Innovations & Technologies for Improving Throughput, Efficiency and Security

AAPA Marine Terminal Management Training Program

October 2014

Topics of Discussion

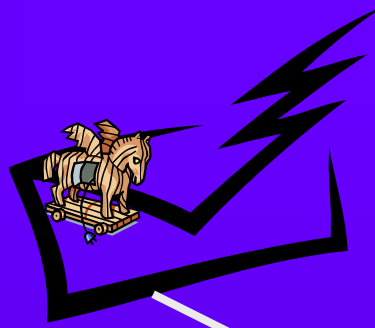
- Redundancy
- Cyber Security
- Digital Dashboards
- Video Management
- Access Control & TWIC
- Truck Green Lanes
- Waterside Surveillance
- Mass Notification
- PSIM

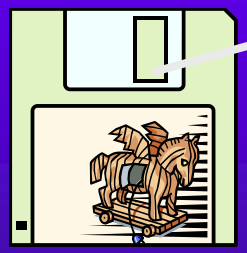
Redundancy

- Clustered Servers
- Offsite Backup Site
- Active /Active Offsite Real Time Data Replication
- Redundant Fiber Paths to ISP Demarcation

Cyber Security

Trojan Horse Attack





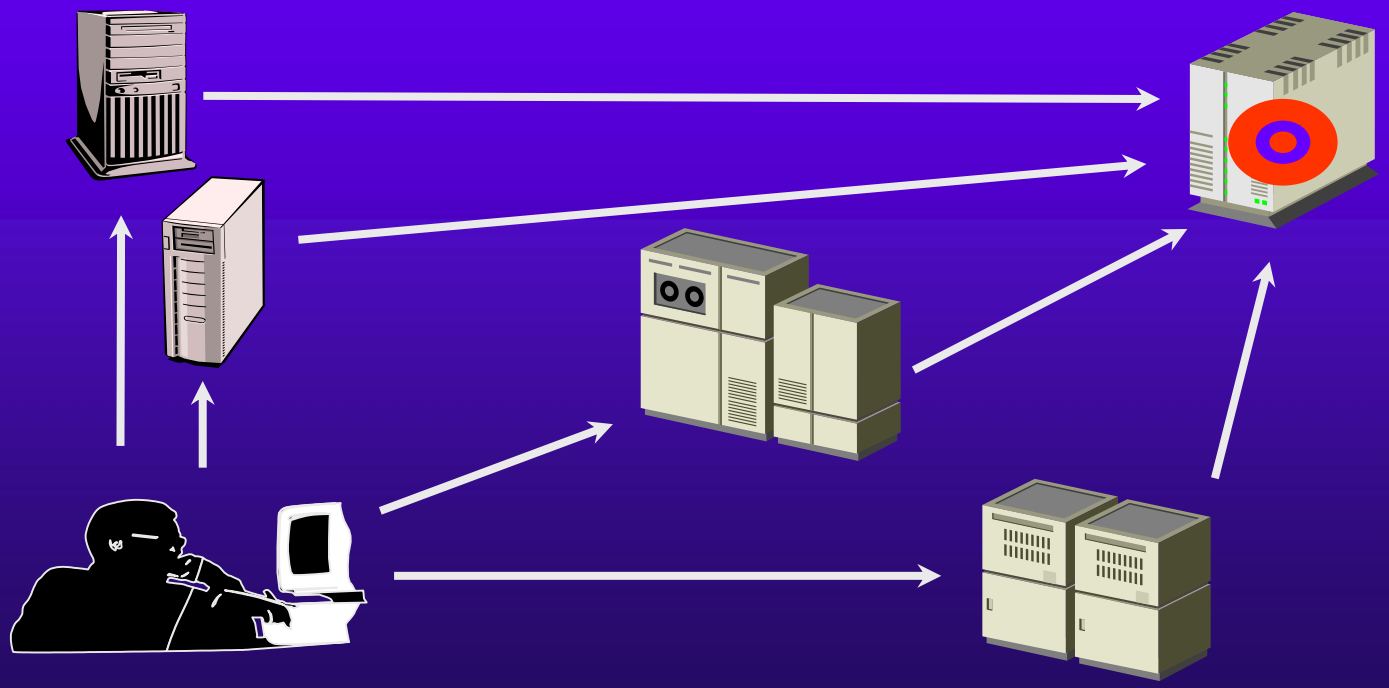
Trojan Horse is activated when the software or attachment is executed.

