Security for the Transport Sector

An Integrated IT and Physical Security System Approach

www.uti.eu.com

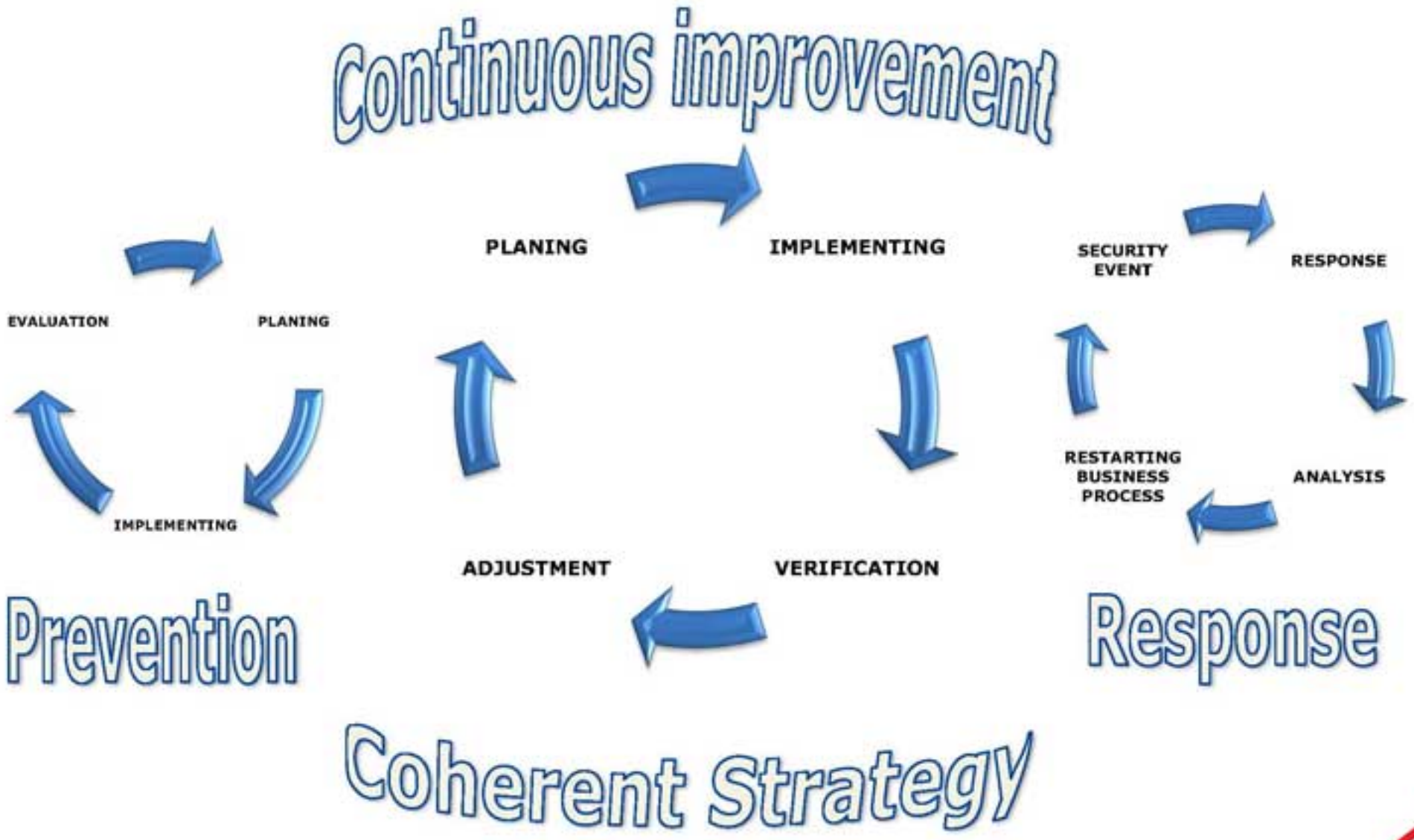
UTI Approach on Security

Systems Solutions

Wide Area Integration

References

Program development



CI Security Solution development

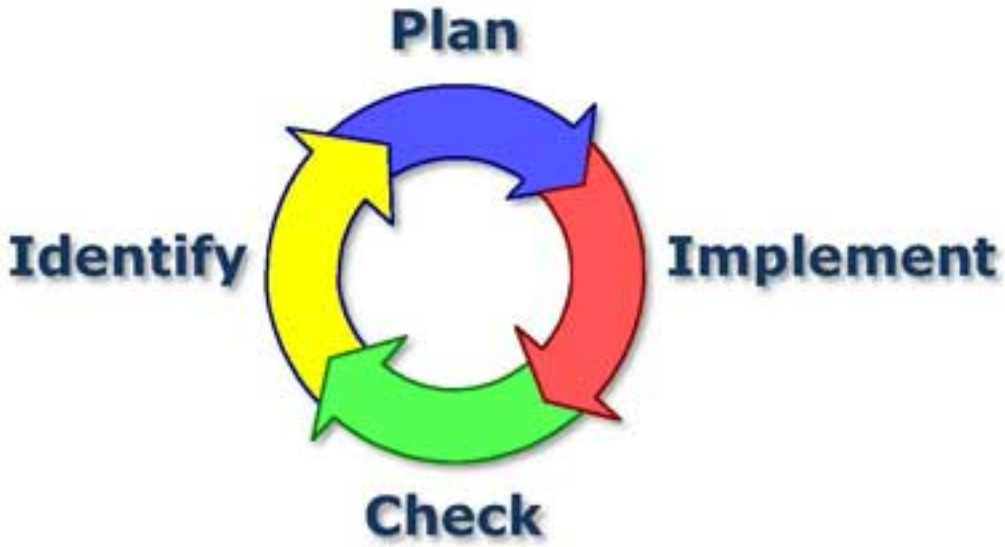
Methods and technologies

- Risk analysis, threat assessment
- Security audits and system design
- System integration: CCTV, access control, intrusion detection, perimeter security, multi level communication networks, physical security barriers, real time and near real time integration software and hardware
- Integrated monitoring centers
- Disaster recovery and business continuity
- Human factor assessment, recruitment and training

