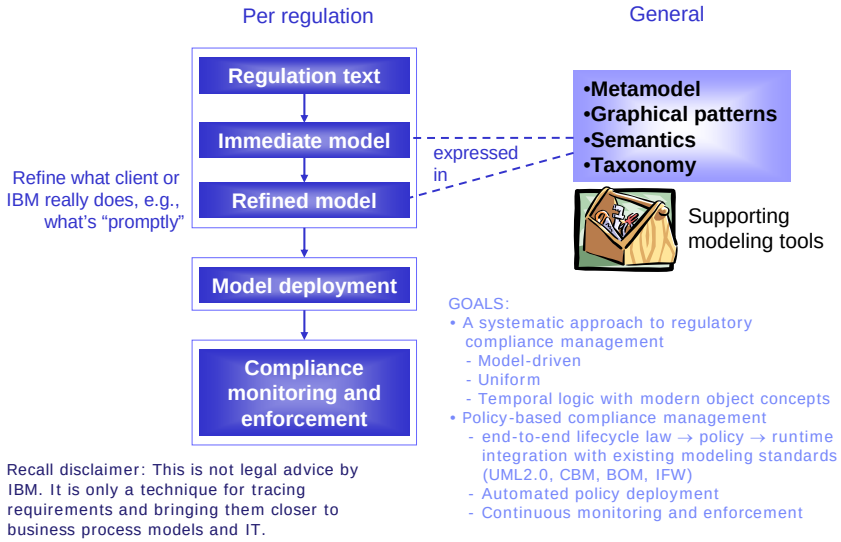


Figure 18: regulatory modelling

3.4 Pervasive Security

Once a compliant security model exists and can act as policy, the enabling PKI can be based on that policy.

