Contamination Avoidance at Seaports of Debarkation (CASPOD) Advanced Concept Technical Demonstration (ACTD):

A Study in the Importance of Early User Involvement During User Interface and System Capabilities Development

Prepared by:

Donald W. Macfarlane
David H. Drummond
and
William J. Ginley
NBC Battlefield Management Team
Edgewood Chemical and Biological Center
Aberdeen Proving Ground, Maryland 21010-5424

ABSTRACT

The CASPOD ACTD provides a valuable example of how important the early involvement of the ultimate system user is in the development of capabilities and user interfaces. A system with suitable interfaces and adequate capabilities that meets the user's mission requirements can only be developed with a clear understanding of the user's role. The CASPOD Port Warning and Reporting Network (PortWARN) System is an example of iterative capabilities definition and iterative user interface refinement based on war-fighter inputs. The combination of war-fighter interviews, proof of concept demonstration (POCD), limited user assessments (LUA), and CASPOD Preliminary and Final Demonstrations (PD and FD) were all sources for invaluable user input for system definition.

The first step in any successful program is the understanding of the user's mission and mission requirements. Top-level requirements provide a framework for a system based on broad mission needs. By working closely with the war-fighter that will ultimately use the system, the extended detailed requirements can be defined. The CASPOD ACTD Management Plan provided the top-level requirements for a network of detectors and a situational awareness capability. Coordination with the war-fighters from the 377th Theater Support Command, 95th Chemical Company, and 143rd TRANSCOM were used to gain a better understanding of the Seaport of Debarkation (SPOD) mission and to influence the development of the detailed system requirements for PortWARN.

System definition is an iterative process that provides opportunities to get the user feedback necessary to ensure the system is of value to the war-fighter and is designed with usable interfaces. The definition of the PortWARN System was and is an iterative process. An early concept based on initial meetings with the war-fighters was presented at a POCD. Valuable feedback was gained that influenced both the capabilities of PortWARN, as well as, the user interface with the system. The feedback was used to refine PortWARN and provide a more valuable toolset for the next opportunity to gain user feedback (i.e., LUAs, PD and FD). The process will continue as PortWARN is installed and trained at the Kuwait SPOD.

Table of Contents

INTRODUCTION

Every successful program takes the needs and requirements of the user in consideration when the design alternatives are being evaluated. The best way to ensure the needs and requirements are met is to get early buy in from the user community and have defined points where the user can test and evaluate the system. In this way, feedback on system deficiencies can be provided to the developer and incorporated into the final product. An iterative process of design, technical test, user evaluation, redesign and retest is required to field a product that will provide a valuable asset and not just a memory hog that only takes up space on the hard drive.

The first step in any program is to identify the overarching requirements for a system. These are generally defined in a Mission Need Statement, Program Management Plan, and more specific requirements could be defined in an Operational Requirements Document (ORD). The lower level detail requirements are the points where specific users or user types need to be considered. In determining the final capabilities of any system, the environment in which it will be used will also be a major consideration.

The steps, procedures, and coordination trail that is required to get to that valued end product which gives the war-fighter a needed or improved capability will be described in the next pages. The focus here is on the interaction of the user with the developer and how both feed into a successful program. The developer can bring state of the art concepts and innovative technology to meeting the war-fighters needs, while the war-fighter brings the reality of mission needs and the mission environment.

The Contamination Avoidance at Seaports of Debarkation (CASPOD) Advanced Concept Technology Demonstration (ACTD) is a prime example of how the developer and the war-fighter can come together to influence system requirements and capabilities. The CASPOD ACTD followed, and is still following the iterative process to link new and emerging technology with real world mission requirements. The focus of the following discussion is on the information technology (IT) and detection network requirements for the CASPOD ACTD.

WHAT IS CASPOD?

