Brochure

SitaWare in Multi-Domain Operations

The MDO concept is more than just adding the Cyber and Space domains to the traditional Joint Operations set-up. Implementation of the concept provides commanders at all levels access to data and information from all domains. This allows for simultaneous and sequential operations using the integration of capabilities across domains, in principle at all levels in a very dynamic operational environment.

The SitaWare Suite can be used as a key enabler of MDO. Since MDO is in a constant evolution with resulting changes in requirements, the SitaWare Suite offers the best development potential for integration of the different domains, including the necessary communications infrastructure and integrated workflows.

SYSTEMATIC

Introduction

The evolution of Joint Operations into a Multi-Domain Operations (MDO) Concept has been in the centre of many recent discussions on Military Operations. MDO is often also known as Joint All Domain Operations. However, there is yet no common definition of MDO, as nations tend to take their own approach.

The NATO working definition is:
“The orchestration of military activities, across all domains and environments, synchronized with non-military activities, to enable the Alliance to deliver converging effects at the speed of relevance”[1].

This definition will be the point of departure for this document, which describes Systematic’s take on the characteristics of MDO and how SitaWare can support nations when transitioning from a traditional Joint Operations Concept into an adaptation of the MDO Concept.

[1] ACT Article: Multi-Domain Operations: Enabling NATO to Out-pace and Outthink its Adversaries, July 29th 2022.

The changes in the Operational Concepts

Nations have seen a significant change in the overall security situation towards a constant state of competition and activities below the threshold of war. This situation combined with enhanced technological opportunities has led to an understanding, that the traditional ways of conducting operations comes short in a near-peer conflict. Thus, the introduction of MDO as a future operational concept is being adapted by nations in different ways.

The traditional Joint Operations Concept

The Joint Force Commander executes the operation plan (OPLAN), issues operation orders, and directs operations. The commander will carry out the following[2]:

- Allocate forces and resources (as necessary) to enable subordinate commanders to accomplish their missions.
- Direct the activities of those formations or units not delegated to subordinate commanders, especially those earmarked as operationallevel reserves.
- Engage with other relevant actors in theatre; and
- Determine the acceptable level of risk to the force and mission.

Thus, the traditional concept for Joint Operations leaves the responsibility for overall Planning, Tasking, Execution and Coordination with the Joint Force Commander and his staff, whereas the traditional Service Component Commands with subordinate units primarily works within their own responsibilities with some degree of direct coordination. However, the concept of “Supported” and “Supporting” components, as determined by the Joint Force Commander, leads to some direct requesting and tasking between the Service Components without direct involvement of the Joint Force Commander and his staff.

[2] AJP-3

The Multi-Domain Operations Concept

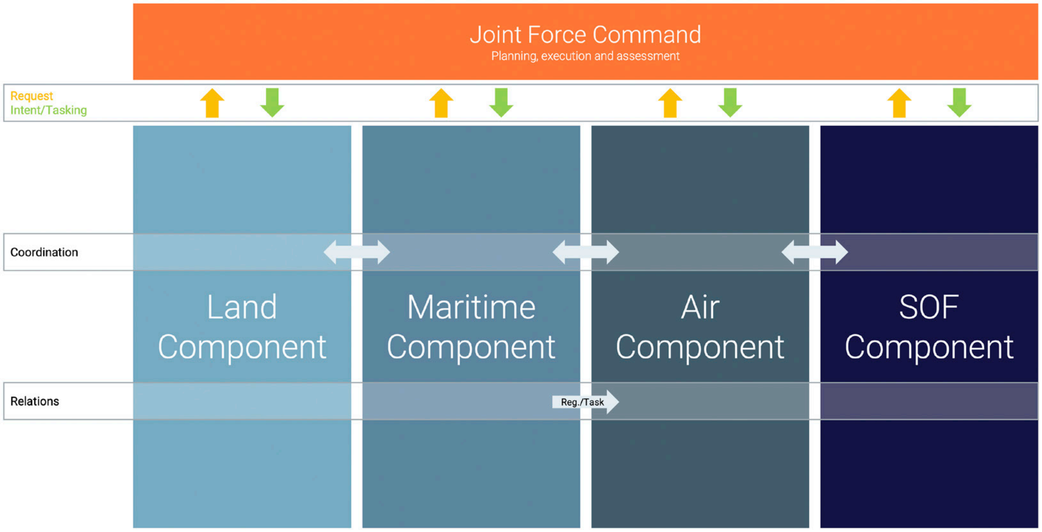
The MDO concept is more than just adding the Cyber and Space domains to the traditional Joint Operations set-up. Implementation of the concept provides commanders at all levels access to data and information from all domains to allow for simultaneous and sequential operations using the integration of capabilities across all domains, in principle at all levels in a very dynamic operational environment.

The concept also calls for a change in perception and a move from "need-to-know" towards "need-to-share" to get the right information out to the right commander at the right time, including other governmental decision makers. The concept furthermore calls for an empowerment of local commanders and decision makers to exploit the cross-domain capabilities in order to rapidly achieve the wanted effects and to achieve the prioritised objectives.

