# Interoperab

## Time to Open Up EW and SIGINT

**By Gordon Hunt and Dr. Ronald Meixner**

Stovepiping of EW and SIGINT systems has become inculcated into the systems design and procurement process, and it is significantly slowing down technology and innovation adoption. The time it takes to "integrate" a new capability into the broader warfighter environment has become unacceptable.

The agile and rapid deployment of SIGINT and EW services requires a rapid integration capability to the wider battlefield environment, if the information is going to be useful to the battlefield commander as well as brigade HQ or higher. Initiatives such as the Tactical Internet and similar network operations system infrastructure developments will enable broader information distribution (but not necessarily sharing) capability. But underpinning these technologies are in fact even greater shifts in systems architecture, design and implementation that will have far-reaching consequences in EW and SIGINT systems design and procurement strategy. Their impact should not be underestimated.

### THE CULTURAL CHALLENGE

There are technical challenges to full information sharing, and this article will cover those. But first we should call out the cultural challenge. The Tactical Internet and similar network operations initiatives will force a new culture into the EW/SIGINT sector, and the sooner it is recognized and embraced the better for the warfighter. The cultural change can be summarized thus:

*"No longer should SIGINT and EW operate on a 'need to know' (Information) basis, but instead on a 'need to securely share' (Data) basis."*

We explicitly call out the difference between *information* and *data* because information is contextual between sender and receiver. Current system architectures implicitly assume that they know who is sending the data, who is receiving it, why it is being sent, and how this data can be turned into information. But this is information-level stovepiping. It creates brittle infrastructures that don't respond well to changing battlefield conditions, to the requirement to integrate a new set of services, actuators or sensors. Any implicit knowledge in any system about a sender or receiver and its function creates stovepipes. These stovepipes either limit how far the information can be passed around the system-of-systems (SOS) and still be understood, or they raise integration cost/time barriers because every new system needs to have a unique message interface to every existing system, further exasperating the information stovepipe problem. Message-centric thinking in systems architectures has to be put aside and replaced in a true network operations or tactical internet environment.

What is needed is *inherent interoperability* between all systems, both those built today and those, as yet not envisioned, which will be built tomorrow. As in human interaction, the systems must know the "language" of every other system that is deployed or will be deployed. Unlike humans, each system only needs to know enough of the language to be able to send and receive communication relevant to its function.

Computers operate on data. The lingua franca of computers is data. It therefore makes sense to:
*". . . make the data definition, both content and context, a first class citizen of a systems architectural specification and thereby drive towards inherent system of systems interoperability."*

This requires a cultural shift in procurement, because it now becomes incumbent on the system specifier and procurer to define the system architecture using data modeling – not the industry. Yet it is the industry that knows what data is needed and how it should be specified. So while defense procurement agencies need to own the data model (often referred to as a System Data Dictionary (SDD), it needs to be constructed with the help of the industry. This may not sound like a likely proposition, but it is exactly what leading programs in the Department of Defense (DOD) and UK Ministry of Defence (MOD) have done. In addition, the SDD output of the DOD's Unmanned Control Segment (UCS) program is already informing The Open Group's FACE (Future Airborne Capability Environment) standardization effort, which in turn is being adopted by the US Army COE (Common Operating Environment). The

# ility


MOD's def stan 23-09 Generic Vehicle Architecture features a Land Data Model at the core of its Interoperable Open Architecture (IOA), developed with industry, owned by the MOD and already moving forward to a NATO Stanag. Similarly, the UCS program has done the same thing, creating an SDD at the core of its IOA specification by working with industry.

There are already 50 commercial companies contributing to FACE, guiding the evolution of their SDD. In all cases, the programs define the non-functional parts of their open architecture using data-centric system engineering processes, and thereby define inherent interoperability between the functional parts that will be procured from industry. Primes will compete to deliver the most effective IOA compliant with UCS, FACE, COE, GVA, etc. This is a shift away from message-centric thinking and towards data-centric thinking. The EW/SIGINT community is the most important military sub-sector that should be tracking this change. Once data starts to flow freely around all connected systems, EW effects and SIGINT decision support tools can start to use every system in the battlefield as an inherent sensor or actuator. EW and SIGINT systems can become truly integral to the entire battlefield and force deployment.