Introduction

Steps in security measures design and implementation

- Security risk analysis
- Security measures design and validation
- Security measures implementation
- Operation and periodic re-evaluation



Security Risk Analysis

- It is required to begin with for any security measures design
- It is required by regulations
- The analysis takes into account multiple threats and vulnerabilities identified during the assessment
- Threats' probability of occurrence and potential consequences depend on the vulnerabilities

Most Common Threats and Vulnerabilities

Potential threats

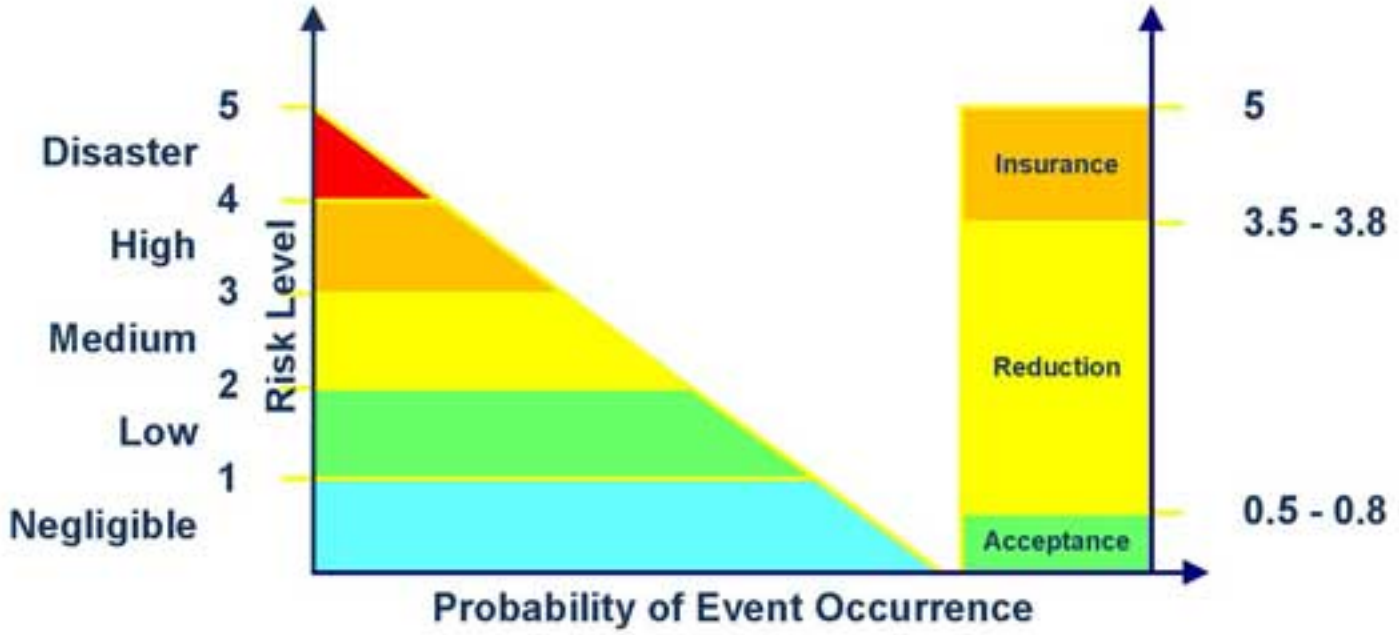
- Biological Contamination
- Theft of Assets
- Bomb Threats
- Chemical Spills
- Data Destruction / Disclosure
- Errors
- Fire
- Flooding/Water Damage
- Sabotage/Terrorism
- Vandalism/Rioting

Potential vulnerabilities

- Insufficient physical protection
- Lack of intrusion detection
- Superficial entry control/ personnel screening
- Lack of package control
- Improper plans for emergencies and incidence response
- Lack of security procedures/ policies/training
- Process installations vulnerabilities

