

Norcontrol IT

Day 2, Session 1
Port Communications and Security

Security initiatives affecting the port environment

Steve Guest
General Manager
Norcontrol IT Ltd

InfoPort 2003

Norcontrol IT

Port Communications and Security

Contents

Norcontrol IT Ltd

Maritime "Surveillance" and "Security"

International Ship & Port Facility Security Code

Security Roadmap

InfoPort 2003

Norcontrol IT

Main Business Areas

Kongsberg Maritime



Kongsberg Defence & Aerospace



Key figures 2002:

- Turnover £551 million
- Total number of employees 4,000
- Backlog of orders £500 million

InfoPort 2003

Norcontrol IT

Kongsberg Maritime a leading provider of marine and offshore technology

Concentrating on these applications:
Building leading market positions within:

- Dynamic positioning
Kongsberg Simrad 
- Marine automation
- Navigation
- Hydro acoustics
- Simulation
- Surveillance & Security
- Information processing

Offshore & Subsea
Kongsberg Simrad

Merchant Marine
Kongsberg Maritime Ship Systems (KMSS)

Yachting & Fishery
Simrad

Maritime Information Technology
Kongsberg Marine IT

InfoPort 2003

Norcontrol IT

Maritime Surveillance and Security

- **Situation Awareness**
 - Recognised Surface Picture/Common Operating Picture for all users
 - Multi Sensor fusion package
- **Prevention**
 - Accurate, **timely** and user friendly data flow enabling high risk situations to be identified








InfoPort 2003

Norcontrol IT

Norcontrol IT Worldwide Deliveries



InfoPort 2003



Norcontrol IT Experience

Norcontrol IT is recognised as the world's leading supplier of maritime surveillance and security solutions:

- 30 years of experience
- 140 systems delivered worldwide
- 50+ systems that consist of 3 or more sensor sites
- Largest system consisting of more than 70 Sensor Sites!

Customers using Norcontrol IT maritime surveillance solutions include:

- Canadian Coastguard: East coast of Canada
- Los Angeles and Long Beach: Port anchorages, channel & harbours
- Port of Singapore: Port approaches and Singapore Strait
- Norwegian Coastal Directorate: Oslo Fjord
- Dubai Ports Authority: Arabian Gulf, Port approaches & harbour
- Spanish Coastal Directorate: Strait of Gibraltar
- Taiwanese Coastguard: Territorial Waters & EEZ
- UK's Maritime & Coastguard Agency: Dover Strait

InfoPort 2003



Security initiatives affecting the port environment

Contents

Norcontrol IT Ltd

Maritime "Surveillance" and "Security"

International Ship & Port Facility Security Code

Security Roadmap

InfoPort 2003



"Surveillance"

What is "Surveillance"?

- The ongoing, systematic collection, analysis and interpretation of data that is essential to planning, implementation and evaluation. Closely integrated with the timely dissemination of data to those who need to know.
- The final link in the **surveillance** chain is the application of these data to **prevent and control**

Reference: Internet Medical Site

InfoPort 2003



"Surveillance"

Prevent & Control:



InfoPort 2003



"Surveillance"

Prevent & Control:

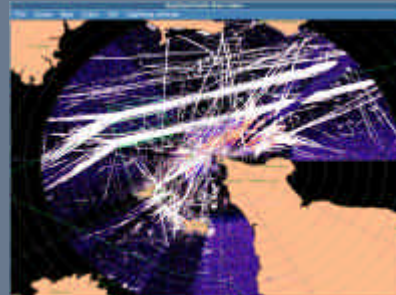


InfoPort 2003



"Surveillance"

The Challenge:



InfoPort 2003

Norcontrol IT

"Security"

NOF CONTROL IT

What is "Security"?

- The condition of being protected from or not exposed to danger.
 - Freedom from doubt.
- Freedom from care, anxiety or apprehension.

Reference: Oxford English Dictionary

infoPort 2003

Norcontrol IT

"Security"

NOF CONTROL IT

What is "Security"?

Freedom from care, anxiety or apprehension from:

- Illegal Immigration?
- Smuggling?
- Piracy?
- Terrorism?

Reference: International Ship & Port Facility Security (ISPS) Code

infoPort 2003

Norcontrol IT

Port Security

NOF CONTROL IT

Little Port Security in Boston, Massachusetts, December 1763 (The Boston Tea Party)



infoPort 2003

Norcontrol IT

Port Security

NOF CONTROL IT

USS Cole attacked in Aden, October 2000:



infoPort 2003

Norcontrol IT

Port Security

NOF CONTROL IT

17 crew members killed and severe damage to the ship



infoPort 2003

Norcontrol IT

"Security"

NOF CONTROL IT

Smuggler, Legitimate trader or



infoPort 2003

Smuggling - Harbour Acceptance Trials?