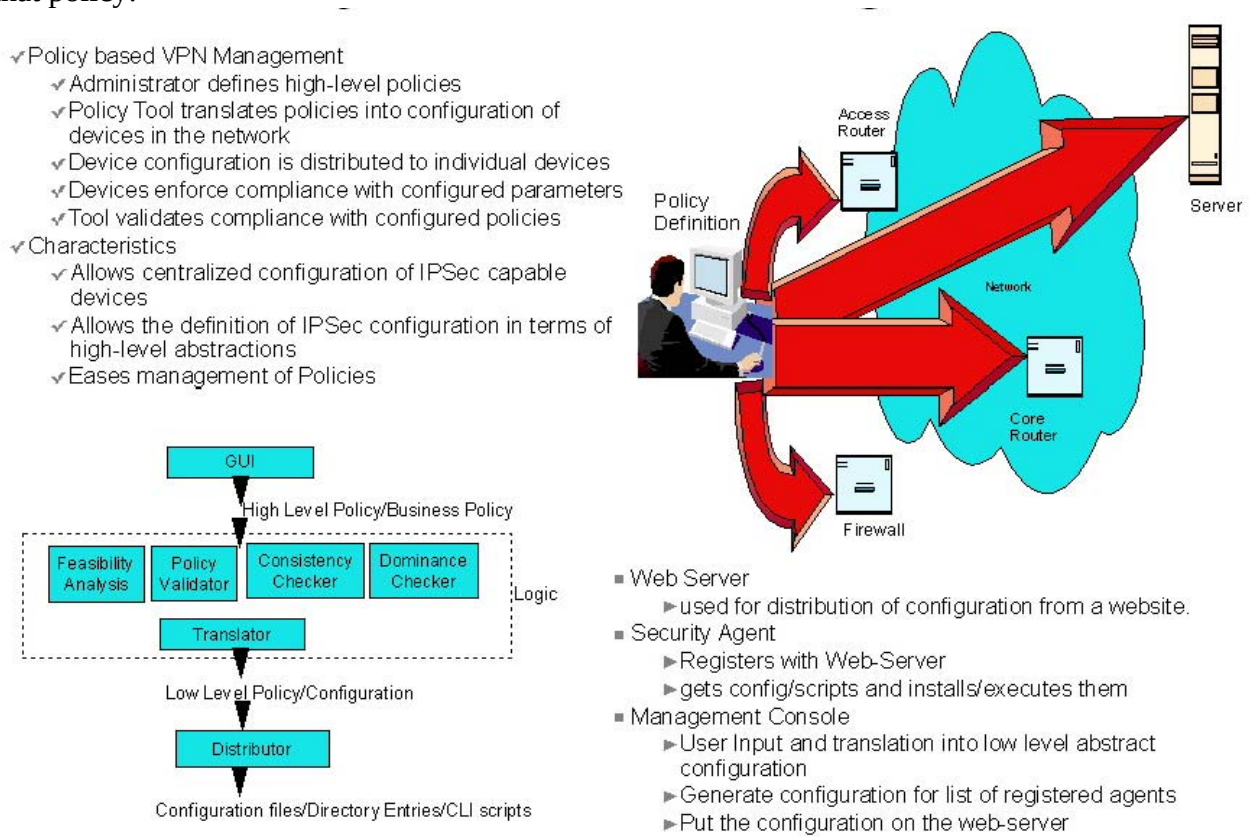


Figure 19: policy-based PKI

4. It is all about Semantics

The architecture aspects mentioned up to now show a common pattern – any event-driven service, whether it is on the level of self-healing data storage or on the operational level of EBO relies on a model of the desired state of the respective ecosystem, the constant monitoring of key indicators and the ability to decide for proactive actions on the basis of analysis tools. In other words, the semantics of the (sub)system under evaluation have to be opened up.

4.1 Global Information Grid

The Semantic Web provides a common framework that allows data to be shared and reused across application, enterprise and community boundaries. It is a collaborative effort led bay W3C with participation from a large number of researchers and industrial partners. Its purpose is to extend the current web by giving information a well defined meaning. The vehicles therefore encompass taxonomies, ontologies and integrated management infrastructure. For the latter lots of standards for database access and integration services (DAIS) are evolving:

- Realtime, streaming data sources
- Persistent, heterogeneous data
- Life-cycle management
- Provenance
- Dynamic access control
- Smart retrieval capabilities
- Virtualisation of data operations
- Persistent context
- Transaction capability to ensure referential integrity

- Publication and discovery
- Statements: data manipulation, definition & control
- Transport: multiway, cryptology, compression, monitor & notify, protocols
- Translation and transformation
- Transaction, sessions & connections management
- Operations and performance management
- Authentication, Authorization & Accounting
- Metadata
- Replication (via data definition, manipulation and transport)

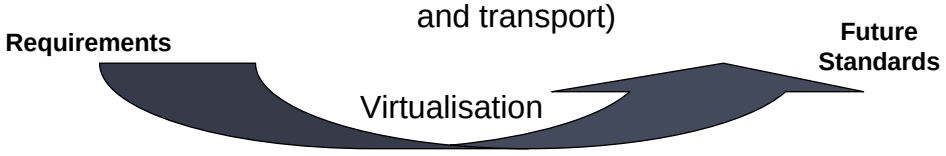


Figure 20: information grid – evolving standards

4.2 Advanced Information Mining

Research regarding the semantic exploitation of heterogeneous, networked environments is being conducted in different projects and causes the need for the development of an integrated management infrastructure to host the various capabilities and lead them to product maturity.

