2010

ROGUEVIDEO

McDowell, Perry

ROGUEVIDEO

www.movesinstitute.org/research-project/roguevideo-research/

Project Abstract

This project has two purposes:

1. To train first responders to cope with a simulated emergency situation while communicating with other departments
2. To streamline protocols and preparation for emergency situations by seeing what doesn't work in a virtual scenario.

Sponsor
EADS

Principal Investigator(s)
Perry McDowell

Point of Contact
Perry McDowell
mcdowell@nps.edu

Real-time Online Game and Use Case Engine for Validating Doctrine in Emergency Operations

Goal:

Improve preparation, prevention, response and recovery by reducing the risk of research, development, transition and adoption of technology; improve our ability to coordinate and test doctrine across multiple agencies.

Approach:

Extend engineer's design tools -architectural frameworks such as DoDAF – so they represent not just equipment, but also doctrine, procedures and expertise. Use existing processes such as exercise planning events to encode both doctrine (how we say we do things) and experience (how we actually do them.) Provide a bridge from these frameworks to synthetic environments to include game engines.

Fire Captain's view of the ROGUEVIDEO game-based doctrine validation framework.

Anticipated Results:

A persistent virtual environment that lets us try engineering prototypes in realistic replicas of operational settings using SME-validated scenarios and doctrine.

Virtual Environment

To simulate and test engineering prototypes, scenarios, and doctrine, an extensive Virtual Environment desktop application has been created. This application lets players adopt roles and participate in live, multi-player scenarios.

Features

- 3D first person view with overhead map displays.
- Enterable rooms and vehicles.
- Extensible inventory system allows scenario designers flexibility in deciding “who gets what”.
- Players can communicate using various devices such as telephone, radio, email, and text messages, just like in the real world.
- Scenario scripting allows for time, position, and actions to trigger events to occur.
- Inventory items can be scripted to fail at the most inopportune time, further testing the doctrine.

