



COALITION WARRIOR INTEROPERABILITY DEMONSTRATION

CONTENTS

Executive Summary	2
Objectives of the CWID	3
Configuration of Systems	4
Supported Processes	5
Logistic Assistance Request	5
Availability and Outlook	6

Software from the SAP® for Defense & Security solution portfolio paves the way for NATO's next-generation command and control systems.

AT A GLANCE

Summary

During the Coalition Warrior Interoperability Demonstration, or CWID, SAP experts demonstrated the effectiveness of software from the SAP for Defense & Security solution portfolio – in particular, its ability to operate decentrally and to seamlessly integrate with command and control information systems (C2IS) used by military forces, ensuring rapid transfer of mission-critical information.

Web Site

www.cwid.js.mil

Key Challenges

- Time-consuming manual tasks
- Lack of integrated processes
- Lack of real-time information to support fact-based decision making

Project Objective

Demonstrate SAP's NATO-compliant interface and effectiveness of SAP® software

Solution and Services

- mySAP™ ERP solution
- Interfaces for military information exchange

Why SAP Solution

- Enables high level of integration
- Complies with ADatP-3 (Baseline 11), the NATO standard format for data exchange
- Supports interconnection of decentralized enterprise resource planning (ERP) systems with the central domestic system
- Provides organizational and resource data for C2IS as well as integrated processes between ERP systems and C2IS

Key Benefits

- Total visibility of resources
- Ability to disseminate information quickly, regardless of location
- Enhanced support for operational planning – for land, sea, and air

Existing Environment

Multiple legacy systems and non-SAP software

Hardware

HP servers and notebooks

Operating System

Microsoft Windows Server 2000 and 2003, Microsoft Windows XP clients

EXECUTIVE SUMMARY

During the Coalition Warrior Interoperability Demonstration (CWID), an exercise conducted by NATO Allied Command Transformation (ACT), SAP experts successfully demonstrated the effectiveness of software from the SAP for Defense & Security solution portfolio. Using a simulated scenario – based on the NATO Response Force (NRF) military command structure – they illustrated the SAP® enterprise resource planning (ERP) system's ability to seamlessly integrate with command and control information systems (C2IS) used by military forces, enabling the rapid transfer of mission-critical information. Of all the participants from 18 nations, SAP was the first organization to offer a viable solution supporting ACT's objective of "integrated logistics."

Lieutenant General Ulrich Wolf, director of the NATO CIS Services Agency, comments, "The participation of SAP as the first ERP provider in CWID clearly demonstrates the benefits our military forces can achieve by seamlessly integrating the command and control systems with the resource information. Total resource visibility is crucial for NATO operations, and the test results reveal that we can support our forces with critical information dedicated to their mission."

In order to expedite data exchange between the ERP and command and control systems, SAP specially developed interfaces in compliance with ADatP-3, the NATO standard format for data exchange. This high level of integration delivered by SAP technology enables the timely transfer of information, which is critical to "net-centric" warfare – in other words, strategies and tactics used to successfully deploy, operate, and support networked forces. The distributed, but logically integrated, network of systems and applications enables soldiers and commanders to seamlessly carry out their tasks, whether they are working in online mode via secure Internet and satellite connections or temporarily disconnected from the command centers.

OBJECTIVES OF THE CWID

Whenever NATO sends troops into conflict areas, it needs to ensure that the computer systems used by each nation's armed forces can effectively communicate across land, sea, and air – which is precisely why NATO developed standards that must be applied to all participating nations' military computer systems. The annual U.S.-led CWID event is where the international community can test new and evolving command and control technologies designed to meet NATO standards and protocols.

“Total resource visibility is crucial for NATO operations, and the test results reveal that we can support our forces with critical information dedicated to their mission.”

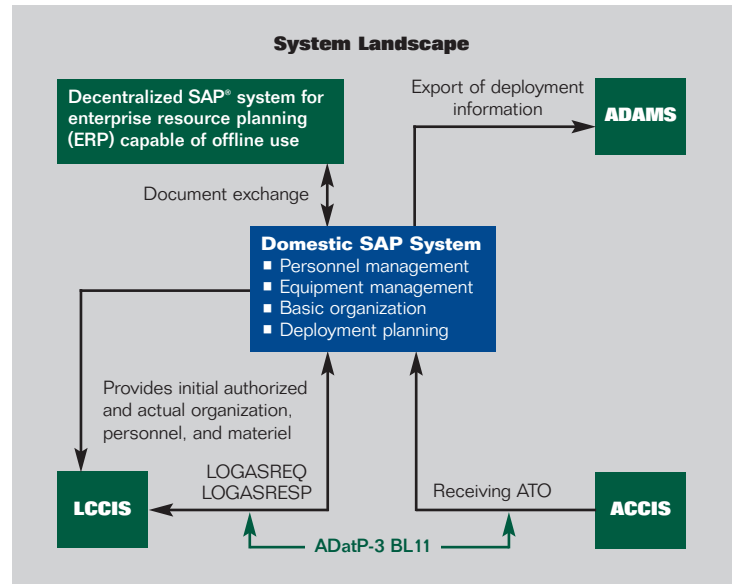
Lieutenant General Ulrich Wolf, Director, NATO CIS Services Agency (NCSA)

Here, government, private industry, and NATO members come together to demonstrate and test technologies in a simulated war-fighting environment.

The goal of CWID is to enhance or enable:

- Mission assurance
- Situational awareness
- Multilevel and multidomain security
- Collaboration information environments
- Intelligence, surveillance, and reconnaissance dissemination
- Wireless security
- Integrated logistics
- Language translation

To this end, SAP demonstrated its new ADatP-3-compliant interface, in conjunction with a special release of its industry-specific software and the mySAP™ ERP solution, during a multinational CWID scenario.



Additionally, the team supported an integrated maintenance scenario, involving personnel on the German frigate Brandenburg, which was located offshore in the Baltic Sea, and staff at central headquarters in Lillehammer, Norway.

SAP contributed to the CWID objectives by:

- Providing the current personnel and materiel information to the NATO Allied Deployment and Movement System (ADAMS) as initial data and to various command and control information systems on a daily basis
- Processing logistic assistance request (LOGASREQ) messages and providing corresponding logistic assistance response (LOGASRESP) messages
- Importing air tasking orders (ATOs) – according to integrated command and control (ICC) software – for further maintenance planning within the SAP line maintenance applications
- Demonstrating the decentralized functions of the software (from the SAP for Security & Defense portfolio) via a distributed personnel and maintenance scenario and remote administration on an offshore frigate

