MLS for Tactical Soldier, Sensor and Munitions Networks

September 10, 2003

MITRE

Outline

- Purpose / Background
- Statement of the Challenge
- Additional Security Discussion
- Emerging Communication Network Architectures
  - Secure Gateway
  - MLS
- Secure Computing Card
- Summary

Purpose / Background

- **Purpose**
  - **The purpose of this briefing is to explore the challenges of Multi Level Security for Tactical Soldier, Sensor and Munitions systems**
- **Background**
  - **The potential solution that will be discussed in this presentation was initially explored through the Anti Personnel Landmine Alternative (APLA) Track 1 Non-Self Destruct Alternative, Spider System**

Statement of the Challenge

- **Networked Communications for the future force will require a seamless architecture ensuring information exchange capabilities between all nodes, including those of dissimilar classification levels**
  - **This type of network architecture requires Multi Level Security (MLS) in order to facilitate information exchange at the lowest possible level**
- **MLS is a complex and intricate issue that has yet to realize a fully effective tactical solution**
- **An effective tactical solution for Soldiers, Sensors and Munitions is critical for the Networked Centric Warfare concepts of the Objective Force**
  - **This solution MUST be capable of being handled as an unclassified, non Crypto Graphic Controlled Item in order to meet current policy and future operational and performance requirements**

Additional Security Discussion

- **While it is now allowable to use Advanced Encryption Standard (AES), a Type III (public - Non CCI) algorithm, for the protection of information up to Top SECRET, protection of classified information in an unencrypted state is still a major challenge for unattended and unclassified systems**
- **The availability of small, affordable, unclassified device that is capable of protecting classified information while remaining unclassified will facilitate a true MLS architecture**
  - **Such a device would only release classified information when authorization was confirmed via password and/or physical key (or other approved method) is supplied**
- **A device such as that listed above in addition to the approved use of a Type III algorithm for the protection of classified information will facilitate true MLS functionality by allowing unclassified through Top SECRET Soldier, Sensor and Munitions nodes to be connected to the same network**

Emerging Communication / Networking Architecture using Secure Gateway

Security

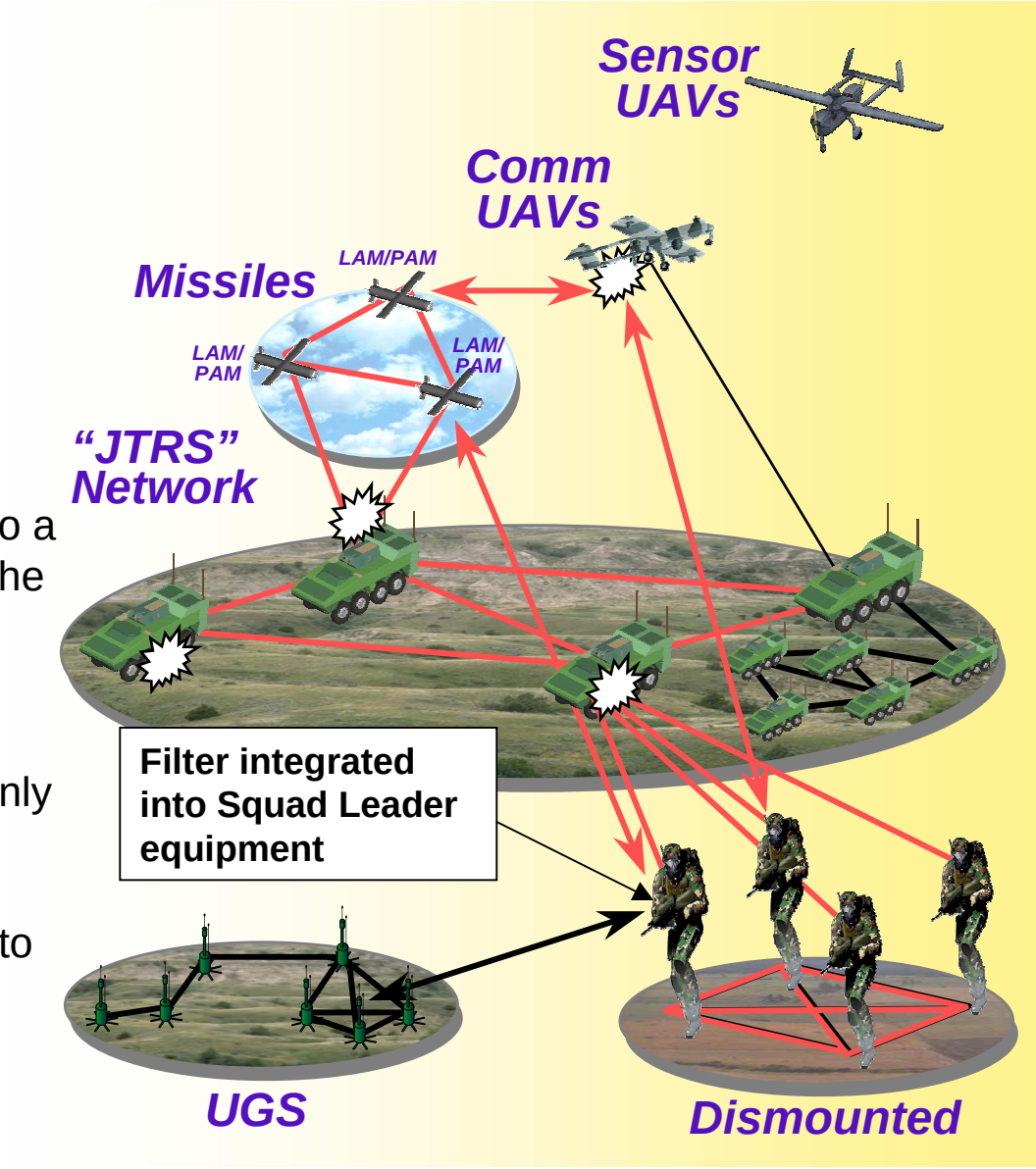
Either a High Assurance Secure gateway is required between the classified network an the unclassified Warriors, or the network needs to be multi level secure

