

Introduction to the Integrated Sensor Architecture

Background

Numerous dangerous attacks in Afghanistan led ASA (ALT) to form the Deployable Force Protection (DFP) program to develop solutions to improve base defense. Interoperability between the various systems on a base was determined to be a critical factor as this enables Soldiers to rapidly share situational awareness and mission needs. Building upon many past sensor and system integration efforts, NVESD created the Integrated Sensor Architecture (ISA) to fulfill the interoperability requirements of DFP. ISA has since been utilized and fielded by many programs in the Army.

Description

ISA is an interoperability solution for sensors, systems, and services to join a network and make use of the functionality found there without requiring prior knowledge of the resources available on that network. This dynamic discovery is a core precept of ISA and is accomplished by requiring all members to self-describe the information they can provide about themselves, the information they can detect, and what behaviors they can offer. Members can change their capabilities at any time and can also search for other members that provide either data or functionality they are interested in. Dynamic discovery in this manner allows for components to adapt to a changing situation on the fly without potential downtime or reconfiguration and leads to the rapid utilization of new resources.

A fundamental requirement of true interoperability is a common data language that enables members to communicate without having to perform costly point-to-point integrations. ISA defines a single semantic data model that can be used across a wide variety of modalities ranging from sensors and C2 systems to unattended data processing services. This common data model, a singular language, can be used to interact with any other device on the ISA network to share information and accommodate command and control without requiring further integration. This self-describing capability using a single semantic data model enables two devices who have never before been directly integration to interact together without confusion.

A multitude of services have been designed to work on ISA networks, but only a small number are essential to provide core functionality. As with all other components, these services must publish their capabilities when they join the network and then are able to make use of what is discoverable. Core services, which are always available, provide for the discovery of other devices on the network, authentication and authorization of actions by another, and the routing of message traffic. The ISA network is designed to form a dynamic mesh where new nodes can be added and others removed without compromising the integrity of the whole. The services work together in a decentralized manner without a communications hub so they can continue functioning when disconnected but will perform better when connected to a larger network.

ISA was originally designed to operate on networks such as those in a tactical environment where communications may be unreliable or limited. In such a constrained network there are obvious benefits to dynamically building a mesh of available nodes and their capabilities. The core concepts of ISA are not limited to such an environment, and ISA has assimilated features from other domains to enable it to operate on enterprise and other network variants. The network behaviors and encodings in use by ISA are different in each of these realms to allow for optimal use of the environment but the core data model and capabilities are the same, and bridges exist that can link the disparate networks in a seamless manner.

Distribution A: Approved for Public Release. Distribution Unlimited

Security was built into ISA in the very beginning and all network connections between ISA components are encrypted and compliant with DoD and IA standards. Services exist to ensure that only authorized components may connect to a network and task other members. These authorization and security services are very extensible to allow for the integration of new standards and dynamic configuration.

Payoff

ISA is a government owned standard enabling the rapid integration of systems, sensors, and services onto a common, data sharing network. ISA provides documentation, compliance tools, data generators, a reference implementation, and an API for integration. The common data model and discovery aspects provide for a one-time integration of an asset into an ISA network and a universal layer that complex data processing services can be built on. ISA reduces the number of integrations needed for each product, the overall cost and maintenance of support, and resolves the problem of individual sensors operating independently from their proprietary control point. ISA has been adopted and is being fielded by Army PM Terrestrial Sensors (Force Protection and Sensor CE v3), Army PM Electronic Warfare & Cyber, PM DCGS-A, JPEO Chemical and Biological Defense, and others.