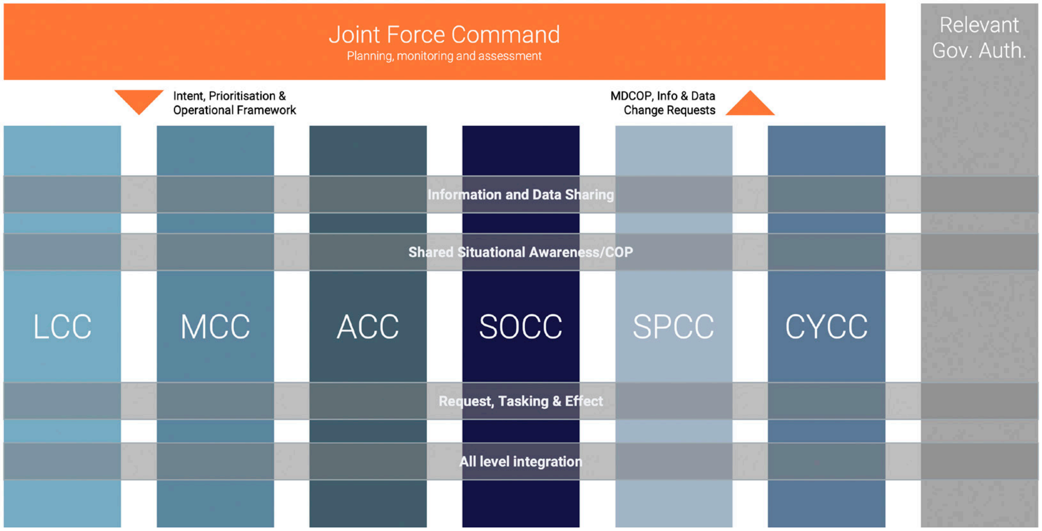
Implementation of the MDO concept will in principle change traditional hierarchical relations towards collaborative relations also outside the military environment, where the communication and exchange of data and information is more horizontal between component entities than vertical up to the Joint Force Command.

The same process will probably change the present task-centric approach to an effects-centric collaboration. As a vital part of this reformation, you will probably also see a change from a platform-centric to an information-centric way of looking at capabilities, where the need for generation of information takes precedence over specialized platform(s), a change also driven by the implementation of 5th generation multi-mission capable platforms, sensors and means of communication.

Full implementation of the principle of "Mission Command" will be essential for the journey towards true MDO, and it will most likely also change the role and tasks of the Joint Force Commander towards intent-based leadership. The joint plans will then change from tasking components to give the overall intent and prioritization of effects for a given time period. Also the plans will provide the operational envelope from within the subordinate components and commanders can act without seeking approval from higher headquarters. Monitoring ongoing operations, assess incoming data and information, and handle requests from components to change prioritisations, envelope limits etc. will be the future basis for the operational workflow.



Simplified principle for the traditional Joint Operations set-up.


Joint Force Command
Planning, monitoring and assessment
Relevant Gov. Auth.
Intent, Prioritisation & Operational Framework
MDCOP, Info & Data Change Requests
Information and Data Sharing
Shared Situational Awareness/COP
LCC
MCC
ACC
SOCC
SPCC
CYCC
Request, Tasking & Effect
All level integration

Simplified principle for MDO. In this figure, Space (SPCC) and Cyber (CYCC) are depicted as separate components. However, many nations include Space in the Air Component and Cyber incl. EMS is integrated in all components.

The MDO challenges

The addition of the Cyber and Space domains into the classic operational framework for Land, Maritime, Air and Special Operations increases the amount of data available for MDO and the complexity of the planning and execution processes. This also presents new challenges for the C4ISR[3] systems necessary to support MDO. The system architecture must enable commanders to

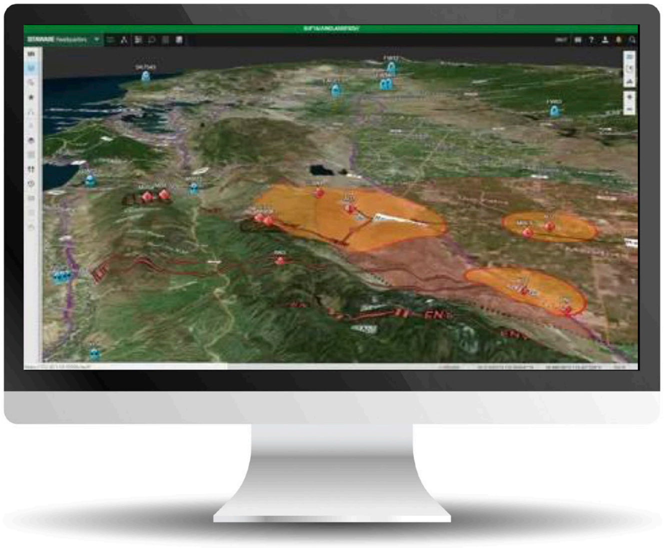
- Rapidly understand the battlespace,
- Direct forces faster than the enemy, and
- Deliver synchronized combat effects across all domains.