Trojan Horse arrives via email or software like free games.

Trojan Horse releases virus, monitors computer activity, installs backdoor, or transmits information to hacker.

Denial of Service Attacks

In a denial of service attack, a hacker compromises a system and uses that system to attack the target computer, flooding it with more requests for services than the target can handle. In a distributed denial of service attack, hundreds of computers (known as a zombies) are compromised, loaded with DOS attack software and then remotely activated by the hacker.

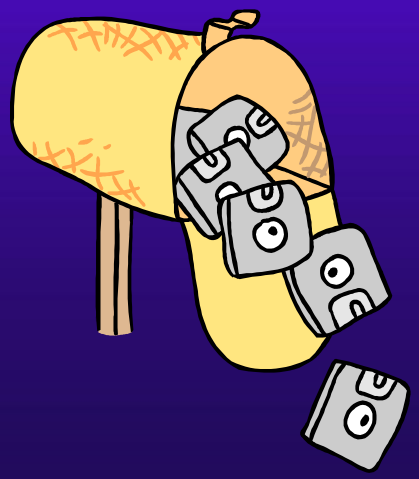


Spamming Attacks

Sending out e-mail messages in bulk. It's electronic "junk mail."

Spamming can leave the information system vulnerable to overload.

Less destructive, used extensively for e-marketing purposes.



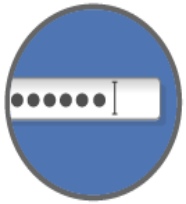
State of the Industry

As per Gartner Research, worldwide spending on security infrastructure, including software, services and network security appliances used to secure enterprise and consumer IT equipment reached approximately $60 Billion in 2012, and is expected to grow to $86 Billion by 2016.

According to IMS Research, the number of internet capable devices connected to the internet passed the 5 Billion Milestone in 2011 and is expected to reach 22 Billion by 2020.

Don’t Be Just Another Victim

Consumers become unwilling victims to data hackers and security breaches through no fault of their own, but while it's impossible to prevent a breach at a company of which you're a customer, there are certain things you can do to make your personal information safer.



Use strong and unique passwords for every site

Never store passwords in your browser

Use a password manager

Avoid accessing important accounts on open wi-fi networks

Verify that email links go to legitimate sites

Never store credit cards, addresses or personal data on websites

Change your passwords as soon as you hear of a security breach

Most security attacks
Occur From The Inside

Physical Access Control

In an open, trusting and tech savvy environment, the best access control system may be predicated upon a link to system access. IF YOU FAIL TO BADGE INTO THE BUILDING, YOU DON’T GET ACCESS TO THE SYSTEMS.

Combine Logical security with Physical Security

Biometrics Devices

The fingerprint and its unique identifying characteristics. Placed on a special reading pad, a designated finger's print is recognized by a computer.

Multi-factor authentication: something you are given (ID Badge) , something you have (your fingerprint)