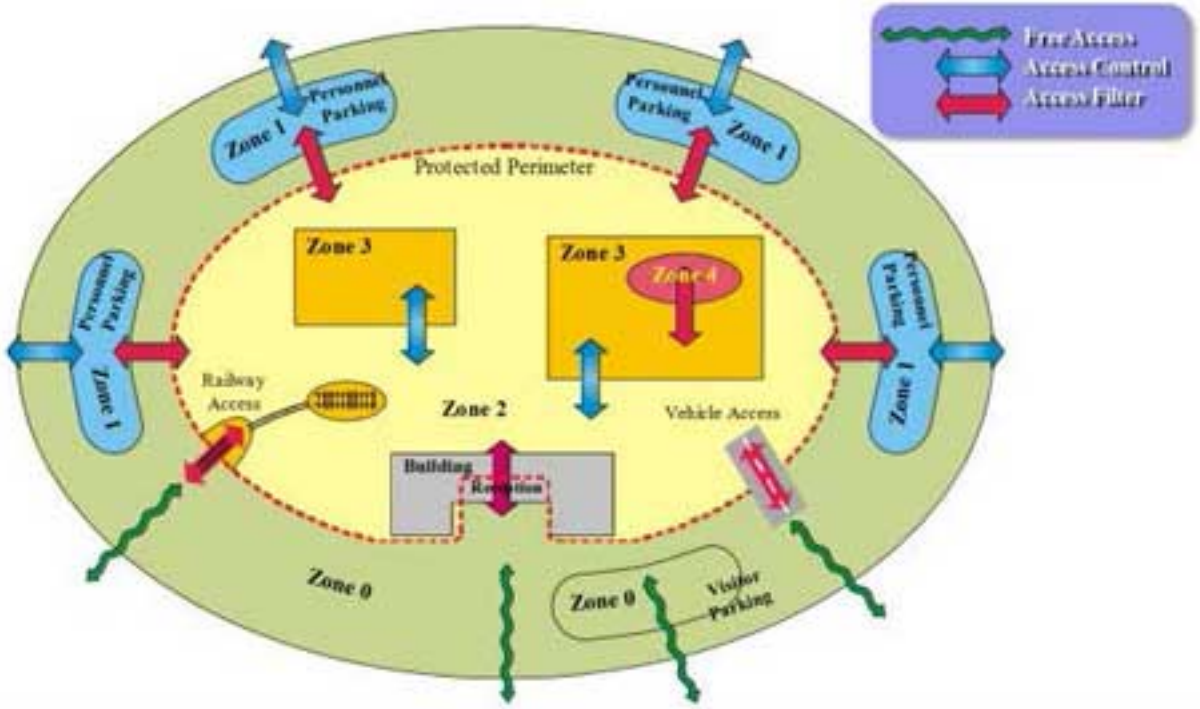
Attitude Towards Risk

- The risk analysis helps in prioritizing security measures
- Different risks may require different measures
- Investment should be targeted on the areas which provide the maximum return on investment (the maximum risk reduction)



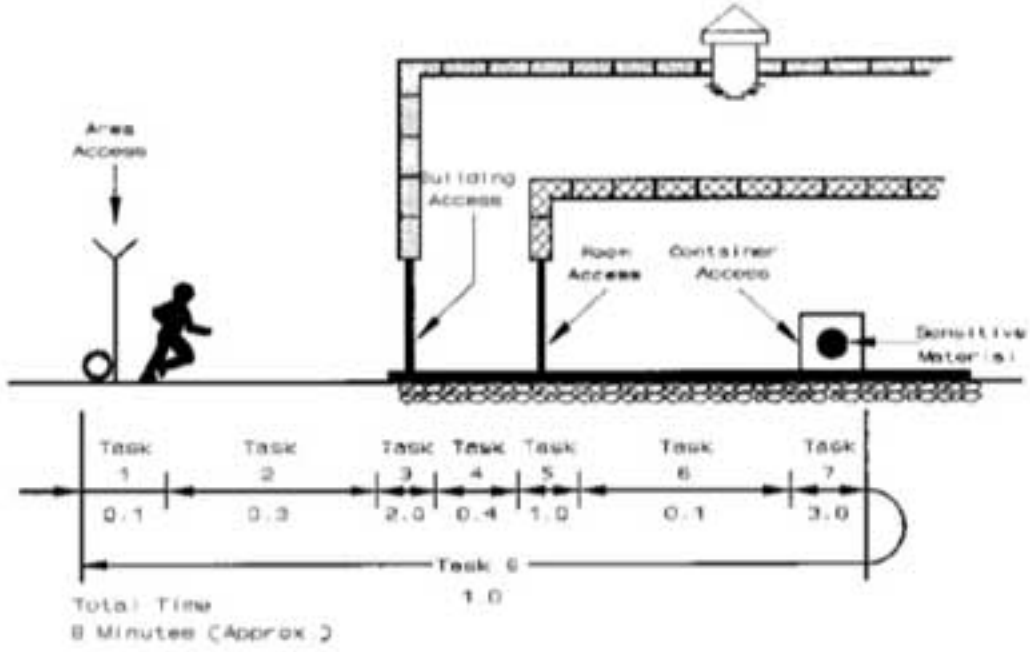
Principle of Defence in Depth

- In order to maximize the probability of detection and adversary action interruption, multiple layers of protection are designed and implemented.
- The Defence in Depth approach maximizes uncertainty for the intruders, provides appropriate protection for high sensitivity areas and optimizes the investment in security measures.



Principle of Timely Response

- Security is effective if an adverse action can be prevented or interrupted before completion.
- In order to be successful in denying an adverse action, the security response action should finalize before the adverse action finalizes.
- Careful design and simulation is required to ensure that the system guarantees the desired performance level.



Principle of Balanced Protection

- A security system is as strong as its weakest (easiest to defeat) point.
- An analysis is made to make sure the protection effort is uniformly distributed.
- Overprotection of an area in the detriment of the others means wasted money.