Case Study: Cyber Attack Scenario

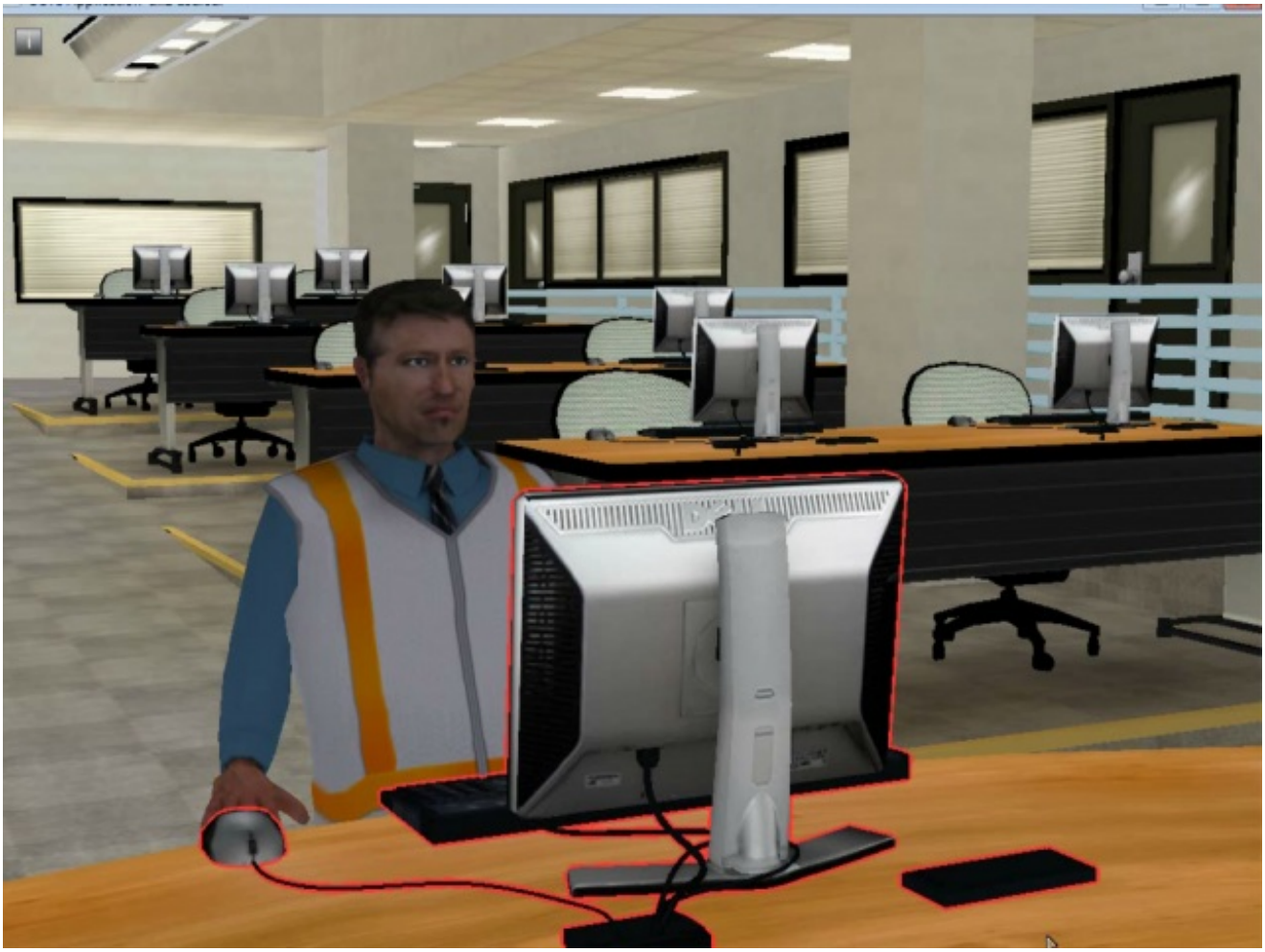
One example of how ROGUEVIDEO can be utilized is the Cyber Attack Scenario, recently added to the ROGUEVIDEO virtual environment. In this scenario, the players use a prototype application on their mobile devices to find the source of a radio signal. The mobile app sends the GPS location and detected radio signal strength to the Head Quarters. The Event Director is monitoring the progress in the HQ using a digital map display which is overlayed with the reported signal strengths.