Digital Dashboards In Terminal Operations Management

Operational vs. Analytical Dashboards

Operational

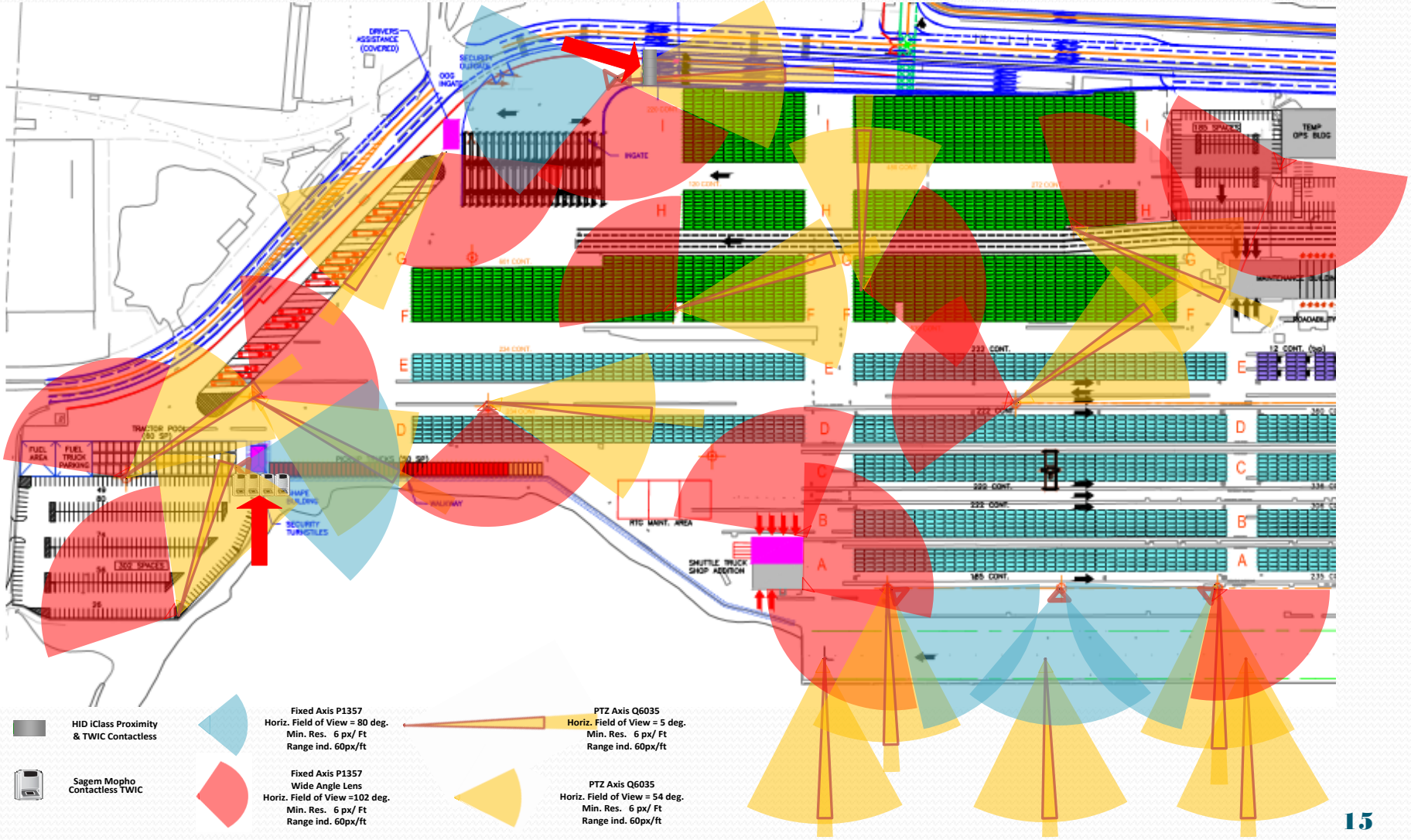
- View of current activities and frequently changing metrics
- Identifies potential operational issues as they occur
- Provides alerts on exception issues, and drill-through to facilitate real-time response
- Require less training than analytical dashboards

Analytical

- Gains insights from a volume of data collected over time
- Understand what happened, why, and what changes should be made in the future
- Sophisticated models, what-if analysis and pivots to identify patterns and opportunities
- Often used by analysts and highly trained staff

Operational, or KPI dashboards tell you what is happening today.
Analytical dashboards set targets for tomorrow.

Physical Security Technology Master Plan (Preliminary Design)



Video Management

- Pixels Per Foot
- Resolution Digital
- Degrees of Coverage
- Camera Selection
- Lens Selection
- Video Analytics