UTI Approach on Security
Systems Solutions
Wide Area Integration
References

Access Control – Personnel & Vehicles

- Control and monitor people and vehicles movement in and between security areas (layered approach)
- Permanent credentials for staff
- Contractors/Visitors badges
- Vehicle License Plate Recognition

Access Control - Materiel

- Screening of baggage, parcels and shipments
- Detect unlawful substances and items
  - Weapons
  - Explosives
  - Narcotics

Intrusion Detection

- Low false alarm technologies (taut-wire, dual technology sensors)
- Indoor detection in equipment rooms
- Integration with CCTV for alarm assessment

Physical Barriers

- Delay systems correlated to
  - Detection capabilities
  - Reaction force performance
- Deterrent effect

Surveillance

CCTV cameras

- For general surveillance
- For detection (VMD, video-analytics)
- For assessment – triggered by other subsystems

Intelligent video processing

- Detection of terrorist threats
- Detection of unlawful behaviour
- ANPR – Automatic Number Plate Recognition

Fire Protection

Early detection

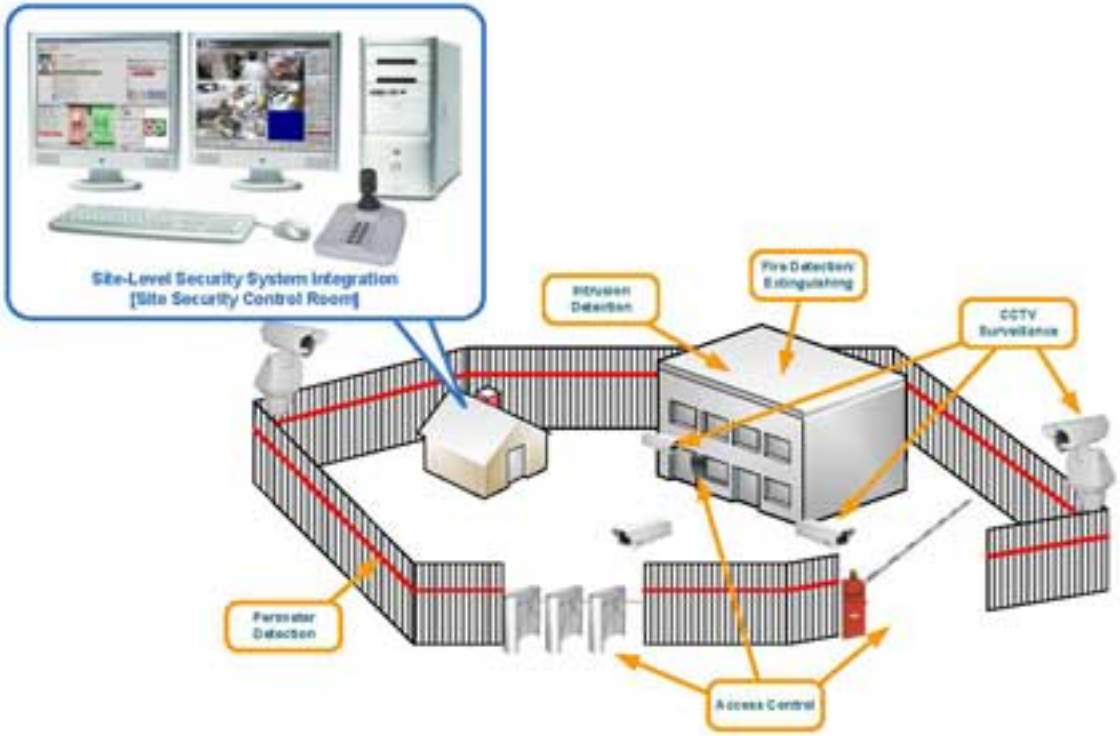
- Flame, smoke, heat detection
- Fast detection with absorption systems