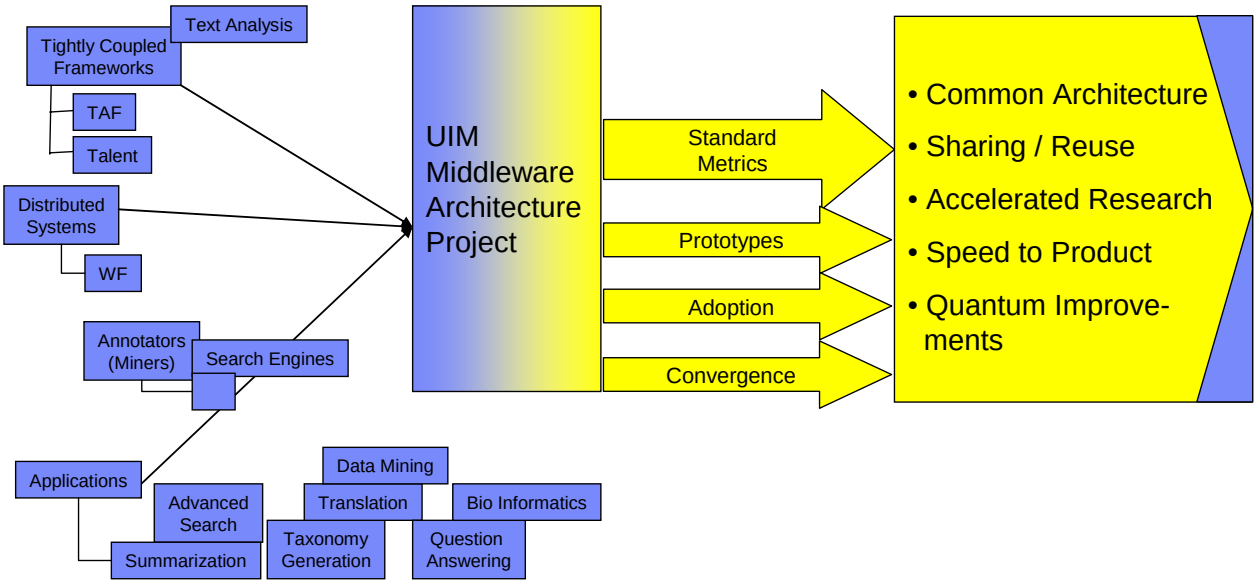


Figure 21: unstructured information management infrastructure (UIMA)

IBM has overtaken the task to develop an unstructured information management middleware (UIMA) in a three-folded way:

- Open source SDK (software developer kit): www.alphaworks.com
- Research: www.research.ibm.com/UIMA/UIMATopPage.html
- COTS: WebSphere Information Integrator Omnifind Edition

UIMA can be used in networked C2 systems:

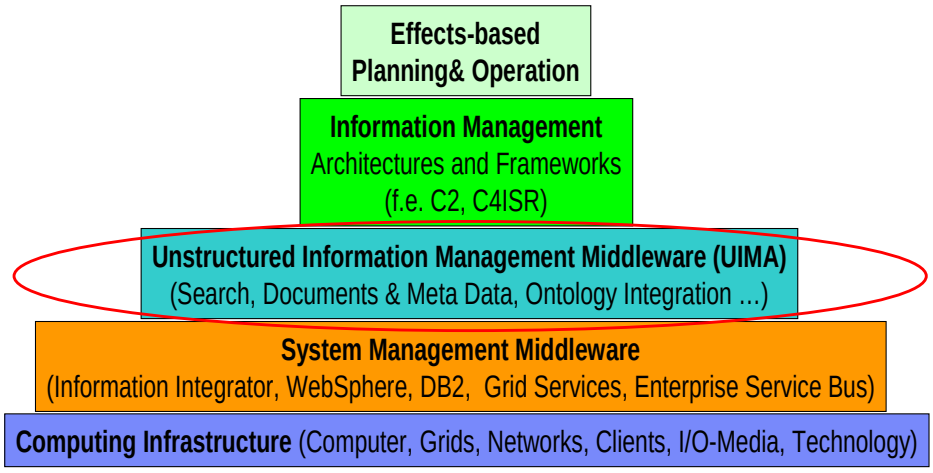


Figure 22: knowledge management framework with UIMA

4.3 Intelligent Software Agents

Multi-agents-systems can be the enabler for the system-of-systems-analysis (SoSA) within EBO as well as for the intelligent risk management in the underlying IT systems.