## THE DRIVERS OF CHANGE

The reasons for this shift in how systems are being specified are the economic imperative – a slashed defense budget while under pressure to sustain a warfighter advantage, in combination with the shift to an asymmetric warfare environment that creates new threats and rapid changes in support requirements from the warfighter.

For example, in today's warfare environment, the enemy is using smartphones quite effectively. This commercial device has been innovated within a few years, it is cheap and highly functional – it can manage location, mapping, and computation or even measure a heartbeat, as well as communicate using several methods. Adding a new capability is as simple as adding an app.

Contrast this with defense market change requests that take many months to bubble up to requirements, are expressed to defense procurement and are eventually delivered by industry over

the course of the following years. While such systems are undoubtedly much more fit for purpose, they are not architected to facilitate rapid technology insertion nor, and perhaps more importantly, to enable open-market competition. This is the commercial catalyst for agile development and rapid low-cost upgrades for the warfighter.

That impetus for change is felt in two ways by the warfighter:

1. The individual warfighters' technology expectations in terms of capability and ease of upgrade are becoming set by the commercial market, not by the defense industry.
2. The enemy is able to access more high tech for less money, and those without defense industries to support them are making effective use of advanced commercial technology and access to information.

To address these drivers of change, the EW/SIGINT community needs to better leverage what the asymmetric enemy cannot – the underlying infrastructure and capabilities of the communication network. This can only be facilitated by grasping the core tenet of Internet-style infrastructures, the free flow and easy integration of data.

## THE SHIFT IN DEFENSE PROCUREMENT STRATEGY

As Rich Ernst of UCS described at Interoperable Open Architecture 2012, "We have to be able to afford our future." To do that, something has to change – and that's the procurement process itself.

While open architecture initiatives have been around for 10-plus years, industry has failed to deliver the key commercial benefits that the MOD and DOD desired. Defense procurement officials have realized this and recognized that they need to define the IOA of the systems they procure.

The technology enabler is the ability to define the non-functional parts of systems-of-systems through its data without mandating an implementation – just state what data is available without specifying how and when to leverage it. Importantly, the DOD and MOD are now starting to mandate the systems architecture across programs of record. GVA, COE and UCS are building umbrella open architectures under which multiple procurements of systems of a similar type will be executed; inherent in their approach is a focus on architecting in interoperability. This will create a commonality of interoperable systems, which facilitates an open competitive market for future upgrades and updates. This shift will encourage industry to innovate and invest ahead of contract bid calls and thereby cut down delivery time to the warfighter, because a sub-system would be integratable in future system procurements.

**This is a huge change opportunity for the defense market; it most greatly affects those parts of the functional sub-systems that are already data and information centric: SIGINT and EW.**

Inherent interoperability architected into the system-of-systems infrastructure is the key technical capability needed for agile system updates and deployment. Supply chain integration gatekeepers are removed and the key to the open market door is now held by the customer.

The DOD and MOD enable the systems to be inherently interoperable by defining the system infrastructure and architecture data-centrically – stating *what,* not *how* to communicate. Through this approach, integration costs are being massively reduced.