The CASPOD ACTD is a 5-year program to address and demonstrate those mitigating actions taken before, during, and after an attack to protect against and immediately react to the consequences of the chemical or biological (CB) attack at a Seaport of Debarkation (SPOD). These actions aim to restore operating tempo in mission execution and the movement of individuals and materiel through a SPOD to support combat operations. The ACTD addresses both technology solutions and doctrinal solutions in order to mitigate the effects of a CB Warfare Agent attack or a release of Toxic Industrial Chemicals (TIC) on force flow and operational tempo within a SPOD.

The Edgewood Chemical and Biological Center (ECBC) has been tasked as the Technology Integrated Process Team (IPT) for the CASPOD ACTD. The IPT has been tasked with identifying existing and emerging technologies with applicability to CASPOD in the functional areas of Detection, Decontamination, Protection, Medical and Information Technology (IT). The initial 3 years of the ACTD focused on the identification and evaluation of applicable technologies in each of the functional areas and the final 2 years are focused on residual support and transition of the downselected technologies. The CASPOD ACTD has completed the evaluation phase of the program and is now in the final 2 year Residual Support Phase.

The focus of the discussion on the user/developer interaction provided in the following pages is directed at the IT Solution that was implemented for the CASPOD ACTD in the form of the Port Warning and Reporting Network (PortWARN). The discussion is however, just as relevant to the other functional areas.

THE BEGINNING – BASIC REQUIREMENTS

The mission capability or more accurately the lack of a mission capability is the starting point for defining requirements for any program. The CASPOD Management Plan provides the basic requirements for IT capabilities. The basic requirements are broken out into 4 requirements.

1. Network of Detectors. Identify a networked system of detectors that can detect to warn SPOD command center, as well as, USCENTCOM and USTRANSCOM Joint Operations Centers.

2. Situational Awareness. Provide situational display on a common user system that gives the Commander an overall defense picture of the port, such as contamination, fires, locations of unexploded ordinance, battle damage assessment, etc…

3. Port Warning. Provide integrated alert and warning system not reliant on local power grid, providing repetitive visual and audible warning announcements to port workers.

4. CENTRIXS Compatibility. Network software/operating system must be compatible/interoperable with current and the projected Combined Enterprise Regional Information Exchange System (CENTRIXS) C2/Information system.

These basic requirements are top level with no direction on how to implement them in a field-able system. This is where the developer/integrator and the user need to begin a collaborative effort and define the specifics for the system. In the case of

CASPOD this was easier said than done. The real world events following 9/11 made the availability of and access to the user community very limited. Developing the concept and adding some specifics to the requirements in the initial days of the program had to rely on limited interaction with the user community and on the past experience of the developers. Drawing on the experience the Tech IPT had with the Restoration of Operations (RestOps) ACTD; the team evaluated available technologies and developed a concept for what would ultimately become the Port Warning and Reporting Network.

THE ORIGINAL/ BASELINE CONCEPT

The original or baseline concept was for an integrated solution to meet the four top-level requirements since no single system or tool met all the requirements. The CASPOD Information Technology Working Group (ITWG) worked towards a solution that would integrate the network of detectors with port warning, NBC modeling, and NBC reporting all controlled from a central command post. The concept that emerged was to have detection nodes that could have four or more different sensors connected at each node. The configuration of each node could vary to provide the maximum coverage possible. Each detection node would be connected to the central command post via radio or Ethernet. Each detection node would be capable of connecting to a port-warning module and providing the path for controlling the port warning from the command post. The Remote Data Relay from Sentel was selected for use as the backbone of communications between the detection nodes and the central database.

Figure 1 – Remote Data Relay (RDR)

The sensors to be integrated in the network would be a combination of currently fielded chemical and biological warfare agent detectors, toxic industrial chemical, weather sensors, and global positioning systems. The ITWG worked closely with the Detection working group to identify the detectors to be integrated into the network and to obtain the detector interface control documents. The CASPOD IT Network Schematic is depicted in figure 2.