Security initiatives affecting the port environment



Contents

Norcontrol IT Ltd

Maritime "Surveillance" and "Security"

International Ship & Port Facility Security Code

Security Roadmap

InfoPort 2003

ISPS Code Security Level Definitions



Security Level 1 - Normal

The level at which ships and port facilities will normally operate.

Security Level 2 - Heightened

The level applying as long as there is a heightened risk of a security incident.

Security Level 3 - Exceptional

The level applying for the period of time when there is the probable or imminent risk of a security incident.

InfoPort 2003

SOLAS Definition of a "Port Facility":



Port facility is a location, as determined by the Contracting Government or by the Designated Authority, where the ship/port interface takes place.

This includes areas such as **anchorage**, **waiting berths** and **approaches** from seaward, as appropriate.

InfoPort 2003

Mandatory Requirements of the ISPS Code:



Security Level 1 - Normal

- Ensuring the performance of all port facility security duties;

InfoPort 2003

Mandatory Requirements of the ISPS Code:



Security Level 2 - Normal

- Ensuring the performance of all port facility security duties;
- Controlling access to the port facility;

InfoPort 2003



Mandatory Requirements of the ISPS Code:

Security Level 1 - Normal

- Ensuring the performance of all port facility security duties;
 - Controlling access to the port facility;
- Monitoring of the port facility, including anchoring and berthing areas;



Mandatory Requirements of the ISPS Code:

Security Level 1 - Normal

- Ensuring the performance of all port facility security duties;
 - Controlling access to the port facility;
- Monitoring of the port facility, including anchoring and berthing areas;
- Monitoring restricted areas to ensure that only authorised personnel have access;



Mandatory Requirements of the ISPS Code:

Security Level 2 - Enhanced

- Ensuring the performance of all port facility security duties;
 - Controlling access to the port facility;
- Monitoring of the port facility, including anchoring and berthing areas;
- Monitoring restricted areas to ensure that only authorised personnel have access;
- Ensuring that security communication is readily available.



Mandatory Requirements of the ISPS Code:

At Security Levels 2 and 3 further, **additional**, specific measures will be implemented in accordance with the guidelines given in Part B of the Code.



Recommended Requirements of the ISPS Code:

Security Level 1 - Normal

- Providing guards and patrols;



Recommended Requirements of the ISPS Code:

Security Level 2 - Enhanced

- Providing guards and patrols;
- Providing automatic intrusion detection devices, or surveillance equipment or systems to detect unauthorised access into, or movement within restricted areas;



Recommended Requirements of the ISPS Code:

Security Level 1 - Normal

- Providing guards and patrols;
- Providing automatic intrusion detection devices, or surveillance equipment or systems to detect unauthorised access into, or movement within restricted areas;
- Control of the movement of vessels in the vicinity of ships using the port facility



Recommended Requirements of the ISPS Code:

Security Level 2 - Heightened

- Use of continuously monitored and recorded surveillance equipment;



Recommended Requirements of the ISPS Code:

Security Level 2 - Heightened

- Use of continuously monitored and recorded surveillance equipment;
- Enhancing the number and frequency of waterside patrols undertaken on the boundaries of the restricted areas and within those areas;



Recommended Requirements of the ISPS Code:

Security Level 2 - Heightened

- Use of continuously monitored and recorded surveillance equipment;
- Enhancing the number and frequency of waterside patrols undertaken on the boundaries of the restricted areas and within those areas;
- Establishing and restricting access to areas adjacent to the restricted areas;



Recommended Requirements of the ISPS Code:

Security Level 2 - Heightened

- Use of continuously monitored and recorded surveillance equipment;
- Enhancing the number and frequency of waterside patrols undertaken on the boundaries of the restricted areas and within those areas;
- Establishing and restricting access to areas adjacent to the restricted areas;
- Enforcing restrictions on access by unauthorised craft to the waters adjacent to ships using the port facility.



Recommended Requirements of the ISPS Code:

Security Level 3 - Exceptional

- Setting up of additional restricted areas within the port facility in proximity to the security incident, or the believed location of the security threat, to which access is denied;



Recommended Requirements of the ISPS Code:

Security Level 3 - Exceptional

- Setting up of additional restricted areas within the port facility in proximity to the security incident, or the believed location of the security threat, to which access is denied,
- Preparing for the searching of restricted areas as part of a search of all, or part, of the port facility.