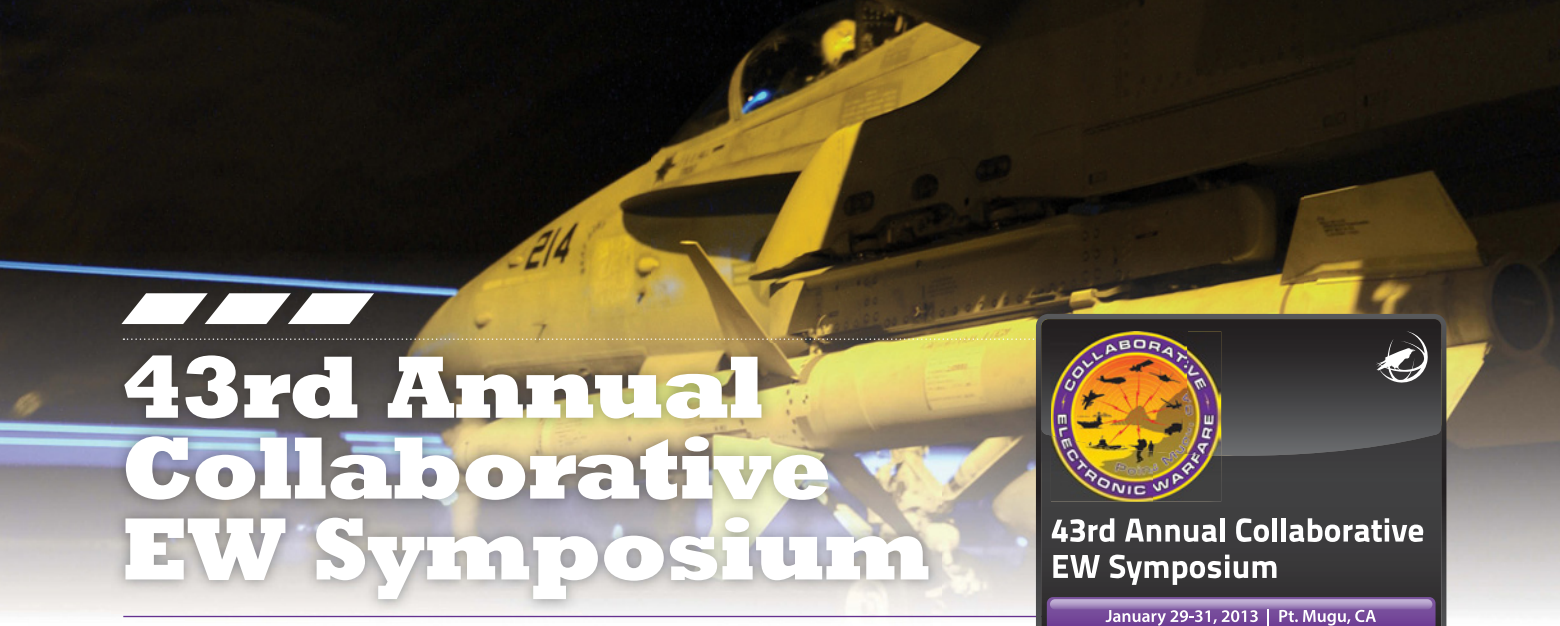
This change in procurement strategy creates an open competitive market, facilitating small businesses to engage where in the past only Tier 1 and Tier 2 companies could operate. It also drives the supply chain to focus on developing and delivering functional modules, not re-inventing the system architecture backbone for every SOS procurement. In such an open environment, the supply chain will be able – indeed will need – to develop functionality ahead of requirement in order to be time competitive, thus accelerating rate of updates/upgrades for the warfighter. The supply chain will need to innovate the functionality of the sub-systems to differentiate, and they will compete directly to implement the lowest cost, most efficient, non-functional, architectural infrastructure compliant with the architectural specification and SDD. This is a huge change opportunity for the defense market; it most greatly affects those parts of the functional sub-systems that are already data and information centric: SIGINT and EW.

## ACHIEVING INHERENT SOS INTEROPERABILITY

There are many definitions of interoperability because there are many levels of interoperability, each one contextual to the issue it addresses. In 2004, the DOD asked the Software Engineering Institute to help define interoperability because, according to their final report on System of System Interoperability (SOSI), "Interoperability to achieve information superiority is the keystone on which future combat systems, logistics systems and other government systems will be constructed." But, to define SOSI, they had to contextualize the broader levels of interoperability into which such a technical interoperability needed to be positioned. They defined a spectrum of interoperabilities, which they called "Layers of Coalition Interoperability." (See **Figure 1.**)

The major advance in interoperable systems architectural thinking is the drive towards assigning data a semantic context. Once data has this context, it becomes information, decoupled from any definition of who the sender is or who the recipient should be as well as how the data is being produced and consumed. This removes the information stovepipes previously discussed, and specifically enables the free flow of data around a system-of-systems, as required in a tactical internet or other network operations based system-of-systems.

Information is interpreted data, when data is processed, related, organized, structured or presented in



# 43rd Annual Collaborative EW Symposium

JANUARY 29-31 // PT. MUGU, CA

43rd Annual Collaborative EW Symposium

January 29-31, 2013 | Pt. Mugu, CA

As EW warfighting requirements continue to evolve in their complexity and interdependency, it is clear that future EW systems must work collaboratively with other air, ground, surface and space systems, such as cyber, intel, kinetic and spectrum management.