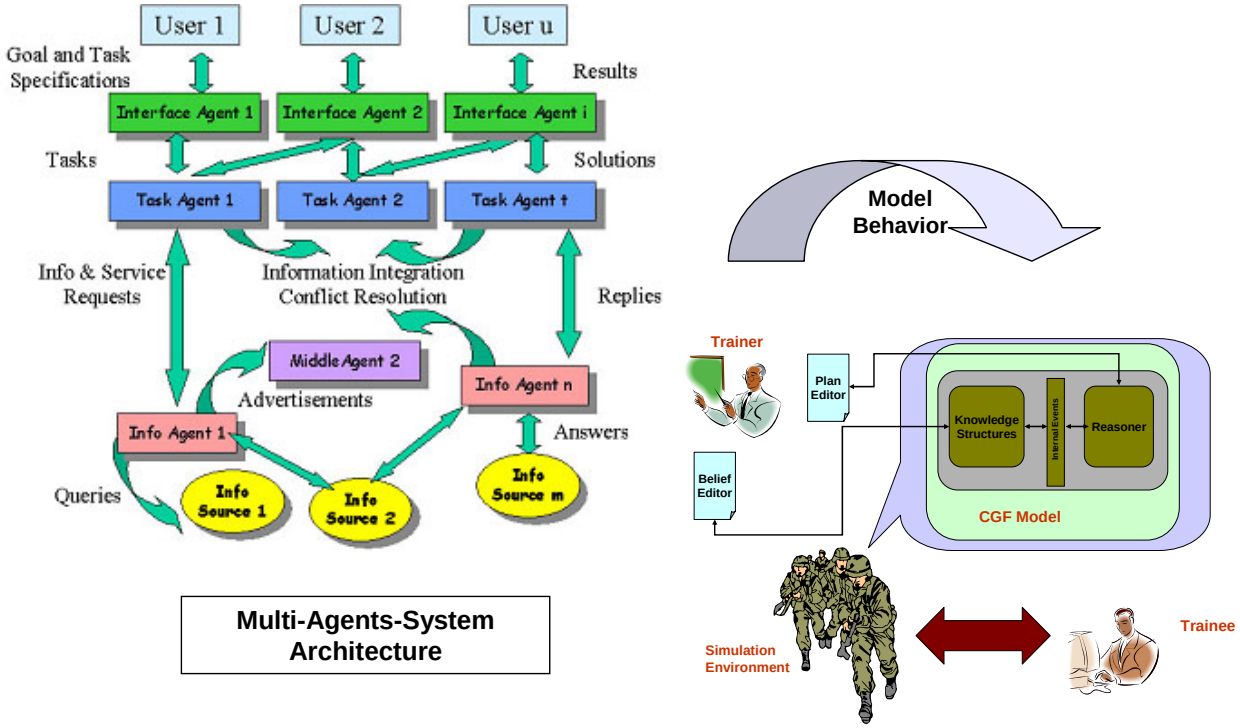


Figure 23: mobile software agents within simulation and decision support

Again, modelling and simulation builds and supports major parts of the decision support process.

4.3 Model-Driven Architecture & NCO

MDA is an initiative and standardization process of the OMG, which addresses the platform-independent application design through modelling techniques based on open standards and automatic generation of runtime- and platform-specific executable code ("model compiler").

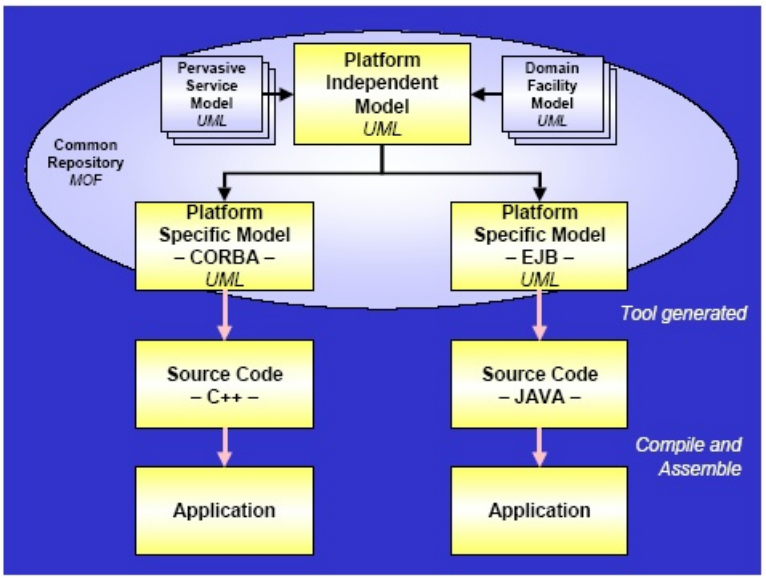


Figure 24: application generation within MDA

MDA is also a way to harmonize interoperability models evolving in different networked environments; it enables especially the combination of live C2 and simulation systems:

LCIM	DEVS/HLA	MDA
Level 5 Conceptual Interoperability	*Domain specific Business models, such as DoDAF*	*Domain overarching Repository of PIM*
Level 4 Dynamic/Pragmatic Interoperability	DEVS	PIM
Level 3 Semantic Interoperability	DEVS Reference FOM	PIM PIM-PSM-Mapping
Level 2 Syntactic Interoperability	HLA	PIM-PSM-Mapping PSM
Level 1 Technical Interoperability	*Net standards Web connectivity TCP/IP etc.*	*Repository of PSM describing net/web solutions*

Figure 25: LCIM – DEVS/HLA – MDA framework comparison

5. Summary

An intelligent sensor grid relies on the trustworthy ingestion of heterogeneous data, not necessarily given trustworthiness of the particular information itself. Therefore, risk management has to be conducted in all its facets. The OODA cycle is the process model for performing this task. Realizing this cycle for the securing of security and privacy/regulatory compliance in the networked world will be the enabler for EBO.