Extinguishing

- Non-lethal extinguishing agents
- Business process continuity

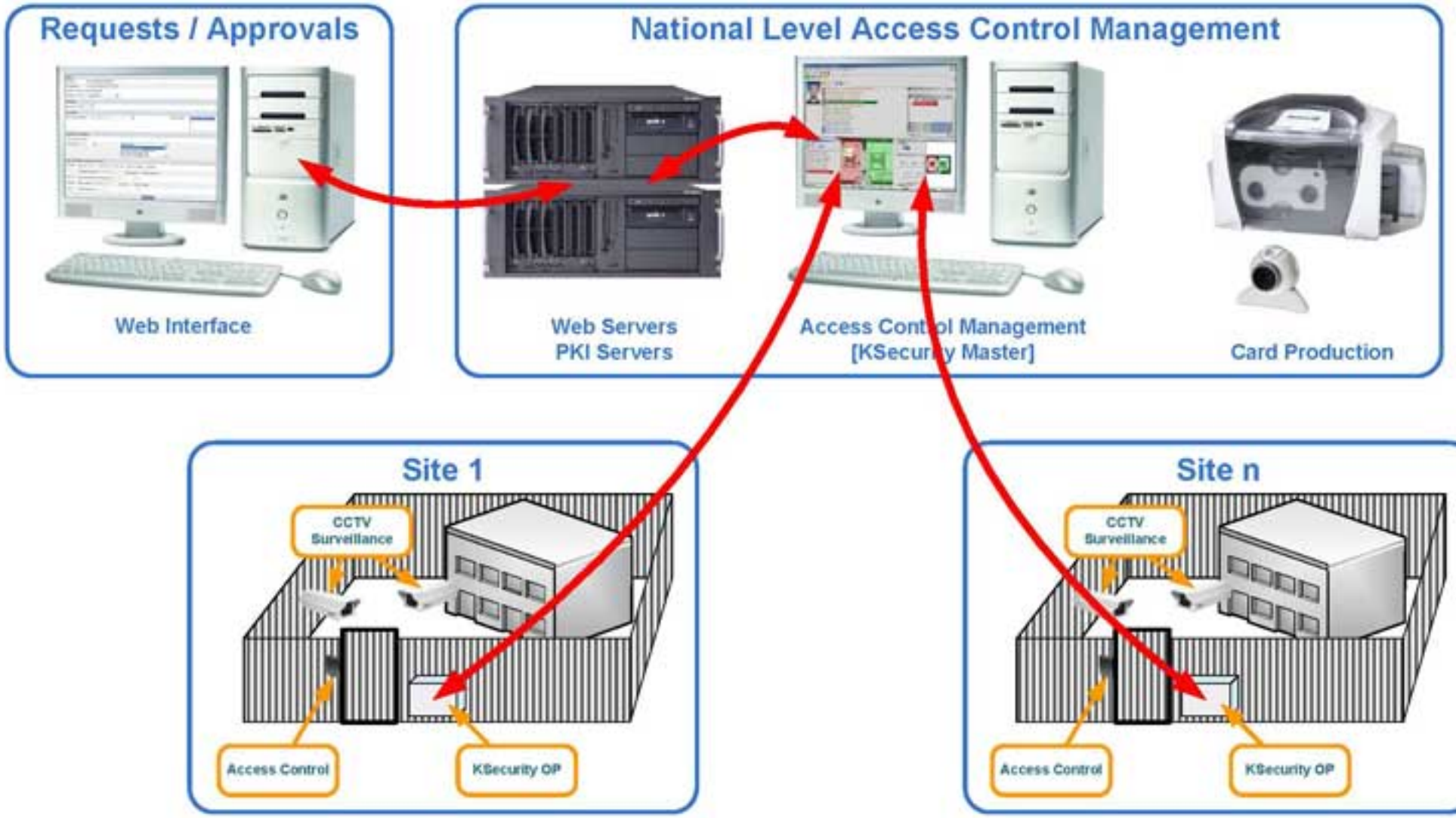
Local Control Room

- Site-Level Security System Integration
- Consistent look & feel of the interface across systems
- Decision support
- Traceability