The 43rd Annual Point Mugu Electronic Warfare Symposium will facilitate the exchange of enabling concepts and provide a venue to disseminate current research in the fields of collaborative electronic warfare. Prominent leaders, contributors and representatives from the military, government, academia and industry will come together to address current electronic warfare gaps and emerging technologies in collaborative electronic warfare required to address these gaps. This three-day symposium will be held at Naval Base Ventura County Point Mugu Station Theater, January 29-31, 2013.

**Supporting Topic 1:** Collaborative EW Innovation and Inventions
**Supporting Topic 2:** Cognitive and Adaptive EW Capabilities
**Supporting Topic 3:** Coordinated / Distributed / Network-Enabled Systems
**Supporting Topic 4:** War fighter Perspective

## CALL FOR PRESENTATIONS

This call for presentations or demonstrations challenges presenters to explore the way forward in enabling collaborative EW through innovation and invention. Presentations or demonstrations from all services, DoD, industry and academia are requested that identify technical paths, options and potential opportunities for EW collaboration.

Submitted abstracts are specifically requested to address one or more of the symposium sessions: collaborative EW innovation and invention, cognitive and adaptive EW technologies, coordinated/ distributed networked-enabled systems and warfighter perspectives. Amplifying information on these supporting topics and draft agenda are referenced below.

Abstracts for presentations are required in unclassified textual format and may be received as email or email enclosures. Please forward abstracts to our speaker coordinators Mr. Michael Herrera at michael.a.herrera1@navy.mil and Ms. Miranda Fulk at fulk@crows.org. The deadline is December 10, 2012.

**Scan with your smartphone's QR scanner to go to the conference website.**

VISIT **WWW.CROWS.ORG** FOR MORE INFORMATION

a given context so as to make it useful, it becomes information. Semantic interoperability ensures that interpretation of data can occur unambiguously. A comprehensive SDD provides a system-wide method to define data in a manner that can be unambiguously interpreted as information by a recipient. With an SDD in place, individual systems can join a network, leverage existing data sources or contribute new ones. Such systems can be developed independently of each other, just as they are in the Internet. Integration now does not need two vendors to explicitly cooperate in order to develop sub-systems that can be integrated, because by definition they are inherently interoperable, they use the same "language." System development cost and time factors are massively decreased and the market moves towards greater openness.

## SECURITY IN INTEROPERABLE OPEN ARCHITECTURES

In EW and SIGINT, the free flow of data immediately raises concerns. Coming back to the original change of ethos to "need to *securely* share," we can see there is at least one more step towards fielding an operational interoperable open architecture. That step is data security.