Sharing and managing data and information

Access to and sharing of data and information between domains, Service and functional components and non-military authorities will be an important prerequisite for successful MDO. However, users and different systems will be overwhelmed if the vast quantity of information and data is available for everyone at all times. MDO requires a framework to determine who needs what information at what time. Thus, information and data management – ensuring the right information reaches the right person and/or role at the right time – will be a vital function in MDO. Compared to the present situation, future data and information sharing will be dependent of closing air gaps between different security domains and networks, allowing data and information to flow using Automatic Security Gateways.

The application of Artificial Intelligence (AI) and Machine Learning (ML) to sort, filter, and expand data and information will enable the effective use of the vast amount of data and information including

[3] Command, Control, Communication, Computers, Intelligence, Surveillance and Reconnaissance



Example of a User Defined Operational Picture

the option of using AI/ML for decision support to speed up the decision cycles.

Interoperability and connectivity

Present joint environments are dependent on legacy C2 systems impeded by multiple barriers, including domains, classification levels and the Services themselves. Instantiating MDO, however, relies on rapid and dynamic communication between numerous dissimilar capabilities and platforms, setting new requirements for the interoperability between different C4ISR systems in the services as well as between participating nations. Being able to integrate with and navigate amongst multiple interoperability standards is a core prerequisite for carrying out MDO.

Establishing and maintaining connectivity between domains and networks is another main challenge for entering the world of MDO, and it is vital for the sharing of data and information and for the distribution of a Multi-Domain Common Operational Picture (MDCOP). Ideally, all communication will be established by setting up robust, flexible, self-synchronizing MESH networks that ensures resilience and effective use of available bandwidth in both high-capacity nets between higher headquarters all the way down to tactical, highly mobile radio networks.

Multi-Domain shared Situational Awareness

The vast amount of available data and the complexity of MDO requires establishing a MDCOP in which disparate data sets from all domains is aggregated, correlated and fused to improve situational awareness and to provide better information to strategic, operational, and tactical decision makers. As the complexity of the decision space for C2 increases, the need for intuitive decision supporting displays and interfaces grows as well.

The MDCOP display may be layered and filtered to convey the right information to the decision makers and operators, so they are able to rapidly analyze different options and track execution of operations. Displays should have the ability to be preconfigured based on the role of the operator, but they must also have the built-in flexibility to be reconfigured to a User Defined Operational Picture (UDOP) to meet the desires of the individual.

Intelligence

The introduction of Space, Cyberspace and the deployment of 5th generation platforms and sensors entails a large increase in data available for intelligence analysis. It is vital to ensure that essential information and data is detected, identified, analysed, and turned into useful intelligence products. The time from detection, identification, and analysis to decision and action must be as short as possible to present an advantage inside an adversary's decision cycle. This shows the need to make intelligence an integrated part of C2 by integrating the workflows, shortening the processing cycles, and increasing the availability of timely information to the decision makers.

However, the analysts and systems can be overwhelmed by the vast amount of data, presenting a problem that cannot be solved only by an increase in manning or by increasing the storage capacity of C2 and intelligence systems. Instead, this calls for assistance from Artificial Intelligence/Machine Learning, preferably integrated with the C4ISR system supporting MDO.

Multi-Domain Operational Planning and Tasking

Planning for MDO, the Commander's responsibility is to assemble a plan from available inputs and specialised capabilities, provided through services or functional components. They need to apply the most appropriate ones for the contingency at hand and use the right ones at the right place and at the right time to achieve strategic, operational and tactical objectives.

The planning processes and procedures are still very traditional and – normally – time consuming. The "need for speed" calls for

a high degree of collaborative planning, flexible planning tools, and a dynamic approach to the planning process. A Commander who wants to destroy or disrupt a target should be able to rapidly consider all available capabilities in order to determine which would be most effective, including non-kinetic capabilities e.g., in Cyberspace.

The operator must be able to rapidly analyse different options and courses of action (COAs), select and modify a COA, and track execution of the planned operation. To operate at speed, relevant MDO elements need to have the authority to task any and all assets relevant to performing their associated function as determined by the intent, prioritisation and operational framework given by the Joint Force Commander – irrespective of the Service or domain from which that capability is drawn.

Data Logistics

Entering the data- and information-centric world of MDO requires policies, procedures and technology used for the collection, storage, governance, organization, administration, and delivery of a mix of structured, semistructured, and unstructured data in significant volumes. Cloud-like constructs seem the obvious solution, but in the military environment, data and information must be available in a highly distributed environment at different levels and protected from an adversary's attempts to destroy, infiltrate, or access essential data. Difficulties in maintaining connectivity in a Denied, Disrupted, Intermittent environment with limited bandwidth (DDIL) can also make cloud-like services difficult or impossible to achieve.

Thus, setting up a robust data supply chain with a resilient MESH network structure is an essential prerequisite for performing MDO.

SitaWare – enabler of MDO

Since MDO is in a constant evolution with resulting changes in requirements, the **SitaWare** Suite offers the best development potential for integration of the different domains, including the necessary communications infrastructure and integrated workflows.

Introduction to the SitaWare Suite
The **SitaWare** Suite consist of

- **SitaWare** Headquarters, C4ISR functionality for Headquarters functions from joint to lower level, incl. ships.
- **SitaWare** Insight, providing a data-lake, intelligence tools incl. AI/ML, IRM & CM as an integrated add on to SitaWare Headquarters.
- **SitaWare** Frontline, mounted Battle Management.
- **SitaWare** Edge, handheld for the dismounted soldier.
- **IRIS** military messaging systems and interoperability.