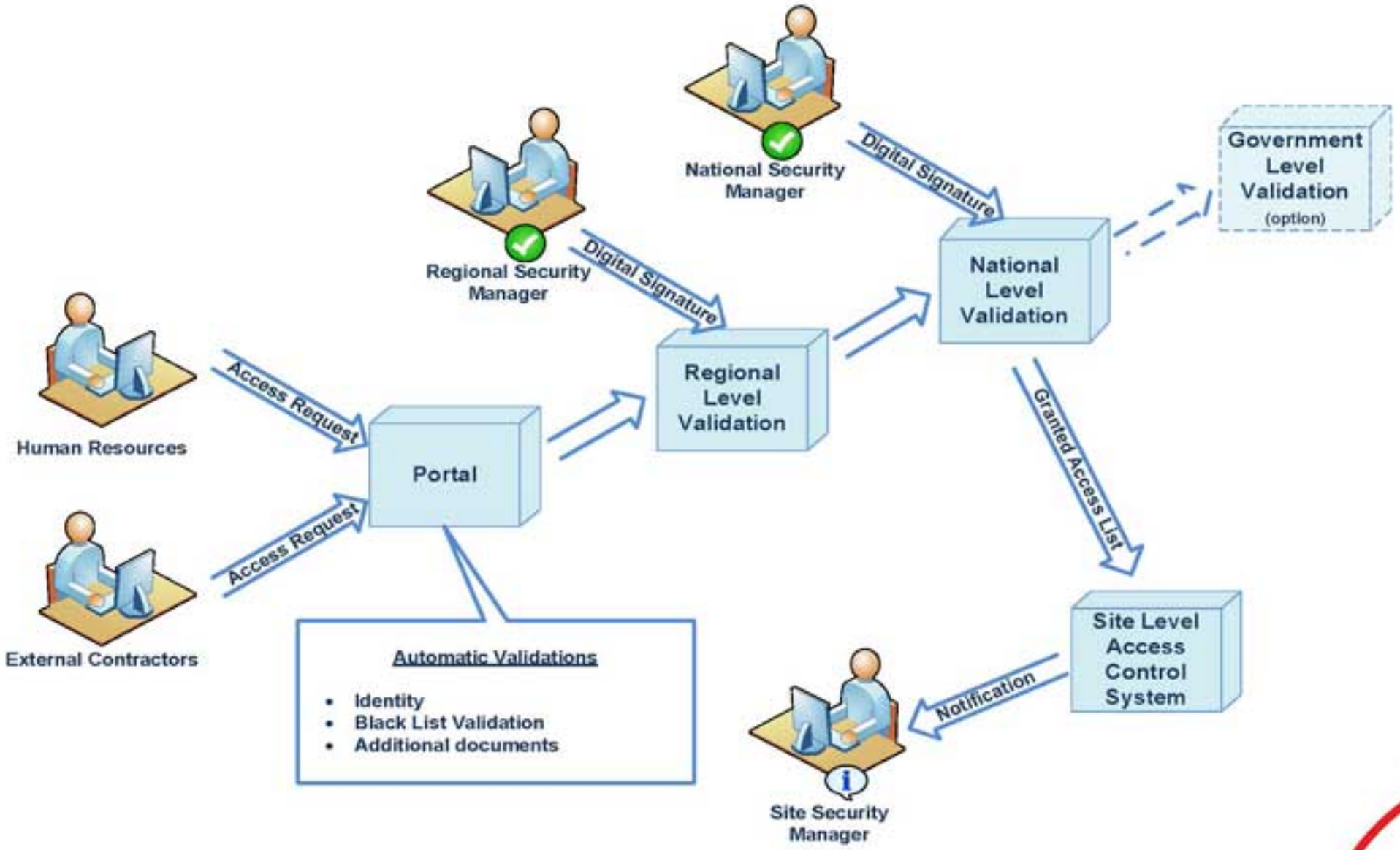


UTI Approach on Security Systems Solutions
Wide Area Integration
References

Access Rights Management System



Unified Access Rights Management



IT & Physical Security Integration

- Unified **Identity Management** system
  - Enrolment
  - Physical security permission management
  - Logical security permission management
  - Classified information clearance management
  - Training and certification information management
- **Unified Identity Credential** for physical and logical access
- Augmented logical access control – condition the logical access with the physical access
- Secure access to physical security systems based on PKI

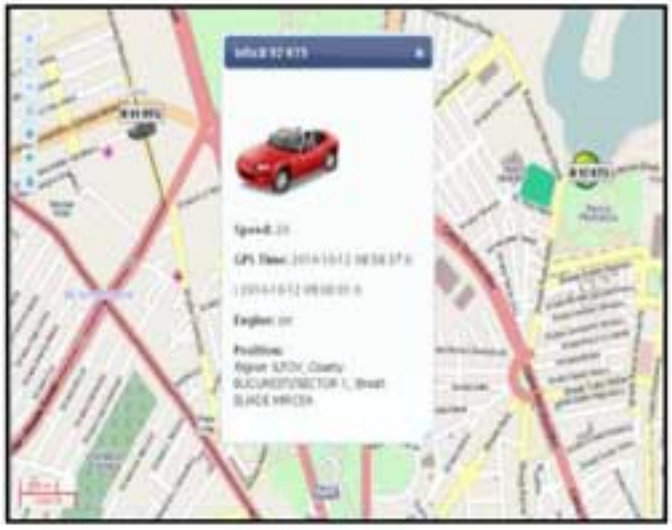
Security Resources Management

Security Agents Monitoring

- GPS positioning
- Direct voice dialling
- Remote-initiated listen-in
- Duress alarm
- Non-motion alarm
- Geo-fencing alarm

Security Teams Monitoring

- GPS positioning
- Mission status information
- Mission parameters monitoring
- Mission assignment assistance