Security initiatives affecting the port environment

Contents

Norcontrol IT Ltd

Maritime "Surveillance" and "Security"

International Ship & Port Facility Security Code

Security Roadmap



Security Road Map

Steps towards provision of "security":

- Awareness
- Prevention
- Response



Security Road Map

Steps towards provision of "security":

- Awareness:
 - Identify vulnerability to potential threats



Security Road Map

Steps towards provision of "security":

- Awareness:
 - Identify vulnerability to potential threats
 - Enlist all potential stakeholders



Security Road Map

Steps towards provision of "security":

- Awareness:
 - Identify vulnerability to potential threats
 - Enlist all potential stakeholders
 - Produce a "Port Facility Security Plan" that considers existing systems, new systems, sensors & technologies



Security Road Map

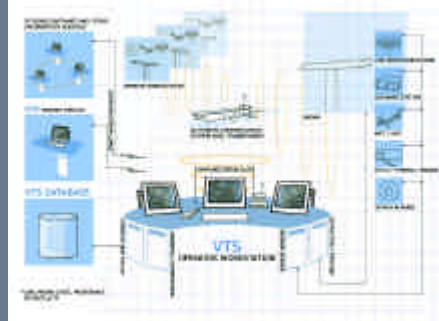
Steps towards provision of "security":

- **Awareness:**
 - Identify vulnerability to potential threats
 - Enlist all potential stakeholders
 - Produce a "Port Facility Security Plan" that considers existing systems, new systems, sensors & technologies
 - Possible sensors include radar, CCTV, Direction Finders, satellite imagery, vessel tracking systems, AIS, sonar, Remotely Operated Vehicles, etc



Port Security & VTS System

Vessel Traffic Service (VTS) System

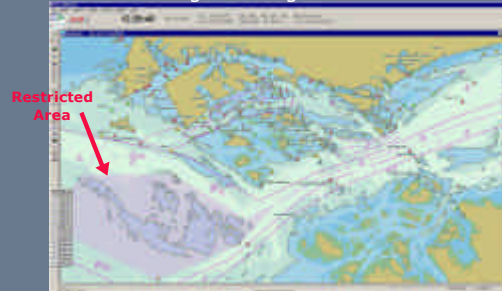


VTS Operator Workstation



Port Security & VTS System

Traffic Image showing Restricted Areas



Security Road Map

Steps towards provision of "security":

- **Awareness:**
 - Identify vulnerability to potential threats
 - Enlist all potential stakeholders
 - Produce a "Port Facility Security Plan" that considers existing and new systems, sensors & technologies
 - Possible sensors include radar, CCTV, Direction Finders, satellite imagery, vessel tracking systems, AIS, sonar, Remotely Operated Vehicles, etc
- **Prevention:**
 - Implement a **credible** security focussed infrastructure



Security Road Map

Steps towards provision of "security":

- **Awareness:**
 - Identify vulnerability to potential threats
 - Enlist all potential stakeholders
 - Produce a "Port Facility Security Plan" that considers existing and new systems, sensors & technologies
 - Possible sensors include radar, CCTV, Direction Finders, satellite imagery, vessel tracking systems, AIS, sonar, Remotely Operated Vehicles, etc
- **Prevention:**
 - Implement a **credible** security focussed infrastructure
 - Provide Standard Operating Procedures within the Port Facility Security Plan for each of the various threats identified

Security Road Map



Steps towards provision of "security":

- **Awareness:**
 - Identify vulnerability to potential threats
 - Enlist all potential stakeholders
 - Produce a "Port Facility Security Plan" that considers existing and new systems, sensors & technologies
 - Possible sensors include radar, CCTV, Direction Finders, satellite imagery, vessel tracking systems, AIS, sonar, Remotely Operated Vehicles, etc
- **Prevention:**
 - Implement a **credible** security focussed infrastructure
 - Provide Standard Operating Procedures within the Port Facility Security Plan for each of the various threats identified
 - Proactive SOPs

Security Road Map



Steps towards provision of "security":

- **Awareness:**
 - Identify vulnerability to potential threats
 - Enlist all potential stakeholders
 - Produce a "Port Facility Security Plan" that considers existing and new systems, sensors & technologies
 - Possible sensors include radar, CCTV, Direction Finders, satellite imagery, vessel tracking systems, AIS, sonar, Remotely Operated Vehicles, etc
- **Prevention:**
 - Implement a **credible** security focussed infrastructure
 - Provide Standard Operating Procedures within the Port Facility Security Plan for each of the various threats identified
 - Proactive SOPs
 - Data Management System that automatically **captures data** sorts and classifies/highlights potential high-risks through programmed logic/intelligence

MCA Data Management System



Security Road Map



Steps towards provision of "security":