- Analog
- Digital (IP)
- Hybrid
- Network
- Recording
- Storage

Uses of Video at Ports

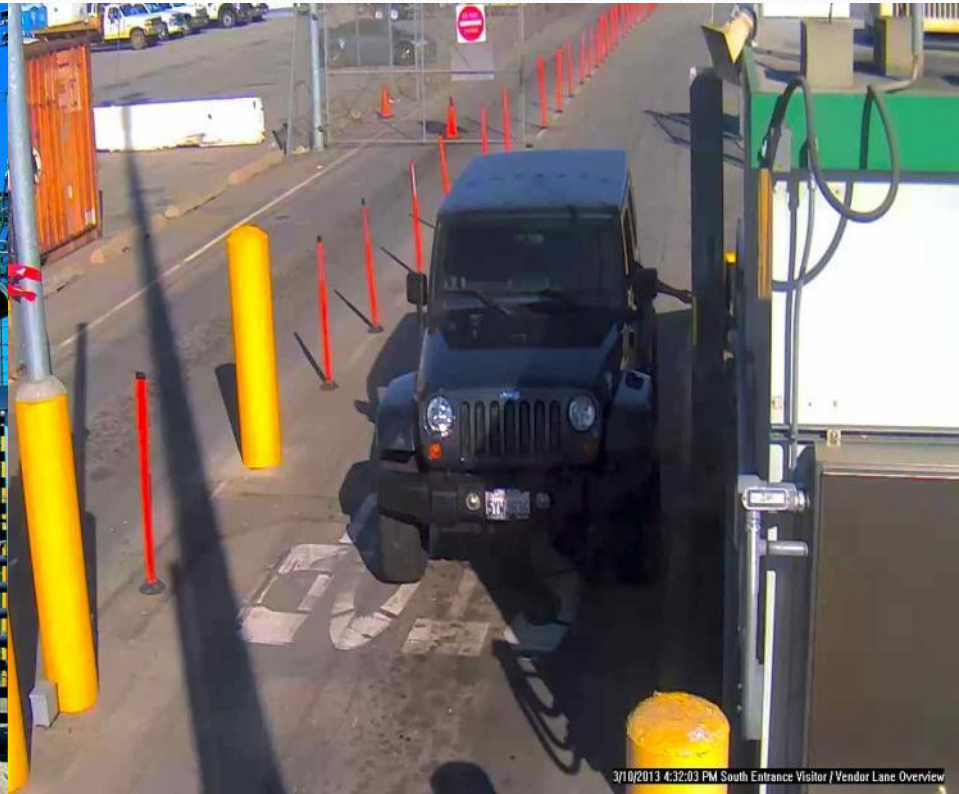
- Security
  - General Surveillance
  - Analytics
- Access Control
  - Piggybacking through access points
  - Invalid Access Card Reads
  - Intrusion Alarms
- Payroll Theft Deterrence
  - One person punching other person(s) time card
- Traffic (Seaports)
  - Cargo Gates Inbound queue surveillance
  - Cargo Gates Outbound queue surveillance
  - Cruise Arrival and Departure Traffic Flow
- Cargo Yards
  - General Surveillance
  - Fence Lines
- Parking Garages and Surface Lots
  - Pay-on-foot Stations
  - Throughout the multi-levels to protect automobiles from forced entry and to prevent violent crimes
  - Emergency Call Buttons
- Ground Transportation
  - Violator Identification
  - Violator tracking
  - OCR Backup (Vehicle license Plate Number)
  - Solicitation Surveillance
  - Taxi Revenue Control
- Cash Rooms
  - Counting of Cash from Parking Revenue,
  - Taxi Collection, Truck Gate Scale Charges,
  - Credentialing, Business Permits
- Customs & Border Protection
  - Passenger Interview Rooms
  - Passenger Holding Cells
- Landside and Waterside Surveillance
  - General Surveillance
  - Radar Target Tracking
- Cranes
  - Productivity of Union Labor
  - Documentation of Safety Violations and how Injuries occurred
- Marketing
  - Viewing cameras via the Web to provide “Live View” of Port Operations during business development trips throughout the world

Physical Access Control

- Access Denied
- Door Ajar
- Piggybacking
- Voice Notification
- Visual Notification
- Turnstiles
- Doors