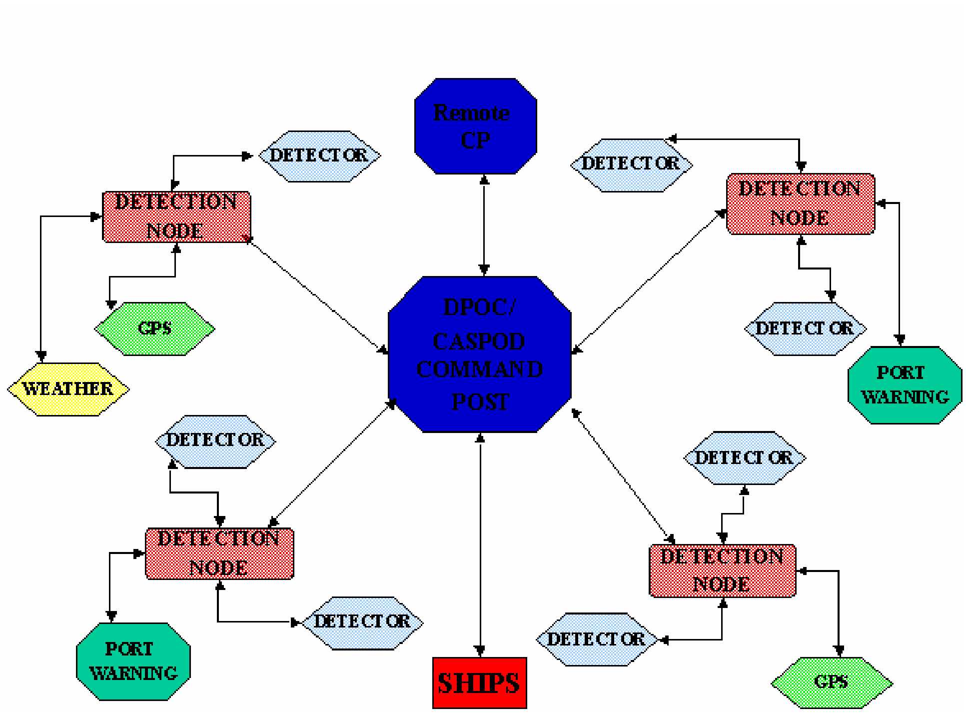

Figure 2 – CASPOD Detection Network Concept

The Restoration of Operations (RestOps) ACTD provided the basis for the situational awareness capability in the form of the RestOps Information Management (ROIM) System. The ROIM System would be used to the maximum extent possible per the CASPOD Management Plan. The ROIM tools provided the situational awareness mapping, NBC messaging, hazard prediction and hazard plotting. The sweep tool component of ROIM provided a quick and easy method for inputting sweep results. As the concept of operations (CONOPS) was further defined, the locations and number of workstations were to be determined. As a minimum, the Command Post would also serve as a workstation. The ROIM tools had significant and successful testing during two Functional Tests conducted at the Air Force Research Laboratory (AFRL) and during the Combat Effectiveness Readiness Exercises (CERE) at Osan Air Force Base in FY02.

Figure 3 – RestOps Information Management System in use at Osan AFB

The port warning system provides a visible and audible warning using commercial off the shelf technology. Several vendors were identified and the selection of the final configuration was made based on factors such as ease of use, network compatibility, power, size, cost, etc… The port warning system selected would have an interface with the network to allow the quickest possible warning to the port workers.

The Remote Data Relay (RDR) is a Sentel Corporation product that provided connectivity of disparate sensors, remotely located sensors and other electronic devices into a single, integrated network. The output of each sensor can be monitored from the CASPOD command post. Each RDR can connect up to 8 serial devices and 3 digital control devices. Each RDR can be connected to the command post via radio or Ethernet.

This original or baseline concept was ready to test and the time had come when user input was desperately needed to identify the shortcomings from an operational point of view. The system was briefed to the potential users of the CASPOD technologies. The first in a series of limited user assessments and demonstrations was scheduled. These assessments and demonstrations provided the mechanism for gaining user feedback, but first the users had to be identified.