- **Awareness:**
 - Identify vulnerability to potential threats
 - Enlist all potential stakeholders
 - Produce a "Port Facility Security Plan" that considers existing and new systems, sensors & technologies
 - Possible sensors include radar, CCTV, Direction Finders, satellite imagery, vessel tracking systems, AIS, sonar, Remotely Operated Vehicles, etc
- **Prevention:**
 - Implement a **credible** security focussed infrastructure
 - Provide Standard Operating Procedures within the Port Facility Security Plan for each of the various threats identified
 - Proactive SOPs
 - Data Management System that automatically **captures data** sorts and classifies/highlights potential high-risks through programmed logic/intelligence
 - Data dissemination to appropriate Stakeholders

Data Dissemination



- **Technical Solutions:**
 - Microwave Links, Telephone, Satcom, etc
 - Military Data Link Systems such as Link Y, 11, 16
 - Intranet/Internet
 - XML, ebXML, etc, etc, Blah, Blah
 - **But**
- **Who are the Stakeholders?**
 - Port Authority?
 - Terminal Operator?
 - National Competent Authority?
 - Ministry of Defence?
 - Emergency Services: Police, Ambulance, Fire, Etc
 - National Intelligence Organisation?

Port Data Management System



Norcontrol IT

Security Road Map

Steps towards provision of "security":

- **Awareness:**
 - Identify vulnerability to potential threats
 - Enlist all potential stakeholders
 - Produce a "Port Facility Security Plan" that considers existing and new systems, sensors & technologies
 - Possible sensors include radar, CCTV, Direction Finders, satellite imagery, vessel tracking systems, AIS, sonar, Remotely Operated Vehicles, etc
- **Prevention:**
 - Implement a **credible** security focussed infrastructure
 - Provide Standard Operating Procedures within the Port Facility Security Plan for each of the various threats identified
 - Proactive SOPs
 - Data Management Systems that automatically **captures data**, sorts and highlights potential high-risks through programmed logic/intelligence
 - Data dissemination to appropriate Stakeholders
- **Response:**
 - Flexible Command & Control Infrastructure

infoPort 2003

Norcontrol IT

Security Road Map

Steps towards provision of "security":

- **Awareness:**
 - Identify vulnerability to potential threats
 - Enlist all potential stakeholders
 - Produce a "Port Facility Security Plan" that considers existing and new systems, sensors & technologies
 - Possible sensors include radar, CCTV, Direction Finders, satellite imagery, vessel tracking systems, AIS, sonar, Remotely Operated Vehicles, etc
- **Prevention:**
 - Implement a **credible** security focussed infrastructure
 - Provide Standard Operating Procedures within the Port Facility Security Plan for each of the various threats identified
 - Proactive SOPs
 - Data Management Systems that automatically **captures data**, sorts and highlights potential high-risks through programmed logic/intelligence
 - Data dissemination to appropriate Stakeholders
- **Response:**
 - Flexible Command & Control Infrastructure
 - Co-ordination of assets using the Recognised Maritime Picture/Common Operating Picture and Data Management System

infoPort 2003

Norcontrol IT

Security Road Map

Steps towards provision of "security":

- **Awareness:**
 - Identify vulnerability to potential threats
 - Enlist all potential stakeholders
 - Produce a "Port Facility Security Plan" that considers existing and new systems, sensors & technologies
 - Possible sensors include radar, CCTV, Direction Finders, satellite imagery, vessel tracking systems, AIS, sonar, Remotely Operated Vehicles, etc
- **Prevention:**
 - Implement a **credible** security focussed infrastructure
 - Provide Standard Operating Procedures within the Port Facility Security Plan for each of the various threats identified
 - Proactive SOPs
 - Data Management Systems that automatically **captures data**, sorts and highlights potential high-risks through programmed logic/intelligence
 - Data dissemination to appropriate Stakeholders
- **Response:**
 - Flexible Command & Control Infrastructure
 - Co-ordination of assets using the Recognised Maritime Picture/Common Operating Picture and Data Management System
 - Resources (?)

infoPort 2003

Norcontrol IT

Resources

infoPort 2003

Norcontrol IT

Summary

- **Norcontrol IT:** 30 years of experience & 130 systems delivered worldwide
 - "Security": means many things to many ports/people/cultures
- **Port Facility Security Plan:** enlist all Stakeholders during compilation
- **Maritime Surveillance & Security System:** build upon existing systems, multi-layered & multi-sensory
- **Data Management System:** data capture, multi-sourced, inherent logic, data dissemination tool
- **Credible Security Plans must have resources available to Respond.**

Thank You & Good Watch

infoPort 2003