

Robust Security Systems

IEEE EMC Society, Sweden Chapter



Bo Granbom

bo.granbom@saabgroup.com

Carl-Gustav Renmarker

carl-gustav.renmarker@saabgroup.com

Linköping, October 2, 2007



Content

- Background
- Introduction to a surveillance system topology
- Robustness and security aspects
- Capabilities and sub-system considerations
- Summary and Conclusions

QUESTIONS and DISCUSSION!

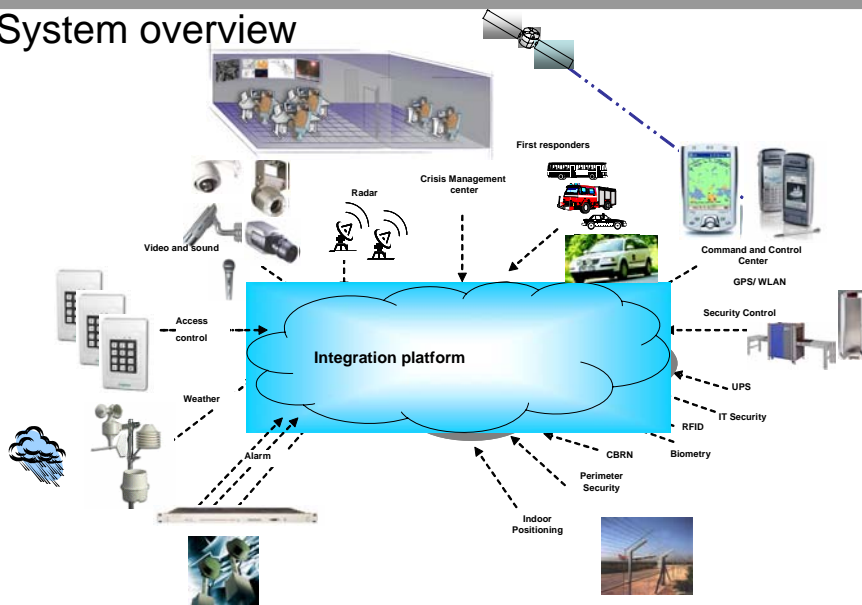


Background

Surveillance technologies for critical facilities

- Surveillance and protection of critical facilities is still a highly person-intensive task:
 - Costly
 - Tedious work make humans unreliable, i.e. vital signals and events may be missed
 - Danger to personnel
- Autonomous surveillance (and protection) techniques can **release personnel** from tedious/dangerous surveillance tasks and reduce the total life cycle cost of the surveillance of critical facilities
- New techniques can provide **enhanced** situation awareness (24/7/365)
- But, Introduction of new techniques **shall not** decrease the dependability or introduce a vulnerability to EM effects!

System overview



Basic System Components

Sensors

EO/IR



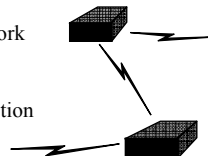
Radar



Other sensors like acoustic, pressure, heat,...

Communication and Processing units

- Robust wireless ad-hoc network
- Sensor data fusion and target tracking.
- Object and behavioural detection and threat analysis



Command and Control Unit



- Operator C2 HSI
- Situation awareness



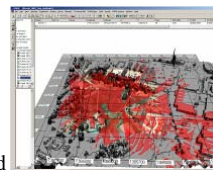
Support systems

Sensor deployment

- Calculates the sensor positions to gain optimal area coverage

Training

- Support for development and training of operational usage of the security system