IDENTIFYING A USER AND THEIR MISSION

The time had come to get the user involved and in the case of CASPOD we sought the help of the 95th Chemical Company, 143rd Transportation Command

(TRANSCOM), Surface Deployment and Distribution Command (SDDC), and 377th Theatre Support Command (TSC). These are the units identified by the Operational Manager (OM) and the sponsoring command, Central Command (CENTCOM) as the main elements for maintaining port operations. The question that was still to be answered was who would the ultimate user of the system be? That question is still being defined today.

Once the potential users have been defined, the next step is to understand the mission of those users. To understand the mission of the users, time needs to be spent with the men and women learning and understanding their roles and responsibilities. This proved more difficult in CASPOD than in RestOps. With RestOps we had a well established user with defined timelines for quarterly CERE that provided ready access to observe operations. CASPOD came along at a time when real world operations made access to the units limited and much more difficult.

We were able to visit the 377th TSC in April of 2002 and the 95th Chemical Company in July of 2003. These trips along with visits to the 143rd TRANSCOM Headquarters in Orlando, FL and to SDDC headquarters at Ft, Eustis in Virginia began to lay the groundwork for developing the concept for the CASPOD IT solution, Port Warning and Reporting Network (PortWARN). These visits were very good in providing a rudimentary understanding of port operations and made clear the main mission of the 143rd and SDDC is moving cargo to support our troops. The problem arises when we realized a rudimentary understanding is not enough and a more advanced understanding is required to provide a system that can meet the needs of the user.

The rudimentary education we received provided an understanding of the functions and the organizations that are necessary in moving materiel through the port and onward to the operational units. The missing piece was a clearly defined command structure and a clearly defined set of responsibilities for each organization. The standard operating procedures (SOPs) for port contingency operations were still evolving and will continue to evolve as the CASPOD technologies are rolled in. As we moved into the demonstrations of the CASPOD IT solution, the command structure was a moving target and was defined based on current doctrine for each event.

The demonstrations and limited user assessments were the beginning of the iterative process. The series of technical and operational demonstrations were geared towards evaluating PortWARN and gaining insight into the operator's real world responsibilities.

OPPORTUNITIES FOR USER INPUTS

The CASPOD ACTD built in opportunities for the user community to provide the real world perspective and real world mission experience to the developers and integrators of PortWARN. From early technical demonstrations through deployment of hardware and software, the war-fighters that would be the operators of PortWARN were made available to evaluate the system. In some cases the PortWARN operator used during an event was not likely to encounter PortWARN in his future duty position, but that operator's input was still valuable with regard to the basic user interfaces. In other cases, the players in the Final Demonstration were the ultimate user of the deployed PortWARN system. These operator's comments were doubly important because they addressed the user interface, but more importantly their comments impacted on the performance of their mission and the impact PortWARN had in performing that mission.

The events that took place provided the venues for the iterative approach of design, test, evaluate, redesign, retest, re-evaluate, etc… The events ranged from a Proof of Concept Demonstration through training with a tabletop exercise with the gaining unit as part of Residual Support. The types of events were designed as technical demonstrations follow by operational events to evaluate the military utility of the PortWARN System. Each event provided valuable insight into the user's real world needs, real world force structure, and real world mission as briefly described below.

Proof of Concept Demonstration: A Proof of Concept Demonstration (POCD) is exactly what it sounds like, a chance to demonstrate the CASPOD IT solution capabilities, graphical user interface, and information flow. In the case of the POCD, the demonstration was for the CASPOD Operational Manager, Technical Manager, Military Utility Assessor, and interested parties from the sponsoring command, CENTCOM. The POCD was held at the Air Force Research Laboratory (AFRL) in December of 2002. Training was provided to participants and a limited amount of tabletop exercise play was conducted. This was the first opportunity for the CASPOD Management to see and operate the initial tool set being proposed by the ITWG.

Objectives: There were several objectives to the POCD, both technical and non-technical. The technical objectives included demonstrating: (1) a network of varying sensors for detection, weather, and positioning that provided data to a central database; (2) control of port warning from a central location; and (3) demonstrating data/information. The main non-technical objective was to get buy in to the proposed solution from the CASPOD Management.