Greater Mobility

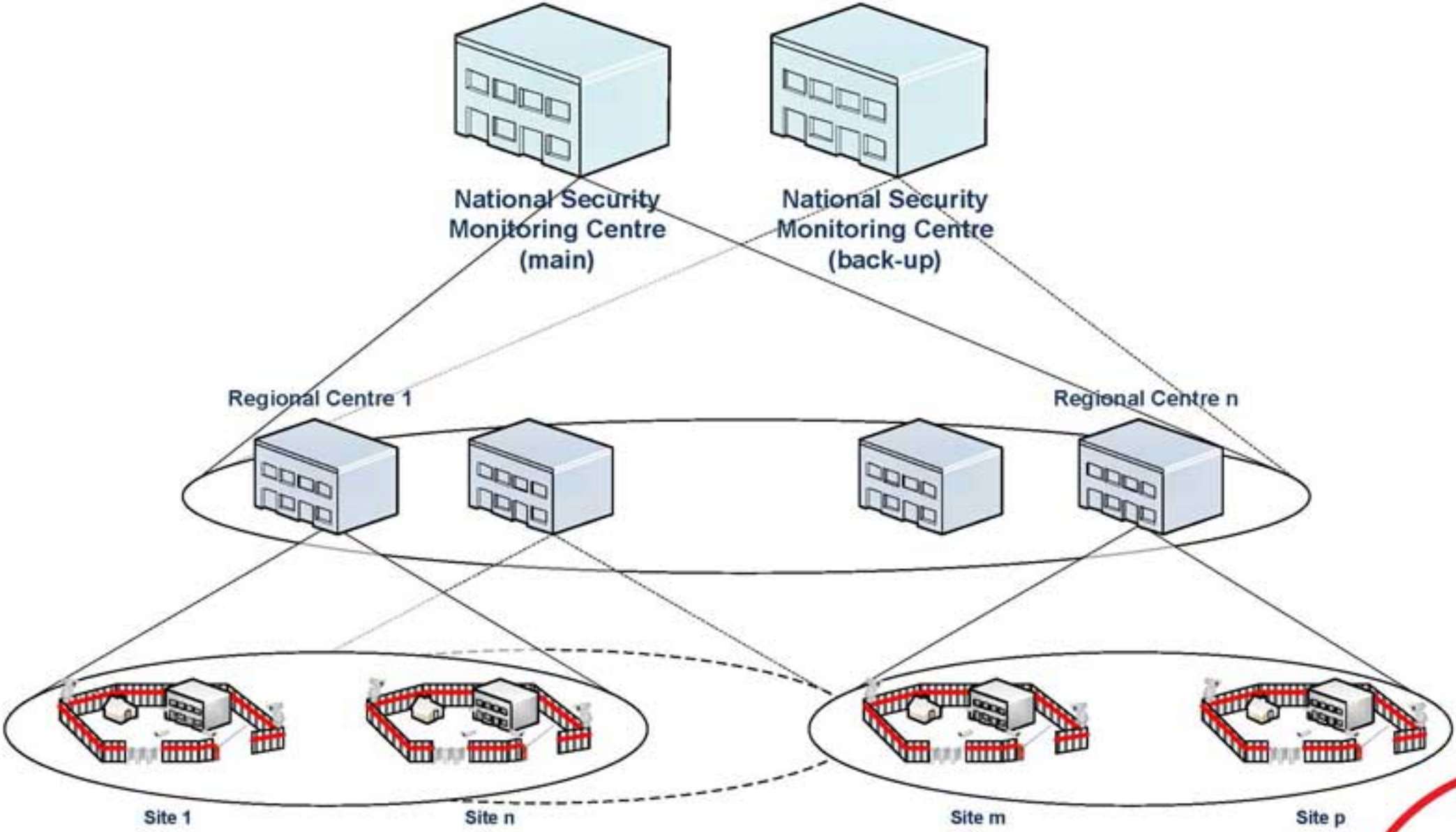
UAV for Forward Surveillance

- Pre-programmed flight
- Gyro-stabilized payload
- Choice of visible, thermal or multi-spectral camera
- Mobile control centre

Deployable Security Systems

- Temporary site protection
- Compensation for part unavailability of fixed systems
- Protection in case of emergency situations

National Level Integration



National Level Integration

- Increase **situation awareness** – create common operational picture and integrate it with other CIP players
- Share real-time information
  - Terrorist alerts
  - Other hazards
- **Realistic threat level assessment** based on wide-area fused information
- Monitor the **security response performance** and compensate for unavailability
- Optimal **resource allocation** in case of emergency situations
- **Centralized reporting and analysis**

Reassessment of Threats

- Analysis of availability of the physical security systems in case of extreme weather
- Analysis of vulnerability to "unconventional" terrorist threats (propelled grenades, car bombs)
- Analysis of insider threat as part of the security threat (stand-alone or in collaboration with outsider threat)

UTI Approach on Security Solutions
Wide Area Integration
References

CAPABILITY FOCUS : PORT AND MARITIME SECURITY SOLUTIONS

Perform Security Assessments

Elaborate Security Plans

Design / implement / operate / maintain Security Systems

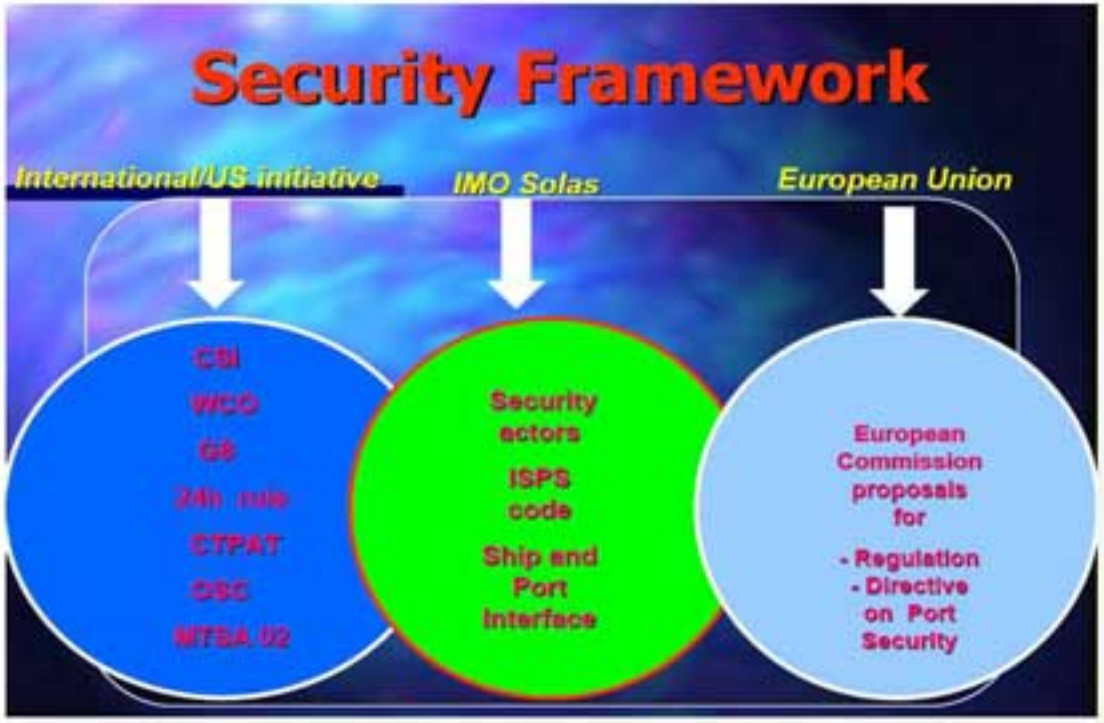
Perform Security Evaluations

FOR

Sea Ports

Inland Water Ports

Port Facilities



UTI is authorized as RSO according to the requirements of the ISPS Code

CAPABILITY FOCUS: INTEGRATED SECURITY FOR SEAPORTS

Perimeter Protection

- Physical barriers
- Electronic detection
- Closed Circuit Television (CCTV)