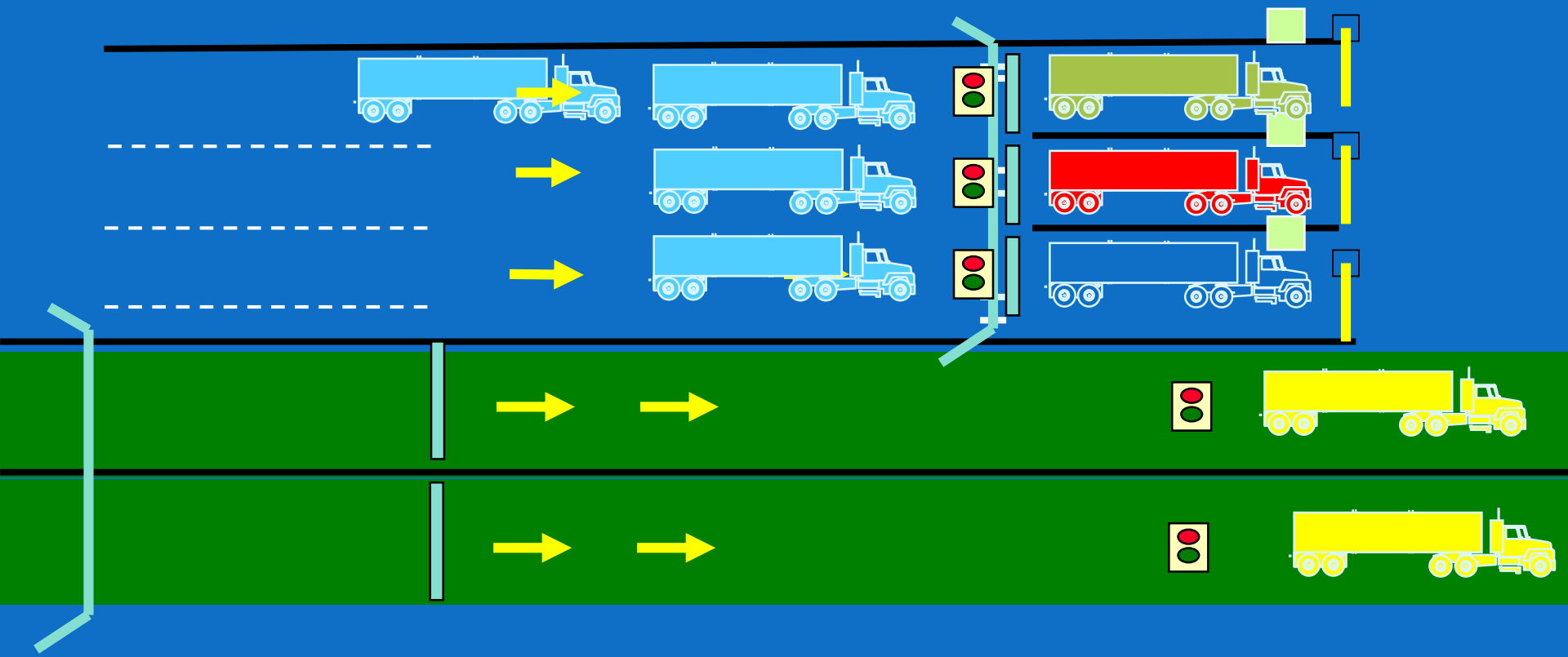
- Gates
- Ingress & Egress
- Proximity
- Mag Stripe
- Biometric
- TWIC

- Challenge for TWIC reader
  - Meet security requirements
  - Withstand harsh outdoor conditions
  - Balance the need to meet Government compliance and the needs of the port operators
  - Maintain rapid access to facility



TWIC Card Implentations

Green Lanes for Cargo Entrance Gates



Cargo Gate Green Lanes

The Green Lane Concept is based on Pre-Gate Portals fully integrated to the Cargo Terminal Operating System(s) and any Port Authority Legacy Security, Operational and/or Business Systems capable of processing and providing all the necessary information to all parties in a secured and safe environment resulting in dramatically reducing truck turn-around time, maximization of usable acreage for the benefit of the Cargo Terminals and reducing Terminal Operator Labor Costs. **Trusted Truck** (RFID Tag installed on the truck), **Trusted Driver** (TWIC Reader/Camera/Wireless Transmitter in an enclosure install inside the Cab) and a **Trusted Trip** (Pre-Arrival information entered via the Web or from other sources – NOT AN APPOINTMENT).

The goal is to allow a driver/trucking company to "**qualify"** for entry via the Green Lane (without stopping at a Security or TIR Gate) and drive directly to the Truck Pad where the driver is delivering or picking up a container. A "WIN" for the Terminal, as greater efficiencies are attained, a "WIN" for the Trucker/Trucking Company, as wait times at Gates are eliminated resulting is greater profitability, and a "WIN" for the Environmentalists as trucks are not idling at Security/TIR gates thus reducing carbon emissions. The Green Lane Concept makes use of cutting-edge Cargo Terminal technology to expedite its operational and security functions