Setup: The setup consisted of five detection nodes spread out across the rooftops of AFRL in Rome, New York. The detection nodes were populated with a mix of live sensors and simulated sensors. A command post was simulated in the office space at the lab and several remote clients were set up in adjacent areas of the lab. Port warning and an interface with CENTRIXS were not demonstrated at the POCD. Concepts were briefed but the cost and technical data was still being collected in December of 2002. A wireless capability was setup that demonstrated the ability for the situational awareness data to be transmitted at high speed to make the addition of remote clients a viable option. The wireless capability was not a stated requirement but would come in handy during the Preliminary Demonstration in Aug-Sep 2003.

The software tools demonstrated were the RestOps Information Management (ROIM) System consisting of the SRC 3.0 Map application, digital dashboard sweep tool, and Nuclear Biological Chemical_ Reporting, Plotting and Messaging (NBC_RPM).

Figure 4 – Proof of Concept Demonstration

Limitations: The POCD demonstrated a limit amount of the capability that would eventually be added to PortWARN. The primary focus of the demonstration was on the display of data and ability to provide sensor data in near real-time to the common operating picture.

Information Technology Functional Demonstration: The Information Technology Functional Demonstration was held in of May 2003. The demonstration was conducted at AFRL in Rome, NY and was the first opportunity for members of the 95^{th} Chemical Company and the 143^{rd} TRANSCOM to operate the PortWARN system. The 95^{th} Chemical Company played the role of NBC Officer and the 143^{rd} provided the players for the Port Commander and the Port Manager. Contractors with previous military experience filled the roles of the other staff positions.

Objectives: The objectives of the Information Technology Demonstration were to demonstrate: (1) a network of varying sensors to include detection, weather, and global positioning systems; (2) information flow to a central database; (3) concepts for port warning controlled from a central location; and (4) wireless data transfer. Additionally, the non-technical objective for the demonstration was to spend time with the 143^{rd} and 95th to gain as much information and insight as possible on port operations, decontamination operations, mission responsibilities, command structure, and existing communications and information exchange processes.

<u>Setup</u>: The setup consisted of six detection nodes spread out across the rooftops of AFRL. Each detection node consisted of an RDR and one or more sensors. One node was setup to hand the audible warning using either an omni-directional speaker or a set of bidirectional speakers. Both live sensors and simulated sensors were used to inject data into the system. Live detection sensors were alarmed using confidence tester simulants. The software demonstrated was again the ROIM tools with a few minor additions to give the application more of a port flavor. For hazard modeling, VLSTRACK was replaced by the Hazard Prediction and Assessment Capability (HPAC) to provide a simpler user interface.

The overall system at this point in time was dubbed the CASPOD Battle Management System (CBMS). CBMS would be a short lived name and was morphed into the Port Warning and Reporting Network (PortWARN) by the end of 2003.

<u>Limitations</u>: The Information Technology Demonstration provided a demonstration of the core technologies and some of the concepts that were still being evaluated for PortWARN. The major limitations to the demonstration were both technical as well as operational. The technical limitations included system power, detector availability, and simulation development.

Power was readily available for the detection nodes, but this is not representative of the operational environment. One challenge that was faced later in the ACTD is the design of power supply system for the deployed detection nodes. During the early stages of the ACTD the detection devices being used were generally on loan from vendors or other Government organizations and final selection of detectors was not completed. Until the selection of the detectors to be used by CASPOD was finalized, only limited work would be done on integration of the detectors. The simulation for standoff detection was developed quickly and was labor intensive to create each individual scenario.

The demonstration setting was non-operational and limited training time was available. In order to promote the use of the system to demonstrate its capabilities, the technical team was asked to operate the main screen for the commander. The authors of the mission event scenario list (MESL) for the demonstration had limited experience with regard to port operations and the MESL did not necessarily reflect the port operations very well.