The **SitaWare** suite has built-in communications; **SitaWare** Headquarters Communication (SHC) for communication between various Headquarters and **SitaWare** Tactical Communication (STC) for communication from headquarters all the way out to the dismounted commander.

SitaWare Headquarters can support multiple user communities without attempting to provide a one-size-fits-all type of product. Users in the different domains have different needs, different conventions and different processes.

However, there are also a lot of similarities and common needs. The commonalities between the domains are located in the **SitaWare** Core system and the specialties for each domain can be applied as a plug-in configuration.

Through this approach users in each domain will be met with a system that is tailored to their particular needs, conventions and processes, while still being able to interoperate with users in the other domains and thus achieve the Multi-Domain vision for intra-operability and shared situational awareness.

SitaWare Headquarters features an open architecture and public application programming interface (API) that enables extensions and integration with other systems. The client-side API allows add-on modules and customised features to be incorporated into a deployable solution. The server-side API facilitates integration with third-party systems and data feeds.

SitaWare contains potential interoperability between **SitaWare** and Cyber and Space SA systems, so that the system can truly support the vision of MDO and provide intra- and interoperability across the board, supporting new ways of working.

SitaWare Headquarters, **SitaWare** Insight and **IRIS** products are all browser-based client applications, allowing the three products to be tightly integrated into one solution and providing the end-user with both operational simplicity and a powerful C4ISR capability for MDO.

Information sharing and – management

The **SitaWare** Suite network enables information sharing across all units and echelons via its built-in communication mechanisms. Information and data from functional components e.g., Cyber and Space can be imported directly using one or more interoperability standards.

Management of the information sharing can be carried out in **SitaWare** Headquarters by setting up software-controlled contracts between entities, roles and/or functions in the SHC and STC networks.

Interoperability and connectivity

Interoperability and connectivity are vital prerequisites in the MDO environment, both for information-sharing and for exercising Command and Control. The **SitaWare** Suite of C4ISR systems ensures both top-to-bottom interoperability from the Multi-Domain Headquarters all the way across the Joint Force down to the individual unit or soldier, as well as interoperability with allied and coalition forces, government authorities and non-governmental organisations (NGOs).

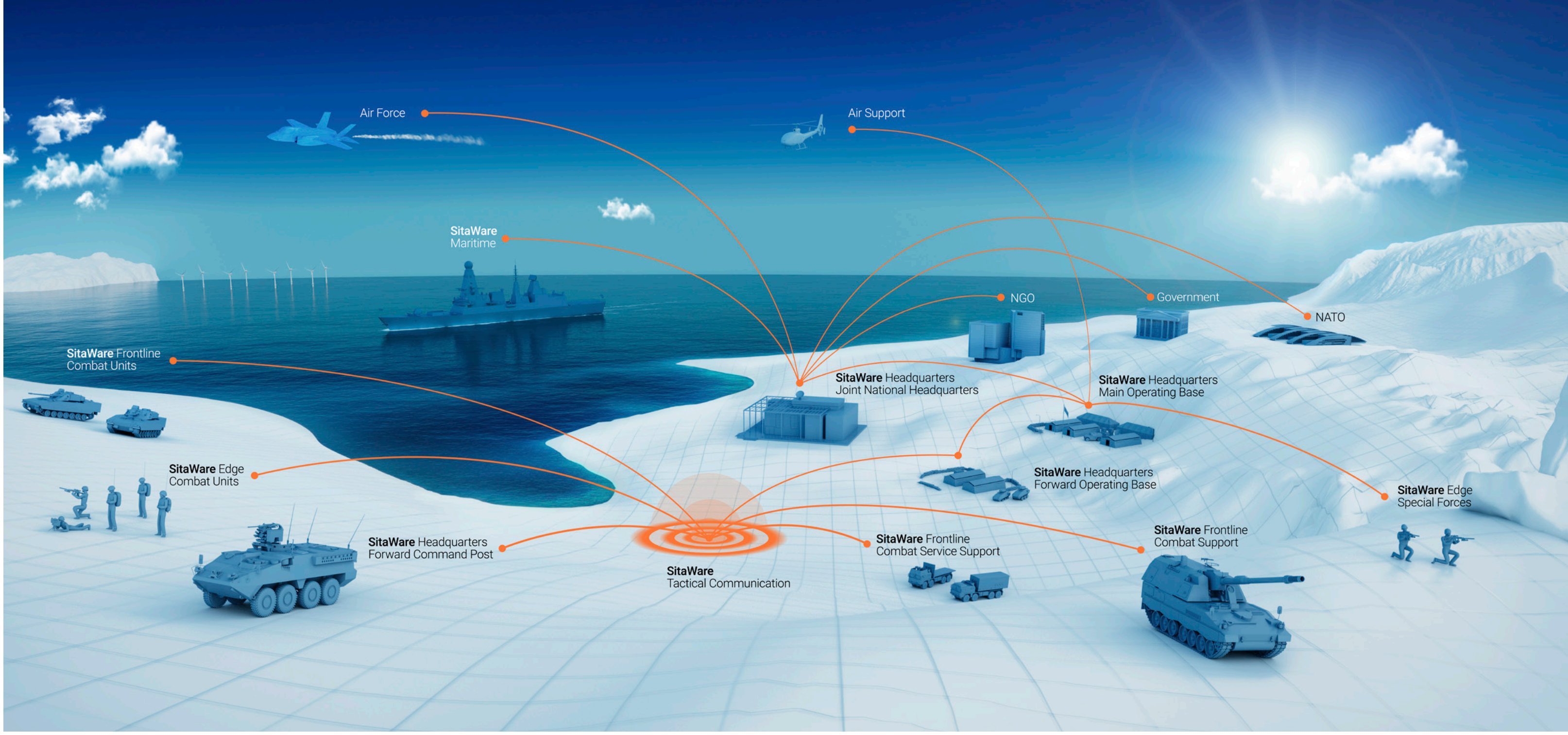
Connectivity and integration across the **SitaWare** Suite is enabled by the use of the built-in communications:

- **SitaWare** Headquarters Communication (SHC) for connecting multiple SitaWare Headquarters nodes and supporting organisation clusters, e.g., forward, rear and main HQ, and
- **SitaWare** Tactical Communication (STC) for connecting mobile nodes in a radio MESH network.

Both networks are self-synchronizing, and while SHC is designed for high capacity, high bandwidth networks, STC ensures connectivity on radio networks with low bandwidth and under DDIL conditions. SHC and STC enable connecting sensors to shooters, but this is only one of the many demands for connectivity to support information sharing and MDO C2, which **SitaWare** can fulfil. **SitaWare** supports a vast amount of interoperability standards and has a proven record for facilitating interoperability between different systems. **SitaWare**'s open architecture allows for the integration of third-party tools into the networked environment, enabling collaborative planning and execution of operations across the various domains.

The **SitaWare** Suite is in use with more than 50 nations worldwide – including US, UK, Germany, Sweden, Denmark, Finland, New Zealand and Ireland.

Systematic products have been tested intensively in NATO interoperability test and exercises. Our customers have participated in CWIX and Combined Endeavour for more than 10 years with Systematic's C4I and military messaging handling systems. The countries include, amongst others, Denmark, Norway, Sweden, Germany, and UK.


Air Force
Air Support
SitaWare Maritime
NGO
Government
NATO
SitaWare Frontline Combat Units
SitaWare Headquarters Joint National Headquarters
SitaWare Headquarters Main Operating Base
SitaWare Edge Combat Units
SitaWare Headquarters Forward Operating Base
SitaWare Edge Special Forces
SitaWare Headquarters Forward Command Post
SitaWare Frontline Combat Service Support
SitaWare Frontline Combat Support
SitaWare Tactical Communication

The SitaWare suite is a C4ISR suite which provides a complete solution from the Joint level to the dismounted soldier connected via SitaWare Tactical Communication (STC) from Headquarters to Frontline and Edge and SitaWare Headquarters Communication (SHC) between various Headquarters.

Multi-Domain shared Situational Awareness.

SitaWare Headquarters provides Multi-Domain shared situational awareness for monitoring the situation, making assessments, and supporting the continuous planning and direction of operations. In a MDO environment with many different contributors, the analysts, planners, and directing personnel need structured access to a geospatial overview of the situation as well as to other information in relation to the operational and general environment in the Joint Operations Area (JOA). The capability is separated into two connected parts. One part is based on the Multi-Domain Common Operational Picture (MDCOP) and the second part is based on structured, semi-structured and unstructured data, imagery, videos, documents, sheets, presentations etc. collected and stored by **SitaWare** Insight in a structured manner, accessible and searchable for authorized users.

The Multi-Domain Common Operational Picture (MDCOP)

SitaWare Headquarters enables the user to compile, view and edit a MDCOP. A multilayer concept enables the MDCOP to be a hub for all tracks and battle space objects as well as Space and Cyber information in near real time and with the ability to perform correlation and fusion of tracks. The MDCOP is able to automatically transfer information internally in the organization as well as with other partners and agencies through one of **SitaWare** Headquarters' existing interoperability protocols.

The process of building a MDCOP during MDO is significantly more complex than just collecting and fusing data. Processes, both automated and human, must be in place to analyze and disseminate the results at the proper organizational level. This process is consistent with the JDL model levels 1-4. The process is continual with all aspects occurring concurrently.