Person Access Control

- Interface with the Port Operators systems
- Metal detection
- Detection of CBRNE

Vehicle Access Control and Screening

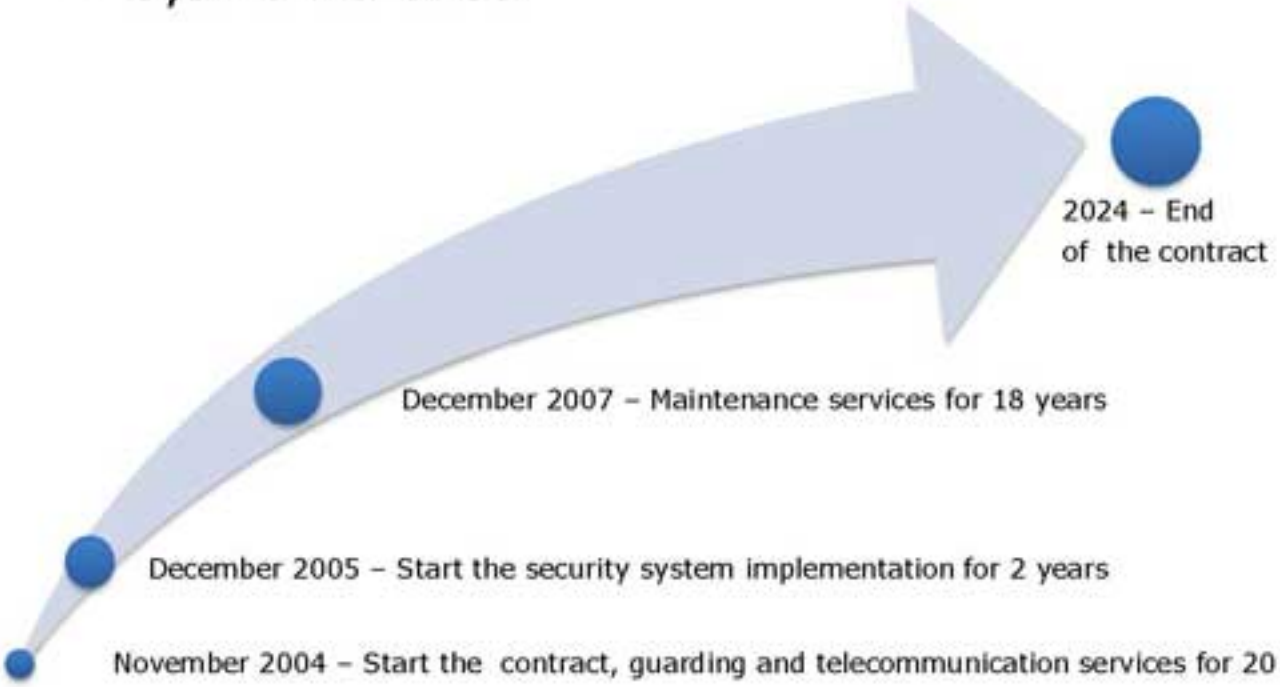
- Automatic Number Plate Recognition
- Interface with the Port Operators systems
- X-Ray Screening
- Detection of CBRNE

Ship, boat and diver detection

- Radar
- FLIR, Long-range Laser Camera

CASE STUDY:
CONSTANTA PORT SECURITY AND IT&C PROJECT

- 19 gates
- 12 km perimeter
- 29,83 km berth length
- 100 million tones/year capacity
- 3,926 ha area



CAPABILITY FOCUS: INTEGRATED SECURITY FOR AIRPORTS

- Construction and terminal installation
- Facility management
- Integrated physical and IT security
- Airfield lighting
- Parking and fleet management systems
- Baggage handling systems
- Integrated Airport Management Systems using our proprietary solution ICAR

CASE STUDY: BUCHAREST INTERNATIONAL AIRPORT SECURITY AND IT&C PROJECT

- 16,000 square meters
- 14 jet bridges
- 24 boarding gates
- Separate departures and/or arrivals flows for Schengen/non Schengen passengers
- Lounge and shopping areas

1996 – Phase 1 of the development and modernization plan : terminal security solutions, low voltage and telecommunication systems

1999 – Icar – ERP proprietary solution

2003 – Domestic Flight terminal: electrical and mechanical installations, baggage handling and passanger control systems

2011 – Phase 3: Schengen terminal construction – electrical and mechanical installations

CAPABILITY FOCUS: INTEGRATED SECURITY FOR SUBWAY

Integrated Security System

- Command and Control Center
- CCTV and Access Control
- Electronic Ticketing solution
- Fire Detection and Alarm System
- Public Address System
- Dynamic Information Display systems
- Radio Communications
- FO networking

Low voltage equipment

- General electrical power and distribution panels
- Warning systems and the energy supply safety systems

Medium voltage equipment

- Medium voltage cells

AC Equipment

- Software application;
- Fiber optic cables
- AC cells equipped with surveillance and protection

UPS System

- Emergency power supply system

CASE STUDY: BUCHAREST SUBWAY

- Metro tracks (main): 4
- Network lenght : 69.25 km double rail
- Depot: 4
- Stations No. : 51
- Average distance between two stations: 1.5 km

- Station's lenght : 135 – 175 m
- Station average depth: 12 m
- Gauge : 1432 mm
- AFC with magnetic card from 1995, upgraded on 2000. From 2006, together with RATB a functional platform was made to allow common ticketing.