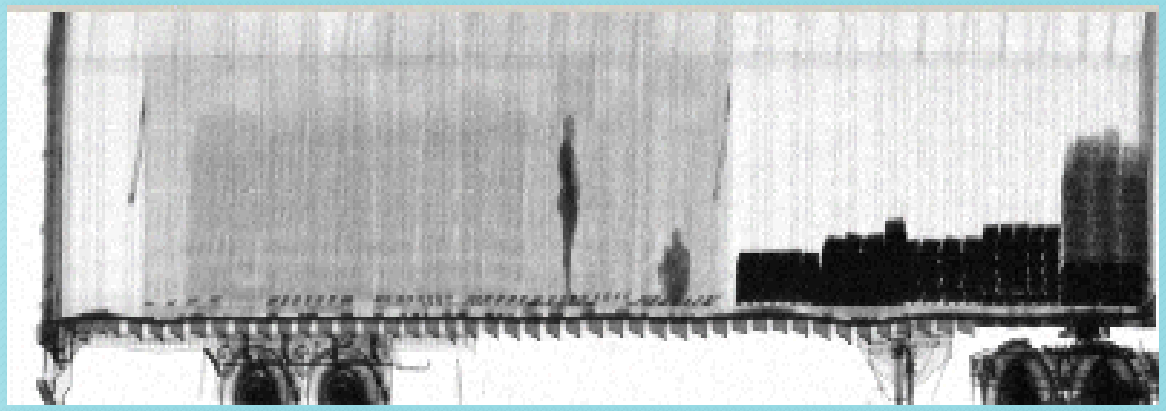
New Technology

High Definition Cameras pass road-ability images to terminal operators for review.

Radio Frequency ID TAG to positively identify the truck

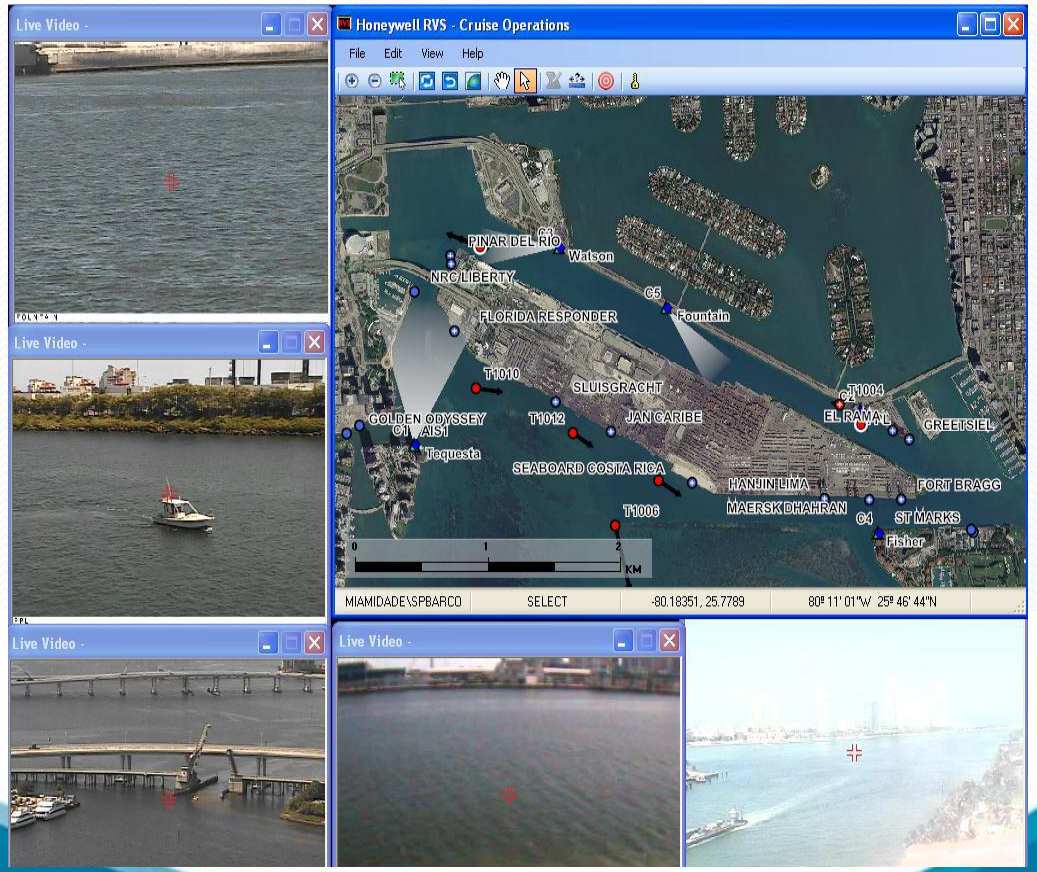
In-Cab Card Reader to verify drivers identify and Screen to communicate with the driver

Gamma ray technology can be introduced to check if container is empty or full



Waterside Radar/AIS Surveillance

- Radar detects moving or stationary targets.
- AIS use radar sensors to detect intruders in user defined alarm zones.
- Video is recorded and distributed over a Local Area Network to provide recorded history and real-time situational awareness.
- When an alarm is triggered, personnel can identify the threat and make security decisions before the threat reaches the perimeter.