***Preliminary Demonstration*:** The Preliminary Demonstration (PD) was held at the Naval Weapons Station in Charleston, SC in August and September 2003. This was the first of two operational demonstrations used to provide military utility assessment data for the evaluation and final down selection of technologies. The PD addressed all five functional areas of the CASPOD ACTD, but again the focus for this discussion is the IT solution, PortWARN. The participants included the 348th Transportation Battalion, 95th Chemical Company, 807th Medical Company, and SDDC.

Objectives: The main objective of the PD was of course to demonstrate the military utility of the PortWARN system. More specifically, the objectives were for the Tech IPT to demonstrate: (1) integrated PortWARN software; (2) improved visual port warning concept; (3) information flow to include NBC messaging; (4) improve NBC hazard prediction interface; and (5) audible port warning.

Setup: The setup included 10 PortWARN Clients online with the map situational awareness GIS application integrated with the digital dashboard. The NBC_RPM was still a stand alone application tied to the common database. Eight (8) detection nodes were setup in various configurations. The sensors that were integrated into the detection nodes included the LCD-3, BAE JCAD, M22 ACADA, Mobile Chemical Agent Detector (MCAD), GPS, and weather. Audible port warning was integrated into PortWARN and was controlled from the Combined Port Operations Center (CPOC). Visual port warning was provided in the CPOC using a small stackable light and outside using a traffic light configuration. The visual warning was also integrated with and controlled through the PortWARN software. A wireless feed was provided so a client could be placed in the White Cell (Test Control) trailer.

Limitations: The Port Operations Concept of Operation were still being defined at the time of the PD and the participants struggled with incorporating their past experience with the current technology. After Action Reviews (AARs) proved helpful in exploring the capability of PortWARN and how the tools could be employed throughout the MSEL play. Again, the scenarios were limited in scope given the relatively small window of time that the MSELs were played. Some of the technical limitations included the elevation of the speakers and the need to simulate the standoff detection.

Standoff Detection Limited User Assessment: A Standoff Detection LUA was held in May 2004 to address the potential of providing and integrating a standoff chemical detection capability as a residual for CASPOD. The 95th and the 143rd again supported the LUA and played the roles of NBC Cell and Port Commander. The Standoff Detection LUA took place at Dugway Proving Ground, Utah.

<u>Objectives</u>: The objectives of the Standoff Detection LUA were to demonstrate: (1) the suitability of standoff detection with port operations; (2) an integrated standoff detection capability controlled from a central location; and (3) the ability of PortWARN to display standoff detection data in a meaningful way.

<u>Setup</u>: The setup consisted of 10 PortWARN clients online with the fully integrated PortWARN software. Fully integrated in this case means a single application providing the user interface for geo-referenced situational awareness, sweep capability, NBC hazard prediction and modeling, port warning control, standoff detection control, etc… Two MCADs connected to RDRs were used as a representative system for standoff detection. Meteorological data was provided by a met sensors connected to a RDR.

Limitations: The LUA was conducted in a non-operational setting, Dugway and the participants from the 95th Chemical Company were members of a decontamination unit and unlikely to be users of the system in a real world contingency. Simulant releases were limited to a defined area, making it necessary for the detection units to be moved in order to test a various ranges. The units were mounted in Cherry pickers and lowered for transport. Leveling of the detector was done on the ground before elevating it to the operational height. Alignment of the unit could not be maintained using this procedure and could have influenced the results.

Final Demonstration**:** The Final Demonstration (FD) was held at the Port of Beaumont, in Beaumont, TX in August and Sep 2004. The Port of Beaumont is reportedly the busiest military port within the United States. The 143rd TRANSCOM, SDDC, 348th Transportation Battalion, and the Beaumont Fire Department were the participants for the FD.

Objectives: The objectives for the FD were to demonstrate: (1) a fully integrated PortWARN software; (2) improved visual port warning; (3) information flow to include NBC messaging; and (4) integrated hazard prediction.