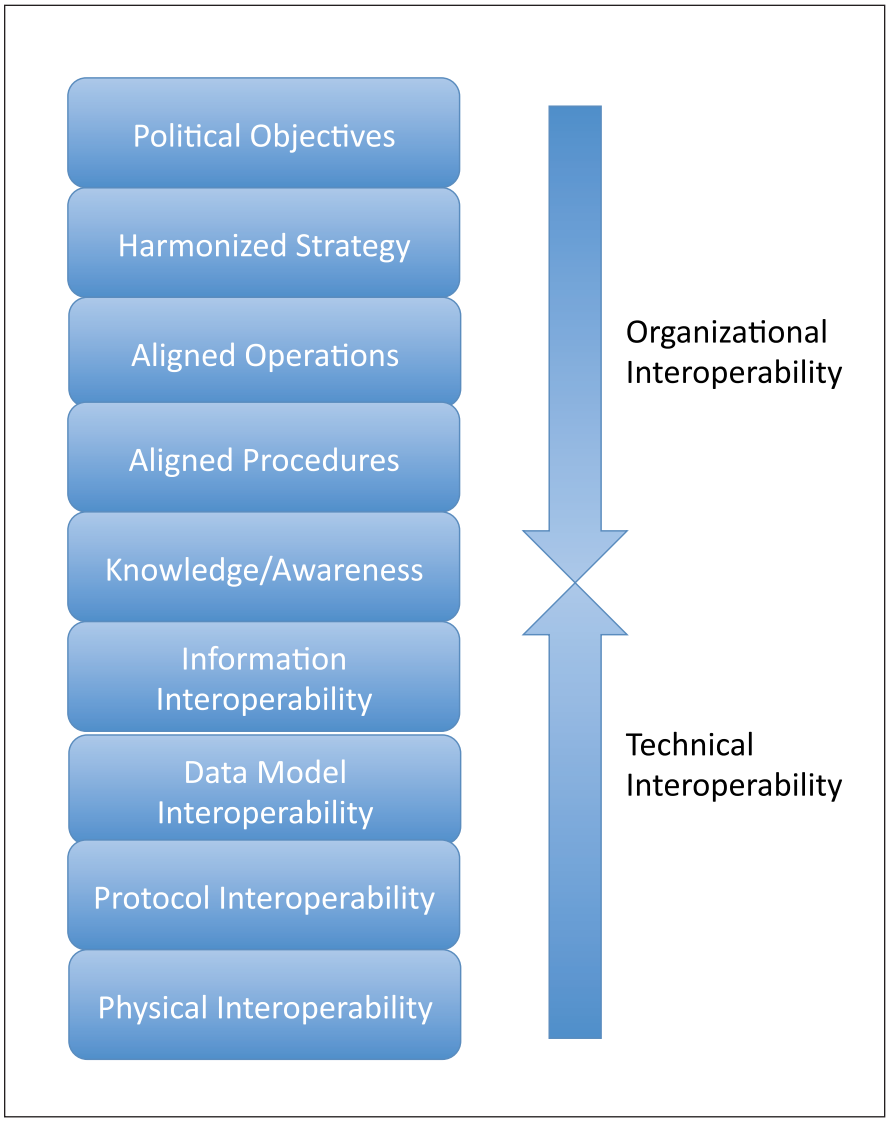



**Figure 1: Layers of Coalition Interoperability**
*Since the 2004 SOSI paper was published, a lot more work has been done to define Interoperability. The latest work from Dr. William Antypas Jr. of RTI has defined 7 levels of conceptual interoperability as defined in Figure 2.*

At the moment, the supply chain of EW/SIGINT system providers works very hard to clearly identify what information is needed by whom, and under what security conditions, as well as who can authorize electronic attack against a target. They then make a system-of-systems that achieves this goal. The trouble is, this thinking translates, unnecessarily, to system design. In effect the security model becomes stovepiped between a set of data sources and a specifically designated recipient. By its nature, this sort of system-of-systems is brittle and hard to evolve. Every new connection point needs to know explicitly about each source and sink of data in order to leverage it, as well as authentication and authorization levels. A change in brigade structure or deployment can limit the effective use of the SIGINT sensors and EW systems, until secure integration has occurred.

The benefit of taking a data-centric approach is that meta-data can be associated with actual data, and that meta-data can be used to define authentication and access rights. These access rights not only apply to the data sent and received but also the context of that information; how much, at what rate, what other related data, etc., should the receiver get. It is just as important to avoid security stovepipes as it has been to avoid the information stovepipes previously discussed. In order for a provider of data to agree to send it to a requester, the meta-data tags should authenticate at the security level, taking into account the context of the requestor, who they are, why they need the data, etc., just as humans do when choosing whether to answer a question or how fully to answer it.

Force structures, authentication levels, secure access, etc., all become aspects of the data. When the security model becomes de-coupled from the system infrastructure and message-centric thinking is removed, data can move freely and securely, and the warfighter gains advantage.

## SUMMARY

Shifting away from a "need to know" to a "need to securely share" thought process creates a need for the free flow

of data. This is critical if SIGINT systems and EW systems are to function as fully integral to the future connected warfighter. SIGINT and EW systems need to embrace the change data-centric architectures are enabling. The most effective way of doing this is to adopt common architectural practices, proven in other aspects of SOS integration and design. The latest thinking drives the need to understand what interoperability is and what it really means, both operationally and also to commercial acquisition. The ability to interoperate will radically change purchasing strategy, defense market organization and most importantly, warfighter capability.