1 **APP-11**
NATO Message Catalogue
ADATP-3

2 **OTH-GOLD**
Over-the-Horizon-GOLD

3 **AIS**
Automatic
Identification System
Civilian Maritime Tracking

4 **CoT**
Cursor-on-Target

5 **USMTF**
United States
Message Text Format

6 **MISB**
STANAG 4609
Motion Imagery (UAS Video)

7 **LINK 16 SIMPLE**
STANAG 5602
Standard Interface
for Multiple Platform
Link Evaluation

8 **LINK 16 JREAP**
STANAG 5518
Joint Range Extension
Applications Protocol

9 **ADS-B**
Automatic Dependent
Surveillance - Broadcast

10 **XMPP**
Extensible Messaging
and Presence Protocol

11 **NVG**
NATO Vector Graphics

12 **KML**
Keyhole Markup Language
Export to e.g. Google Earth

13 **NFFI / FFI**
STANAG 5527
NATO Friendly
Force Tracking

14 **MIP**
Multilateral Interoperability
Programme 3.1 and 4
JC3IEDM & MIM

15 **VMF**
United States
Variable Message Format

16 **ASCA**
Artillery Systems
Cooperation Activities

The SitaWare suite supports a wide variety of Interoperability Standards enabling an integrated collaboration environment for MDO

Managing the MDCOP

The picture management of **SitaWare** Headquarters uses a layer technology which overlays the collated information from different sources and displays it in layers to create an overview. An essential part of developing situational awareness is access to detailed and precise geographic information for the area of operation. The map and chart display in **SitaWare** Headquarters supports a large variety of map and chart formats as basis for the MDCOP, plans, intelligence pictures etc., providing the user with precise geodetic information and references.

The integration of **SitaWare** Headquarters and **IRIS** military Messaging system allows for the import and export of multiple messages and forms, of which some can be displayed on the MDCOP e.g., the Air Tasking Order (ATO) and the Airspace Control Order (ACO). **SitaWare**'s open architecture and API's also enables data and pictures from external sources e.g., Cyber and Space to be imported for display on the MDCOP.

Intelligence

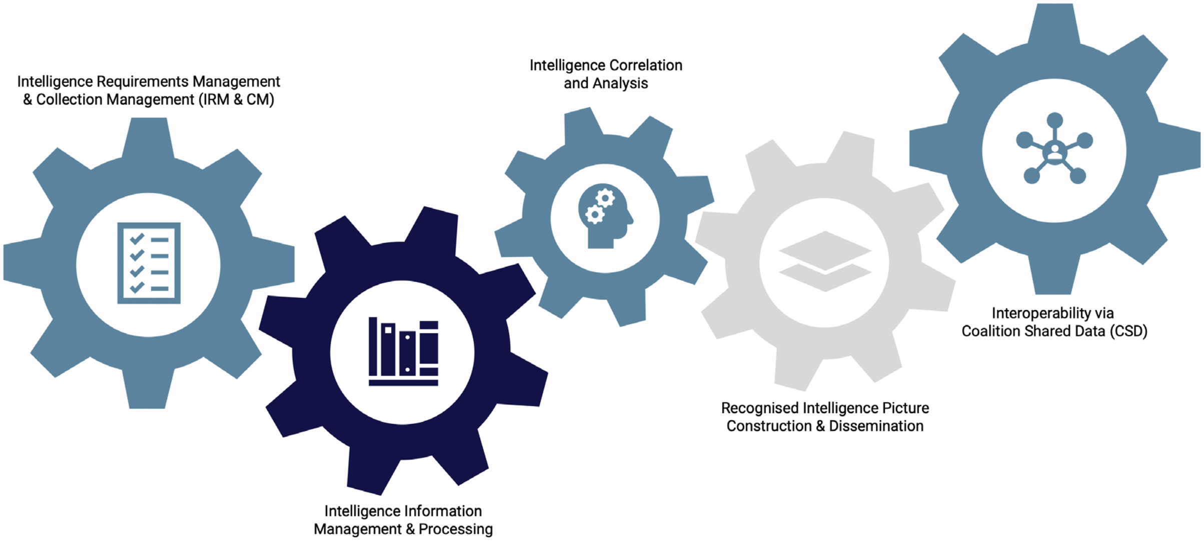
Despite the increase in complexity and amount of available information and data in the MDO environment, the classical purpose of the intelligence processes remains the same.

SitaWare Insight provides the **SitaWare** Suite with a dedicated tool for intelligence in a MDO environment. Fully Integrated with **SitaWare** Headquarters, it enables the integration between the intelligence cycle and the operational cycle.

SitaWare Insight supports the intelligence workflows for activity-based intelligence and intelligence preparation of the battlefield and it contains tools for Intelligence Requirements Management and CollectionManagement.

It provides the basis for implementation of Artificial Intelligence (AI) solutions for analysis and decision support, automated data processing and a seamless integration with **SitaWare** Headquarters, enabling sharing of intelligence information and intelligence products through headquarters interoperability gateway, SHC/STC and integration with one or more Coalition Shared Databases.

SitaWare Insight is providing the platform for the data lake, giving the intelligence analysts a data-centric platform for developing fast intelligence products, e.g. using AI assistance in a demanding MDO environment. **SitaWare** Insight enables the user to search


Intelligence Requirements Management & Collection Management (IRM & CM)
Intelligence Information Management & Processing
Intelligence Correlation and Analysis
Recognised Intelligence Picture Construction & Dissemination
Interoperability via Coalition Shared Data (CSD)