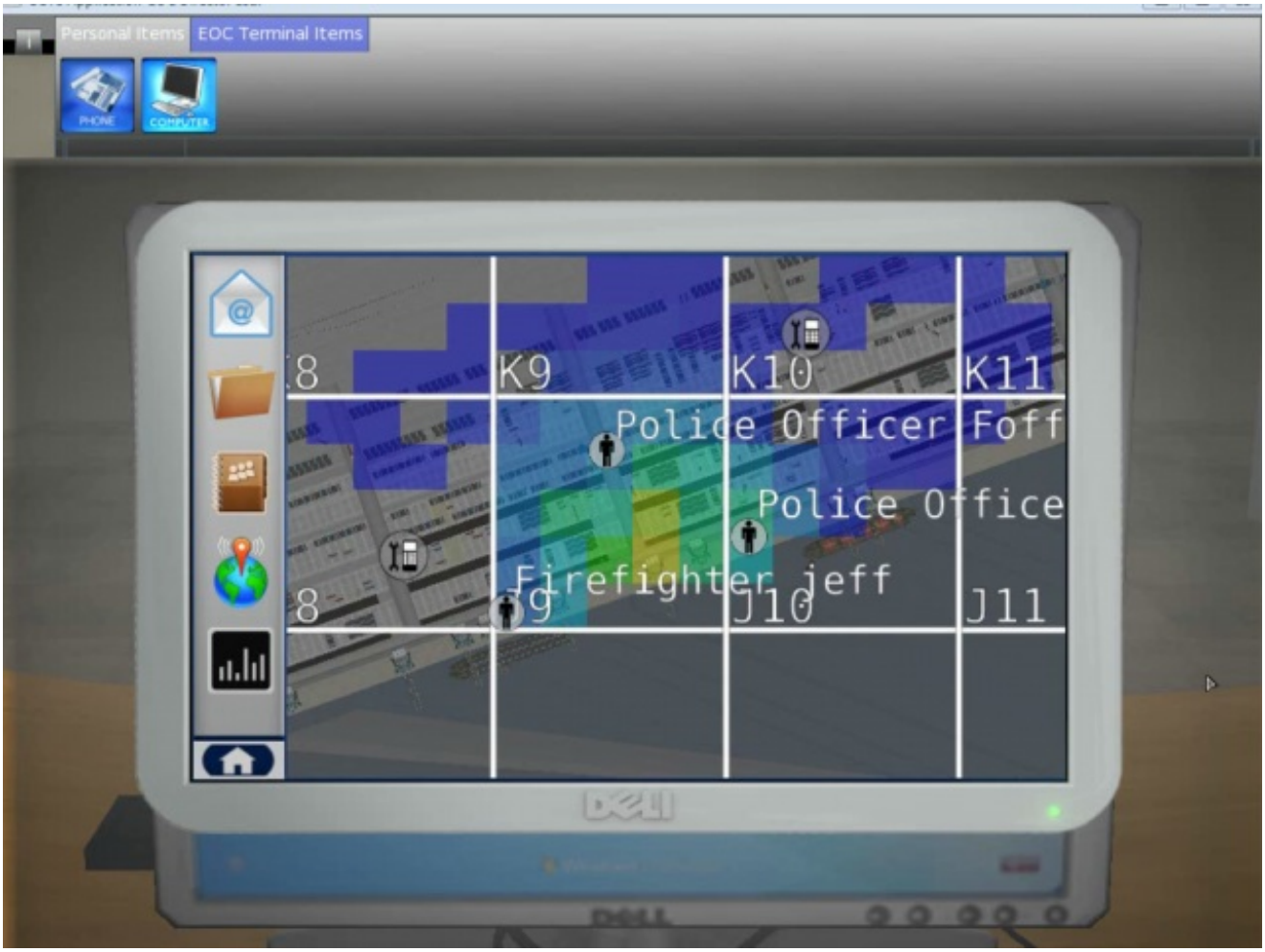
Unfortunately, one of the player’s mobile devices contains a virus! It’s up to the Network Administrator to detect the unusual network activity and isolate the problem before the whole network goes down.

New additions include:

- Configurable smart phones running various applications
- Location-based radio and cell phone jammers that disrupt communication
- Prototype of a Network Security display allows for event detection and blocking of traffic sources
- Simulated computer network systems for email and other packet-based protocols
- 2D Map display with configurable heat-map overlays


POLICE
LONG BEACH
POLICE




Personal Items
EOC Terminal Items
PHONE
COMPUTER
K9
K10
K11
Police Officer Foff
Police Office
Firefighter jeff
J10
J11


Personal Items
SMARTPHONE
RADIO
COMQUACK WIRELESS
SIGNAL DETECTOR
STRONG
WEAK
HEXCOMM
ELECTRONICS

In the event of a disaster, emergency teams need to stay connected to maximize efficiency and response time
The EOC Director receives data sent automatically from field workers to his computer in the Emergency Operations Center.
Using GPS, the EOC director can log the location of field workers in addition to receiving important data.
A field worker's smart phone is hacked, rendering mobile communication unavailable.
the network administrator must identify and manage potential security threats to the network.

*Period of Performance:*Jan 2010 to Nov 2012
*Tags:*Game-Based Training, Research, Simulation
*Focus Area:*Visual Simulation and Game-based Technology