5 www.saabgroup.com
© Saab AB 2007



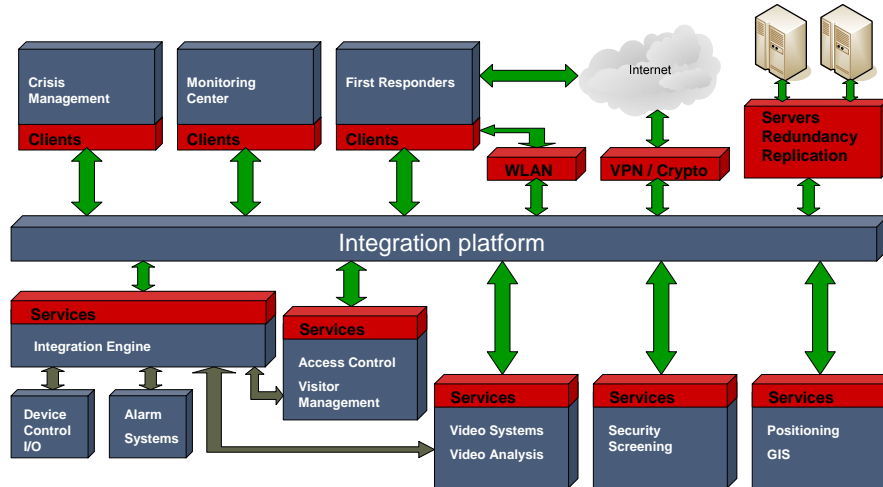
System Dependability

- The system needs to be robust and dependable even when subjected to intended disturbances and malicious attacks
- The system concept must be based on a combination of fault tolerance, redundancy and protection techniques, in order to achieve needed dependability
 - Redundant and/or complementary sensors and sensor technologies
 - Redundant and protected power supplies
 - Redundant and information-protected communications
 - Protected and authority controlled operator center(s) and computers
 - High EM shielding and protected installations
- The system responses and operator interfaces shall be easily understood

6 www.saabgroup.com
© Saab AB 2007



System overview



7 www.saabgroup.com
© Saab AB 2007



Capabilities

Intrusion detectors

Intrusion detectors are chosen individually for each situation to get optimal performance, extremely low false alarm rate and high detection capacity. The common types are:

- Passive infrared detectors (PIR)
- Passive infrared and doppler detectors (PIR+MW)
- Magnetic contacts
- Glass break sensors
- Infrared barriers



Perimeter detectors

Perimeter detectors primary function is to detect intrusion by humans, vehicles or other threats outside along the perimeter around a site. The most common perimeter detectors used at high security sites are:

- Ground Pressure Sensors
- Electrostatic field sensor
- Active microwave barriers
- Taut wire systems



In high risk areas normally two separate detection technologies are used in parallel.

8 www.saabgroup.com
© Saab AB 2007



Capabilities

Video analysis

In many cases analysis of video pictures from normal cameras, night vision cameras and thermo cameras can be used for efficient detection of large outside areas. The following analysis principles are all covered:



- **Advanced video sensor technology**
 - That is video motion detection that also analyses perspective, object speed and direction and combines that with filters for snow, rain and other climate conditions.
- **Object classification**
 - Analyses form, movement pattern, speed and more to differ between animals, humans, cars, trucks and more.
- **Static object detection**
 - The system learns the static framework of the scene and detects unknown new objects and removed known objects.
 - For example a car left in a forbidden area longer than a predefined time can trigger an alarm as well as a left suitcase at an airport.
- **Object behavior analysis**
 - For example if a human starts to crawl in an area where humans normally only walk or run it can trigger an alarm.

Capabilities

Sensor fusion

This means that data from many sensors of the same or different types are merged together to get as reliable detection as possible and also positioning of the object. In certain cases these solutions can give very good performance.

Highly focused area for development and research.

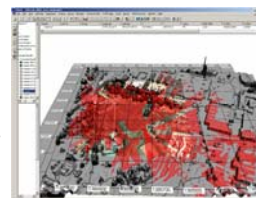
Presentation

In the monitoring center an “easy-to-understand” common situation awareness picture should be presented to the operator.

At bigger sites it is normal to have a local monitoring center combined with one or more centrally localized.

It is very important that there are always backup monitoring centers and communication links to keep the security level high.

Guards can have robust field units, WCU's (Wearable Command Units), that show maps, alarms, video images and more and also make possible receiving and sending text messages.