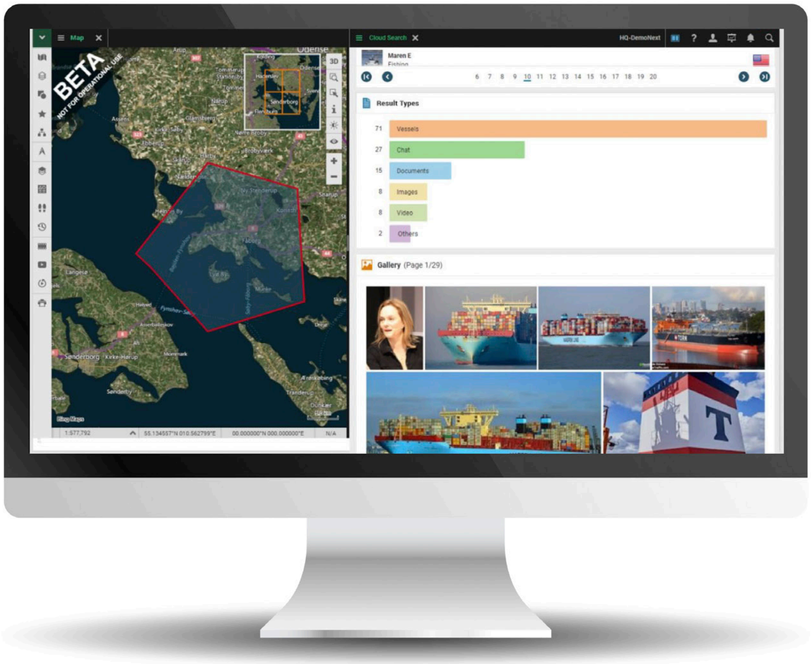
The Intelligence capabilities of SitaWare Insight.

in space and time, create dashboards, search from and annotate battle space objects, and receive notifications for Conflict Of Interests (COI).

SitaWare Insight is the backbone for information and data storage in the **SitaWare** MDO solution. **SitaWare** Insight is designed to ingest data of virtually any kind – including virtualisation of data from other systems. Regardless of the data type, a federated search index for the entire data lake enables users to search across all the data in **SitaWare** Insight.

Using **SitaWare** Insight as a web-based portal to manage information can centralise control of accessibility. Users can organise information into different folders which may have specific permissions, ensuring access to different information at different levels, but at the same time enabling timely distribution and sharing of vital information to the right receivers.

Multi-Domain Operational Planning and Tasking
The **SitaWare** Suite supports the collaborative planning processes with multiple input integrated into the plan and order complex. **SitaWare**'s open architecture enables input from both functional components, external sources, superior, same level, and subordinate headquarters/commands. **SitaWare** Headquarters provides the core functionalities for MDO planning, while **SitaWare** Insight provides the tools for a comprehensive system analysis (political, military, economic, social, information and infrastructure factors) in the area of interest as basis for the operational appreciations, center of gravity analysis and operational design leading to a Concept of Operations (CONOPS).



Example of the result of a search for available information within a defined time and space. The search result is presented in a set of widgets some are used to filter your search results and others are used to display the data in different ways.

SitaWare Headquarters directly supports the development of Courses of Actions (COA) as part of the planning process, including composition of the actions/tasks needed to fulfil the mission. It enables working in different workspaces e.g. Blue (Own), Red (Enemy) and Green (Neutral/Civilian) for the development of COAs and ECOAs (most dangerous/most likely). COA evaluation can either be supported as war gaming using **SitaWare** Headquarters graphical overlays or in a numerical evaluation using predefined templates.

The collaborative planning capability allows the authorisation and distribution of orders in stages. This means that the Commander can authorise a partially complete plan and send it to his subordinates during the planning process. This allows the subordinate components to start their own planning much earlier, thereby saving valuable time in the process. A plan can include several overlays (layers) for illustration of plan aspects such as course of action, campaign plans, prioritised targets, maneuver, 4WGrid, mobility, logistics sites, and intelligence.

Complex task-based mission planning often involves scheduling and deconflicting individual unit and sub-unit tasks and sub-tasks. The synchronization matrix tool automatically generates an overview based on the task and timing information defined in the plan overlays and the resources assigned from the plan's task organization. The matrix can be attached to the relevant plans and overlays and can also visualise tasks and activities which are unassigned to the actual task organisation, e.g. Cyber and/or Space activities.

Integration of Functional Area Tools

The information management framework and **SitaWare**'s open architecture allows third-party tools to be an integrated part, providing capabilities such as:

- Chemical, biological, radiological, and nuclear (CBRN) analysis tools such as Bruhn Newtech's CBRN-Analysis application that automatically calculates the CBRN-predicated area and can display that information on **SitaWare** Headquarters' Geographic Information System (GIS). The same data is used to identify key interest areas and units that are at risk.
- Cyber Infrastructure, Nodes and Threat Assessments. Geo-referenced information can be imported and visualized on **SitaWare** Headquarters GIS.
- Direct access from **SitaWare** Headquarters to various dashboards and widgets, e.g. Vessel Data base information.
- Import and visualization of space asset coverage on the JCOP and in plan overlays.

Data Logistics

Performing MDO is heavily reliant on the collection, distribution and storage of large amounts of data available from the tactical edge to the headquarters and enterprise levels. Data must be distributed and accessible through the entire MDO network and at the same time be protected from destruction, spoofing and exploitation by adversaries.