Setup: The setup consisted of 14 PortWARN clients online loaded with the fully integrated PortWARN software. Six detection nodes were erected with a mix of LCD-3 and M22 ACADA detection systems. Five sites were equipped with port warning light towers and two had speakers systems attached. The omni-directional speakers were ground mounted near the pier and the bidirectional speakers were mounted on a cherry picker for elevation. The unique feature of the setup was there were 7 additional detection nodes simulated and displayed on the PortWARN map.

Limitations: The limitations included: (1) the limited equipment and manpower made it necessary to simulate entire detection nodes; (2) simulant could not be release making it necessary to simulate the standoff detection; (3) speaker was limited due to the proximity to a neighborhood church; and (4) the event scenario was limited in time and scope – no night operations. The FD was the most realistic setting of all the demonstrations and LUAs conducted, but volume of cargo and the volume of people of a real world operation could not be replicated.

RESIDUAL SUPPORT**:** Installation of the PortWARN in an operational port took place in September 2005. The residual support in the case of CASPOD may be the most informative of all the user/developer interactions. A thirty-day visit to the unit gaining the system can be more valuable than all the previous trips and meetings combined. Spending those days on site with the 143rd TRANSCOM and SDDC gained the development team an insight into the real world operations in a port and the expectations of the real world events that impact a port.

Objectives: The objectives of the Tech IPT were: (1) to install the full operating capability of PortWARN with the exception of the audible warning; (2) to provide PortWARN operator training; (3) to validate performance of the deployed network; and to support a table top exercise with the PortWARN operators.

Setup: There were 10 fixed site detection nodes and 3 mobile detection nodes mounted in trailers installed. Each detection node consists of the RDR, LCD-3, light tower; and battery solar panel power assembly. Four PortWARN clients are online with one driving a 50" display.

Limitations: The limitations for the efforts during installation and training included: (1) equipment resources were limited and required dual use as training assets and live system testing assets; (2) early training scenarios were unrealistic; (3) training done offline from the operational network in a classroom setting; and (4) all detections were simulated.

EVOLUTION OF A SYSTEM

The list of technical demonstrations, user assessments, and operational demonstrations is quite impressive for the PortWARN system. Each one of those events provided valuable information from the war-fighter, the port commander, and even from the occasional misplaced person that will be unlikely ever to operate PortWARN again. If you track the changes in the setups for each of the events discussed in the previous pages, you can see the evolution of the PortWARN system from a concept created by the joint experience of a handful of developers to a deployed system with the mark of many users. At the end of each of the events, many comments were received and when technically feasible and where a reoccurring theme was identified, improvements were incorporated into PortWARN.

In 2002, the concept that was called the CASPOD Battle Management System had capabilities with respect to the situational awareness and detection network requirements that were mandated in the CASPOD Management Plan. Three separate software tools provided the capabilities for situational awareness: Survival Recovery Center 3.0, Digital Dashboard, and NBC Reporting, Plotting and Modeling (NBC_RPM). These applications ran independently with different user interfaces, but shared data by feeding a common database. Development of a common user interface was desired to make the training and operation of PortWARN more user friendly. NBC hazard prediction, NBC messaging, and integration of the detection data into the modeling and messaging were other areas that were identified for further refinement. In 2002, the port warning concepts were just beginning to be explored and CENTRIXS was identified as a capability to address later.

The year 2003 brought significant user input, added capability and a new name, PortWARN. The IT Functional test and the PD provided two significant opportunities for the users to have hands on experience with PortWARN and give the

Tech IPT some valuable feedback and insight into port operations and mission requirements. The SRC3 capabilities were integrated into the digital dashboard and HPAC was integrated with NBC_RPM providing simplified user interfaces. Audible and visual port warning was demonstrated, but not finalized as issues like the brightness of the lights and loudness of the speakers were identified. Detection integration with the RDRs was on going for several detectors being evaluated under CASPOD.