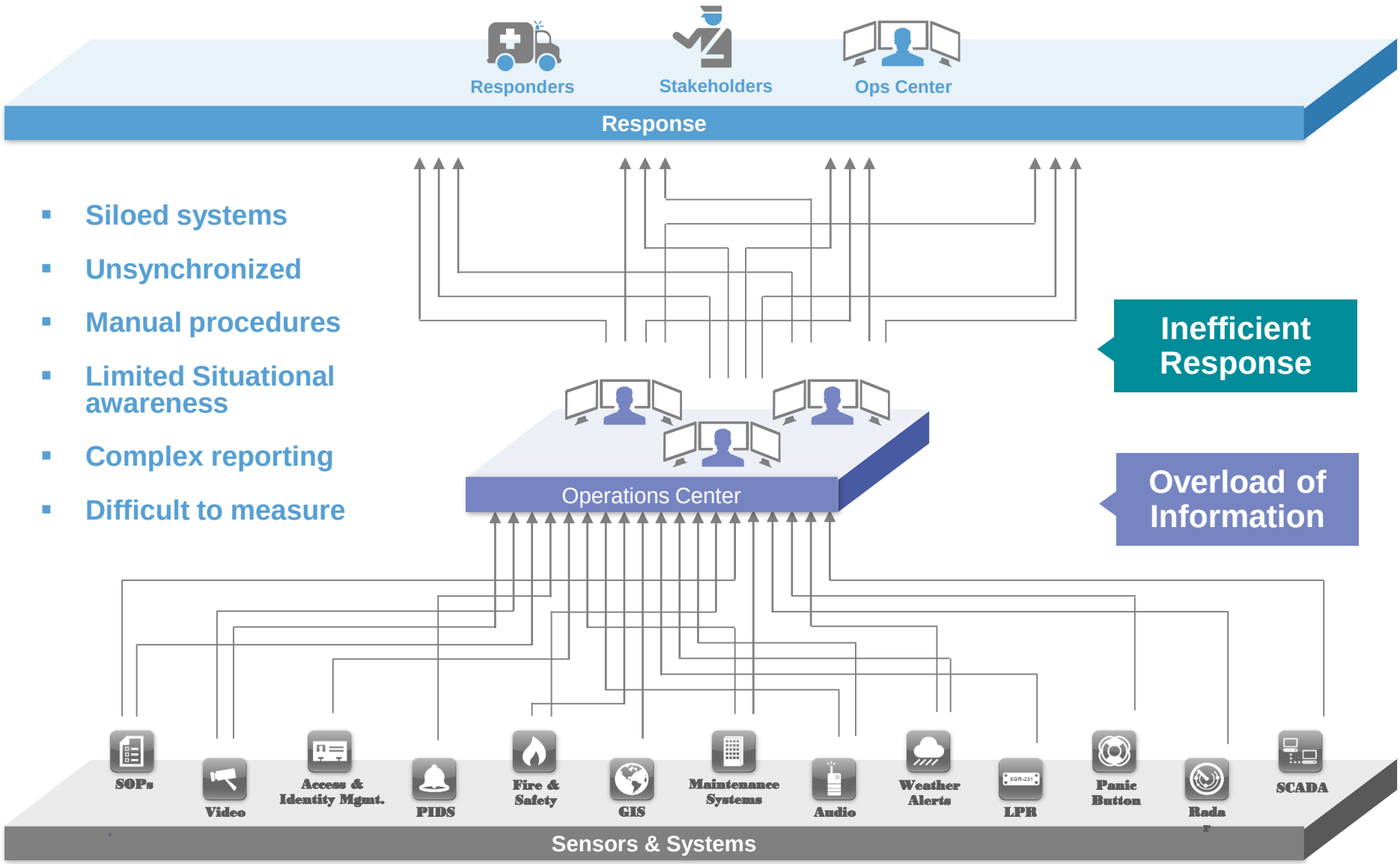


Mass Notification

The integrated use of networks, mobile devices and modern cloud technology, combined with the ability to integrate with legacy communication devices results in a uniquely complete and robust solution for the safety and security market

What Do I do?