The data supply chain and **SitaWare** Insight can collect and store live and historical data and information through the entire network enabling:

- Transfer of data to the largest storage and processing resources.
- Further analysis and investigation (painting the bigger picture)
- Provision of advanced decision support using artificial intelligence.
- Train artificial intelligence algorithms.
- Support of the use of data for briefings and lesson learned processes.

The data supply chain is also able to provide centrally managed data and information from the Headquarters/Enterprise level to the tactical edge, such as:

- Maps, ORBATS, platform databases etc.
- Software updates
- Centrally produced information (intelligence products, weather maps etc.)

Data are exchanged via either an encrypted wireless network or – in the homeland and/or between more static sites – a cabled solution. The capability to store data is different between the sites depending on role, need and server capacity. The data supply chain enables fluent replication and update of data between servers and sites whenever the network allows. However, in case of wireless network failures or blockage, exchange of data can also be done using physical media, such as USB keys, portable harddrives or other storage media. A major challenge for sharing of data and information is different classifications of the individual networks. Systematic's cross-domain solution establishes a gateway which allows the transfer of data between lower and higher classified networks, e.g. from a restricted network to a secret network enabling the smooth sharing of data and information.

The combination of **SitaWare** Headquarters and **SitaWare** Insight in a data supply chain set-up enables data and information handling between deployable and static entities and Headquarters as well as the transfer of data and information to static, stand-alone data centers to cope with the challenge of storing huge amounts of data for a longer period of time. The data supply chain set-up is data centre agnostic and enables the user to choose a construct dedicated and customized to needs and possibilities.

Conclusion

Systematic delivers an integrated MDO solution built on several commercial-off-the-shelf (COTS) products with the **SitaWare** Suite and **IRIS** as the key applications. The solution consists of a strong set of operational capabilities which can cope with the MDO challenges and at the same time cater for the needs of the individual Services.

The Systematic solution is built on battle-proven COTS software thus introducing minimal risk to cost, schedule, and quality of service. The open architecture in the Systematic solution provides flexibility to adapt to both the current and future operational requirements and enables the interoperability with specialised functional area subsystems that may be selected for additional support not provided by **SitaWare**. The immediate benefits of the **SitaWare** Suite are:

- **SitaWare** Headquarters is a browser-based client application and therefore does not require any software to be installed and maintained on client computers and thus has a much lower cost of ownership compared to competing C4I systems.
- **SitaWare** can interoperate across domains (land, maritime, air, Cyber and Space) by receiving, converting, and forwarding battle space information from/to most modern interoperability standards. This ensures full compatibility and interface with third-party systems and tools including C4I systems for Cyber and Space thereby achieving a truly joint and interoperable MDCOP.

- **SitaWare** can interoperate with coalition partners regardless of whether they are using MIP Block 2, MIP Block 3.0, NFFI, or other prevailing interoperability standards (requires **SitaWare** C2 Server).
- **SitaWare** Headquarters can publish data layers as Keyhole Markup Language (KML) for Google Earth and thereby provide a simple and very cost-effective means for sharing user defined, relevant (classified or unclassified) parts of the MDCOP with civilian authorities, non-governmental organisations, and the media, thus supporting effective Civil-Military Cooperation (CIMIC).
- **SitaWare** offers a wide variety of tools and functionalities, e.g. support for collaborative planning, and
- **SitaWare** built-in communication, SHC and STC, provides the needed connectivity to enable MDO.

SitaWare Insight is designed to enable knowledge discovery and decision support through data fusion and activity-based intelligence and:

- Enables search in space and time, creation of dashboards, searches from and annotation of battle space objects, and also receives notifications for COI.
- Facilitates and enables data and information sharing across domains.
- Supports the cycle of intelligence processing.
- Ingests all kinds of data; structured, semi-structured and unstructured from the **SitaWare** Suite as well as from other sources.
- Automates much of the data pre-processing. It will employ artificial intelligence to enhance information understanding and perform artificial intelligence processing, e.g. anomaly detection.
- Features custom interfaces to third party systems, which will be enabled via the public APIs and the Software Development Kit (SDK).
- Functions as a distributed data and document repository.

SitaWare Headquarters in combination with **SitaWare** Insight may not necessarily provide the complete solution for MDO. However, with the open architecture, inherent interoperability and the use of COTS products, **SitaWare** is the optimum platform on which to build a solution for the MDO environment.

Systematic has long and proven experience in delivering complete solutions that are integrated into operational environments. Systematic believes in long-term customer relations and is committed to providing the optimal solution. Systematic provides services to adapt the solution to specific requirements if or when they occur. Continuous learning is part of our philosophy, also when it comes to customer projects — our goal is to see the system in operation.

About Systematic

Systematic delivers world-leading command-and-control, military messaging, and electronic warfare solutions – providing commanders at all levels of the battlespace with comprehensive situational awareness and advanced miassion management tools. Operating across domains, our reliable, user-friendly, and operationally proven C4I software has been delivered to more than 50 customers worldwide.

Contact us

Do you want to learn more about Systematic and how our state-of-the-art C4I solutions are raising the bar for mission management across domains all over the world? Contact Systematic Defence to learn more.

Email: systematicdefence@systematic.com

Phone: +45 8943 2000

Web: www.systematic.com/defence