A. Appendices

A.1. References

Within the scope of this paper a lot of subjects could only be touched and not fully elaborated on. There is further information and reading available on – among other – sources:

/1/ www.research.ibm.com
/2/ www.zurich.ibm.com
/3/ www.ebXML.org
/4/ www.ggf.org
/5/ www.eclipse.org
/6/ www.trustedcomputinggroup.org
/7/ www.bsi.de
/8/ www.nc3a.nato.int
/9/ www.airdefense.net
/10/ www.act.nato.int
/11/ Building & Integrating M&S Components into C4ISR Systems for Supporting Future Military Operations, Dr. Andreas Tolk und Dr. Michael Hieb, Position Paper for the 2003 International Conferences on Grand Challenges for M&S, 2002
/12/ www.omg.org/mda/
/13/ www.uml.org
/14/ www.aanpro.org
/15/ www.xprogramming.com
/16/ www.projtech.com

A.2. Abbreviations

Acronym	Description
ICCRTS	International Command & Control Research and Technology Symposium
CCRP	Command & Control Research Program
IFOR	Implementation Force
SFOR	Stabilization Force
KFOR	Kosovo Peacekeeping Force
ISAF	International Security Assistance Force
C2	Command & Control
NCO	Network Centric Operation
SOF	Special Operations Force
NRF	NATO Response Force

NATO	North Atlantic Treaty Organization
NNEC	NATO Network Enabled Capabilities
KPI	Key Performance Indicator
VPN	Virtual Private Network
IPSec	Internet Protocol Security
EBO	Effects-Based Planning and Operation
CROP	Common Relevant Operational Picture
SSA	Shared Situational Awareness
SoSA	System-of-Systems Analysis
KBD	Knowledge Base Development
OODA	Observe-Oriente-Decide-Act
ESB	Enterprise Service Bus
SOA	Service Oriented Architecture
ITIL	IT Infrastructure Library
MDA	Model-Driven Architecture
PKI	Private Key Infrastructure
IT	Information Technology
RFC	Remote Function Call
HRM	Human Resource Management
SLA	Service Level Agreement
DPM	Declarative Privacy Management
ISG	Intelligent Sensor Grid
GIG	Global Information Grid
CES	Core Enterprise Services
COI	Community of Interest
GPS	Global Positioning System
TDL	Tactical Data Link
GIS	Geographical Information System
InfoSys	Information System
IAM	Identity and Access Management
FIM	Federated Identity Management
EPA	Enterprise Privacy Architecture
EPAL	Enterprise Privacy Architecture Language
BPEL	Business Process Execution Language
REALM	Regulations Expressed As Logical Models
COTS	Commercial of the Shelf
UML	Unified Modeling Language
BOM	Business Object Model
CBM	Component Based Modeling
IFW	Information FrameWork
C4ISR	Command, Control, Communication, Computer, Intelligence, Surveillance and Reconnaissance
I&C	Information & Communication
MQ	Message Queuing
J2EE	Java 2 Enterprise Edition
CPU	Central Processing Unit
I/O	Input / Output
XML	eXtended Markup Language

EJB	Enterprise Java Bean
JCA	Java Connector Architecture
JDBC	Java DataBase Connector
SOAP	Service Oriented Architecture Protocol
	Simple Object Access Protocol
GUI	Graphical User Interface
CLI	Command Language Interface
W3C	World Wide Web Consortium
DAIS	Data Access & Integration Services
UIMA	Unstructured Information Management Architecture
CGF	Computer Generated Forces
OMG	Object Management Group
CORBA	Common Object Request Broker Architecture
MOF	Meta Object Facility
LCIM	Level of Conceptual Interoperability Model
DoDAF	Department of Defense Architecture Framework
HLA	High Level Architecture
TCP	Transport Control Program
IP	Internet Protocol
DEVS	Discrete Event System Specification
PIM	Platform Independent Model
PSM	Platform Specific Model

A.3. About the Author

Margarete Donovang-Kuhlisch, Masters Degree in Mathematics & Computer Science, works as a senior consulting Client IT Architect for IBM Germany, Public Sector, Cluster Defense in Bonn, Germany. She furthermore is elected member of IBM's Technical Expert Council (TEC), the IBM Academy affiliate in Germany. Her main work area is the architecture and the solution design and project management within the military transformation scope of NCO. She can be contacted by telefone +49-228-881-435 or electronically at mdk@de.ibm.com.