In 2004, the Standoff Detection LUA and the FD again brought the user community in direct contact with the developers for a valuable exchange of information. PortWARN was fully integrated with a three components now under the umbrella of the digital dashboard. A TIC detection capability for a limited number of industrial chemicals was added to the LCD-3. A light tower with red, yellow, and green lights was designed, built and tested and received favorable reviews from the participants of the FD. A CENTRIXS Solution was designed and coordinated with the CENTRIX Program Office.

In 2005, a single PortWARN detection node was deployed for environmental testing. A solar panel battery power assembly was designed and built to minimize the logistics burden of powering the PortWARN nodes. The LCD-3 TIC library was expanded to include sulfur dioxide. The PortWARN message center was demonstrated to be compatible with the program of record, JWARN (Joint Reporting and Reporting Network). The PortWARN system was deployed and training provided to the gaining unit. Continued support will be provided throughout 2006 and into 2007 as part of the CASPOD Residual Support Phase of the program. Throughout the Residual Phase, reliability, availability, and maintainability data will collected and refinements and improvements will be added as appropriate to minimize the logistics burden on the unit.

LESSONS LEARNED

Many valuable lessons have been learned throughout the CASPOD ACTD. First and foremost is that user involvement early and often is essential in building a system that has value to the war-fighter. Understanding the mission of the war-fighter that will be using a system early in the development process helps the developer avoid the pitfalls born out of inexperience. Understanding the mission and the deployed environment will help drive the detailed requirements of a system, help generate a more valuable training package, and ensure the system is of value in the field.

No matter how much a system is exercised and tested, the next environment will be different. The environment in this case means a wide range of things that include everything from a physical feature of the location to just the number of detection nodes that are required. In every case the environment for the demonstration and deployment has caused some kind of issue. For example, the PD required the use of the wireless connection and this had been technically tested at the POCD and worked well. Unfortunately, at the PD a line of trees was in the path and added elevation was required. No usable towers were available, so a few quick phone calls were made and two telescoping masts were acquired to add height to the wireless antenna.

Prior to the FD demo the number of users had never exceeded 10 at one time on PortWARN. That number was exceeded and the combination of a large volume of users and a memory leak with the software that wasn't evident during technical testing brought the system to a crawl after a few hours of operation. Some long hours and hard work solved the problem and the FD was completed successfully. The deployment brought several challenges as well, from how to power the detection nodes to how to handle the simulation for training. Power was not readily available and the logistic burden of filling and maintaining generators was unacceptable, so a solar/battery power assembly was design and successfully deployed.

These were just a few examples of how an unknown issue that was not anticipated can cause reworks or the development of creative solutions. The goal is to minimize and anticipate the major hazards, so the minor ones can be handled. One factor that may not ever be able to be anticipated is the human element. The users are not developers and developers are not the users. The developer tends to test in a methodical way and in the same pattern. Unfortunately, real world events and war-fighters in the field tend to do things in a random way. The developer can't foresee all the potential random combinations that could happen and cause problems within a software system. During training for the deployed system one operator opened a minimum of six maps at once and up to 15. Testing had been done with two and possibly three maps opened with no problem. The maps are fairly memory intensive and the additional maps caused the client to lock up. The developers never saw the need for more than a few maps opened at the same time and didn't think to open six let alone 15 maps at once. The main point here is the developer can't replicate every combination of actions in the lab that will be taken in the field.

Training will always be an issue with any fielded system and two points need to be made with that in mind. First, definitely make use of subject matter experts to ensure the training is representative of the unit's mission and the real world threat at the time. Unless the training can be related to the mission and the threat it will be of limited value when a system is called into service for a real world contingency. Secondly, to the maximum extent possible keep installation and training activities separate. This maybe possible either by schedule or by increased resources, but when these activities coincide there is a battle for resources in both equipment and manpower.

In closing, the emphasis is and always should be on the war-fighters and their needs and requirements. Early involvement is essential and can impact favorably every aspect of a system from the system functionality through the system logistical tail. Training is a vital part of any system package and the early understanding of the unit's mission can go a long way in building a training package that provides a representative scenario that prepares the user for real world operations. Again get the user involved early and often.