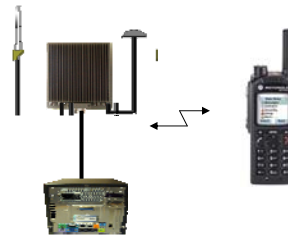


Capabilities

Communication

Different means of communications could be used to connect detectors and sensors with the presentation and control system at the monitoring centres.

Normally a fibre optic cable system would be used, as detectors/sensors require high bandwidth. Microwave or other radio based systems would be used for mobile detectors/sensors. Between different monitoring centres any high bandwidth communication system, public or private, could be used. If WCU is used for guards, patrols etc, a range of radio based communications systems may be used, such as TETRA, GSM, 3G or WiFi.



Summary and Conclusions

- The most important criteria in all large security solutions is reliability, robustness, flexibility and easiness to use.
- One solution is to use autonomous subsystems (alarm systems, video systems ...) and make them interact with each other through an integration platform.
- The integration platform makes it possible for the subsystems to exchange information with each other in a very secure way.
- On the other hand all subsystems work on their own in the case of communication failure. This is very important to get the robustness and it is always a must in high security applications.

Konstruktionsprinciper och metoder för telekonflikt-reducerande åtgärder

Studie genomförd inom FMV Teknikstudie Elektromagnetiska Mät- och Analysmetoder (TEMA)

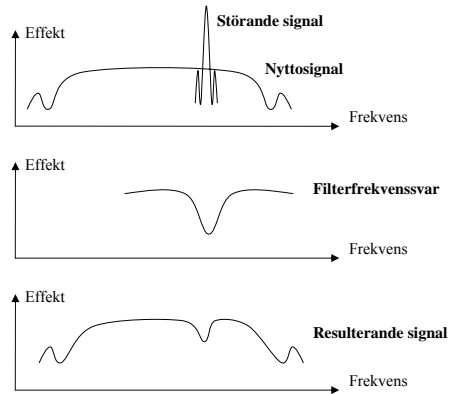
- **Beskrivning:**
- **Identifiera och utveckla lämpliga metoder och principer för att reducera telekonfliktseffekter i mottagarsystem.**
- Allmänt om mottagare utsatt för störning
- Kort beskrivning av ett urval av metoder
- Jämförelser av olika metoder

Allmänt om mottagarens situation vid störning

- Situationen skiljer sig markant från avsiktlig störning
 - Forskningsområdet har detta som grund, men med olika inriktning.
- Mycket finns att göra som förbättrar situationen.
 - Dock är informationsteoretiskt data förstörd.
- Värsta fallet är pulsat vitt brus
 - Ju mer man sedan vet om störningen desto bättre metoder kan implementeras

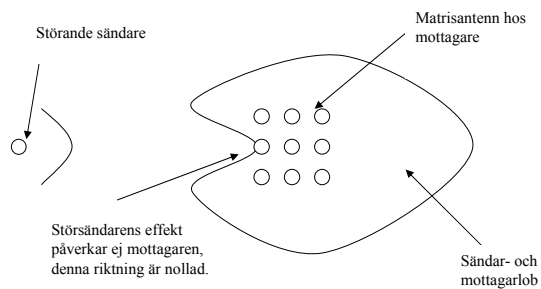
Notch-filtrering

- Enkel metod, ger inte så stor förbättring



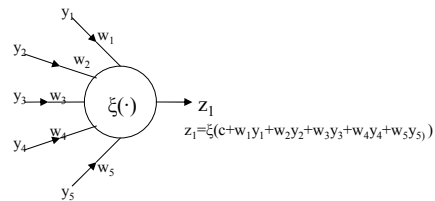
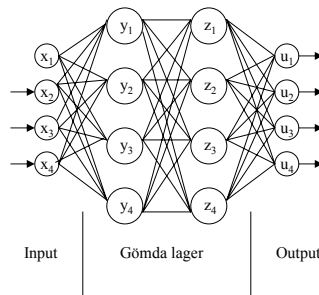
Lobstyrning

- Effektiv metod, men kräver multipla mottagarantenner.
- Ej digital metod



Neurala nätverk

- Effektiv metod, men skapar snabbt komplexa och minneskrävande system.