## ABOUT THE AUTHORS

***Gordon Hunt,*** *Chief Application Engineer at RTI is the company's acknowledged Open Architecture expert and principle consultant for distributed systems architectures. He is also a Commander in the US Naval Reserves and a qualified Engineering Duty Officer.*

***Dr. Ronald Meixner,*** *Sales & Business Development, Plath GmbH, has a Doctorate in Electrical Engineering from the Federal Armed Forces University and has previous combat experience in surface warfare and EW. He retired from the German Navy in 2009 at the rank of Commander.*

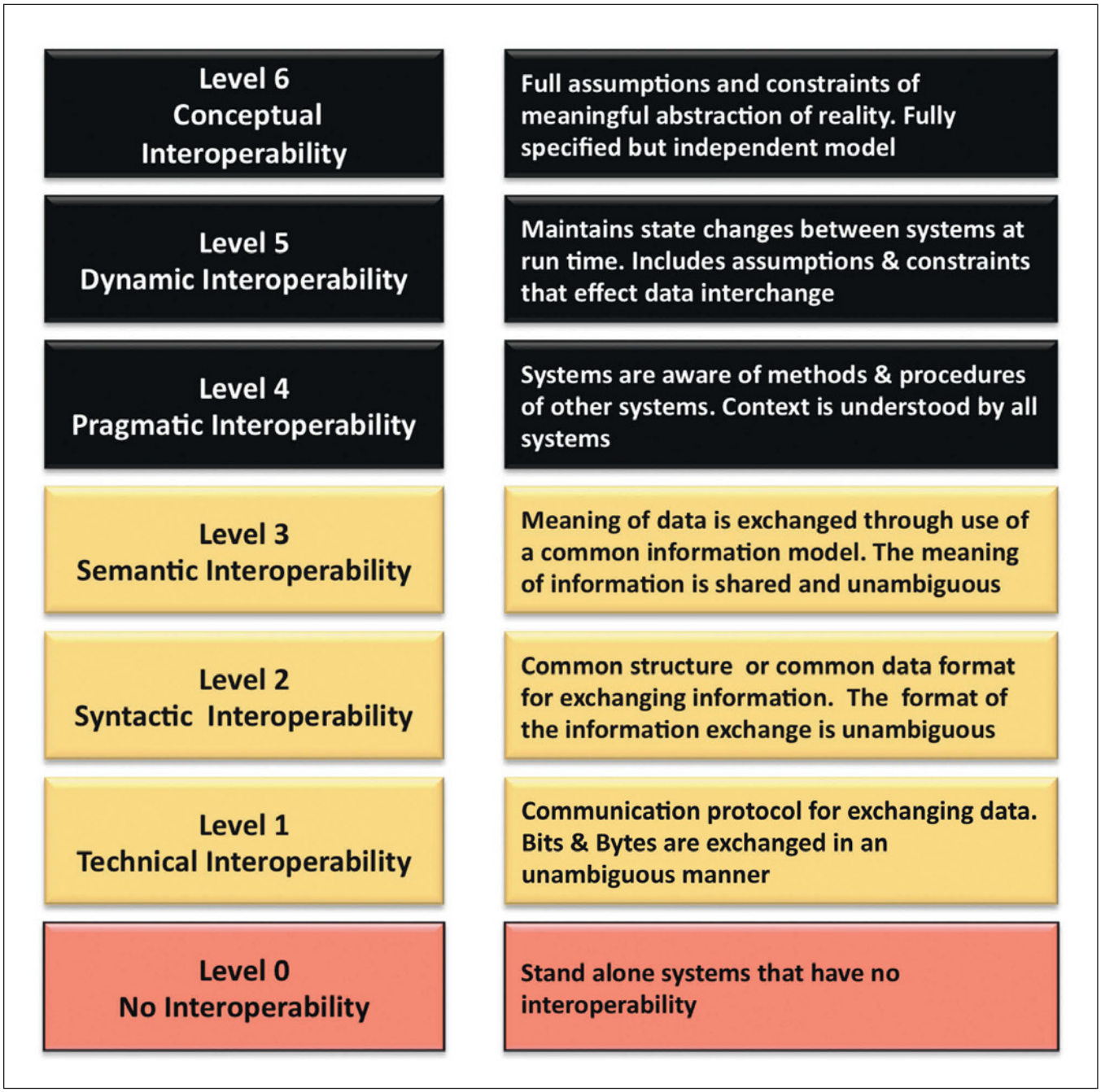



**Figure 2: Levels of Conceptual Interoperability Model (LCIM)**

*Most Systems-of-Systems have been architected to achieve Level 2, syntactic interoperability, because they have been message centric. Where programs like GVA and UCS are different is that they are starting to define Level 3 Semantic Interoperability. They are achieving this through a data model.*