Command and Control Centers
The Situation Today



- Siloed systems
- Unsynchronized
- Manual procedures
- Limited Situational awareness
- Complex reporting
- Difficult to measure

Inefficient Response

Overload of Information

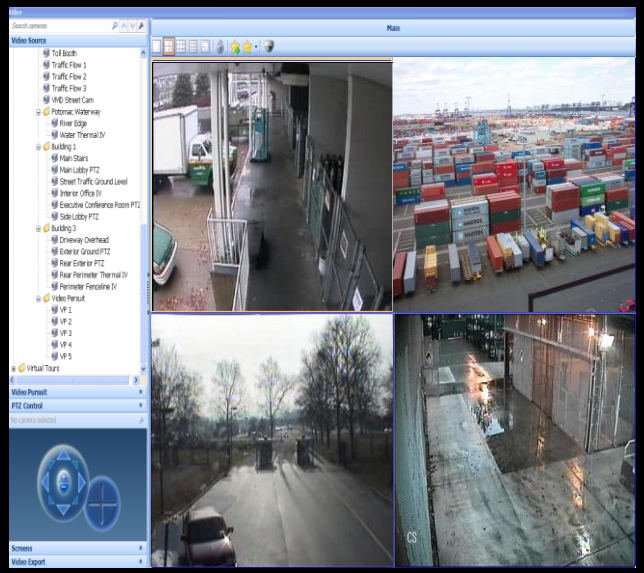
Physical Security Information Management (PSIM)

WHAT:
Physical security information management (PSIM) is a category of software that provides a platform and applications created by middleware developers, designed to integrate multiple unconnected security applications and devices and control them through one comprehensive user interface.

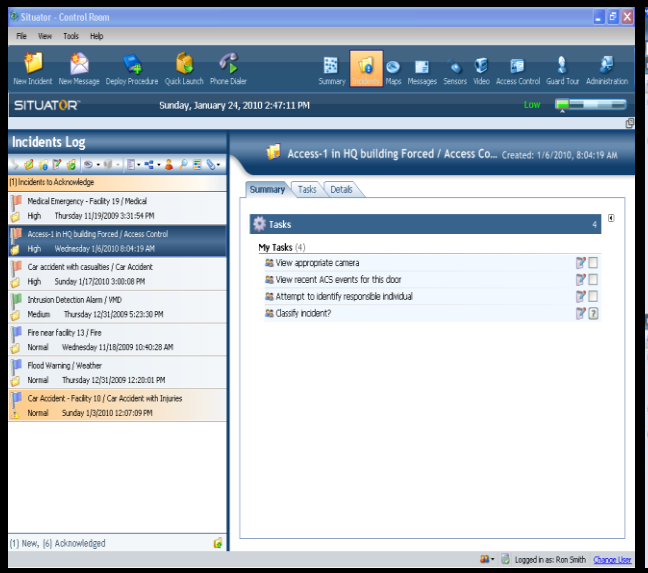
HOW:
It collects and correlates events from existing disparate security devices and information systems (video, access control, sensors, analytics, networks, building systems, etc.) to empower personnel to identify and proactively resolve situations.

WHY:
PSIM integration enables numerous organizational benefits, including increased control, improved situation awareness and management reporting. Ultimately, these solutions allow organizations to reduce costs through improved efficiency and security through increased intelligence.

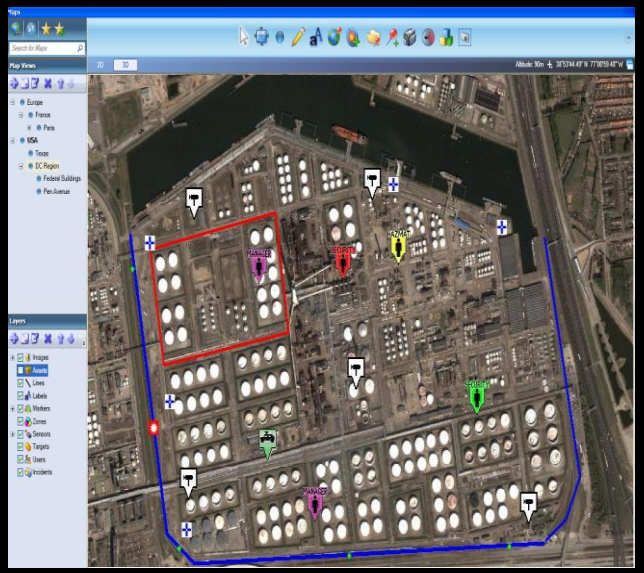
Video Management



Adaptive Response



GIS Visualization



Scenario

Louis A. Noriega

Transportation and Critical Infrastructure

Operations and Physical Security

Technology Consultant

Louis.Noriega@aportsolutions.com

(305) 491-3908

www.aportsolutions.com