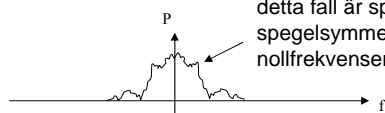


17 www.saabgroup.com
© Saab AB 2007

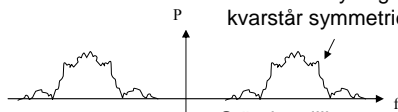


Cyclostationär filtrering

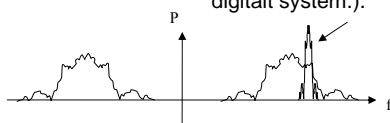
När modulation sker skapas en cyclostationär basbandssignal, i detta fall är spektrumet spegelsymmetriskt kring nollfrekvensen



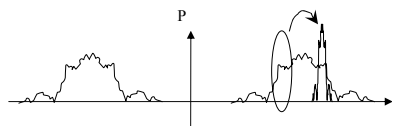
Efter heterodyning kvarstår symmetrierna



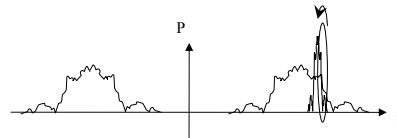
Störning tillkommer, även denna symmetrisk kring sin mittfrekvens (Om den kommer från ett annat digitalt system.).



Genom rätt digital frekvensskiftning och filtrering kan information från en ostörd del av spektrumet kopieras och ersätta den störda.



Ekvivalent kan den störande signalens redundans utnyttjas för att till del släcka ut sig självt.



18 www.saabgroup.com
© Saab AB 2007



Allmänt om störreducerande metoder

Analoga/digitala metoder

- Digitala mer flexibla, kan enkelt göras adaptiva. Kräver dock beräkningsresurs och skapar försening.
- Fel som uppstår i de analoga ingångsstegen avhjälps bäst analogt.

Blinda/ickeblinda metoder

- Användning av träningssekvenser, skapar adaptionsbrus

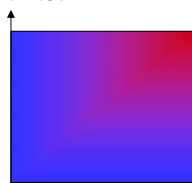
Linjära/olinjära metoder

- Olinjära teoretiskt mer effektiva men mer komplexa

Metoder för en kanal eller för flera kanaler

- Kräver multipla mottagarantenn

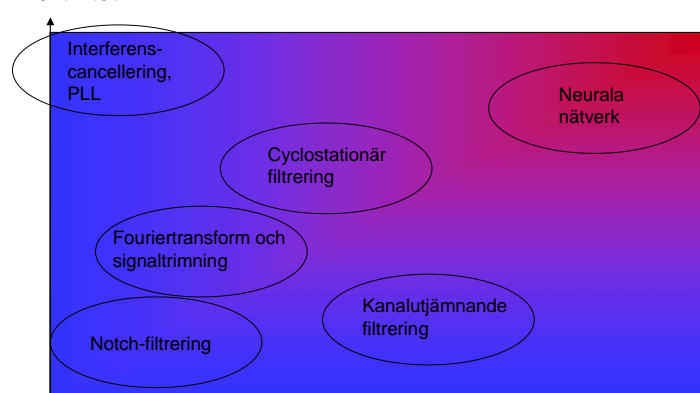
Effektivitet



■ Snabb åtgärd

■ Långsam/beräkningskrävande åtgärd

Effektivitet



■ Snabb åtgärd

■ Långsam/beräkningskrävande åtgärd

- Skall man bryta mot detta krävs extra åtgärder, t.ex. extra antenn eller fysisk flytt av antenn

Simuleringar

Några av metoderna simulerades

- Syfte att visa att det är relativt enkelt implementerbart
- Vissa förbättringar gavs genom användning. Många metoder är dock ortogonala, d.v.s. båda kan implementeras i samma system och ge varsitt förbättringstillskott.