High Assurance Secure Gateway

The backbone network is classified, so a secure gateway is required between the backbone and the unclassified node (warrior)

- Where will the gateway be?
- All nodes *below* the gateway will only have access to unclassified Information and every message coming in to the gateway will have to be filtered by that Gateway node

Classified Net
Unclassified Net



Emerging Communication / Networking Architecture using full MLS solution

Security

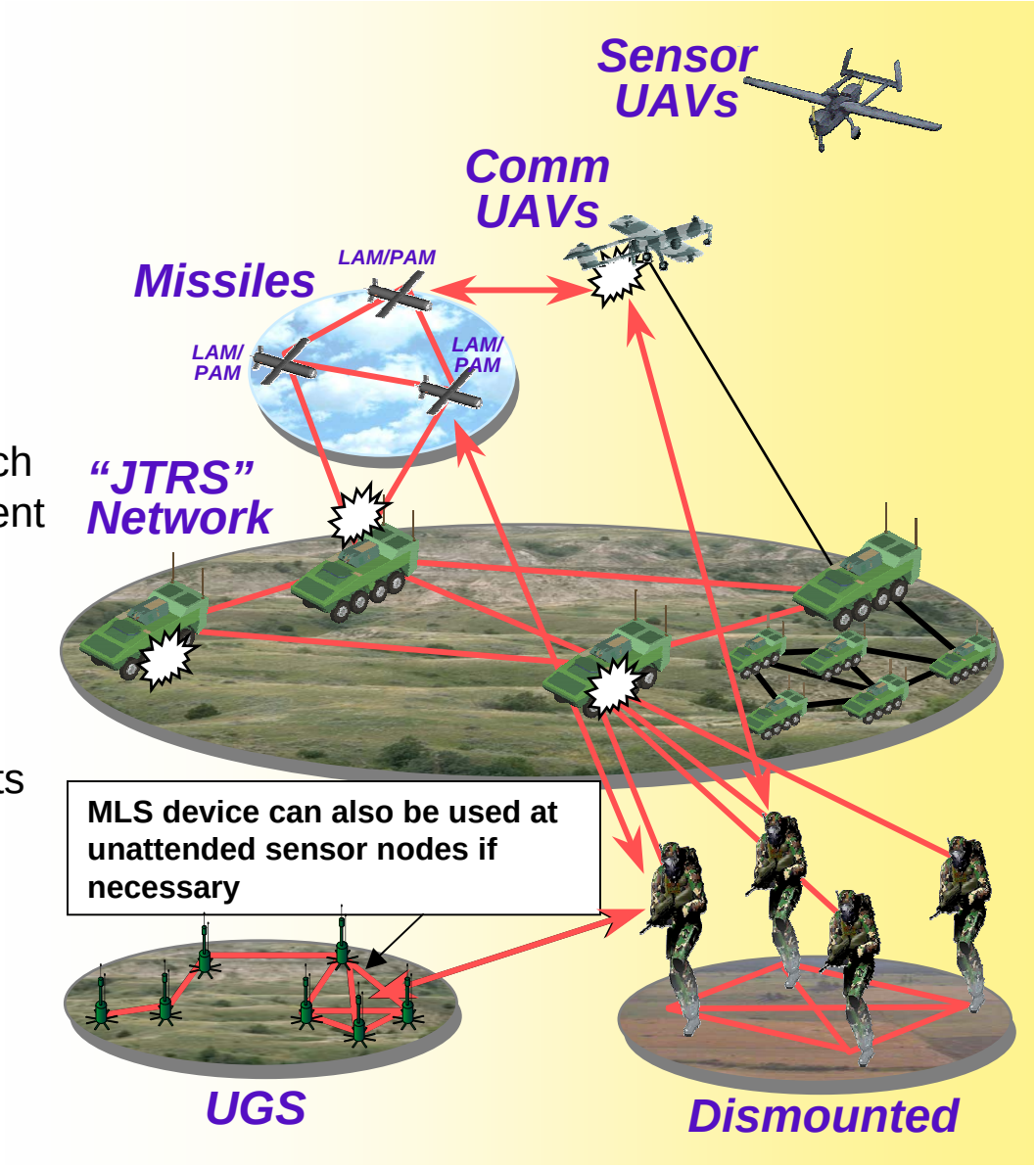
Either a High Assurance Secure gateway is required between the classified network an the unclassified Warriors, or the network needs to be multi level secure

Multi Level Security

The network is classified, but now each node (Warrior) has the same equipment that is configure for that soldiers clearance.

No choke point for message filtering.

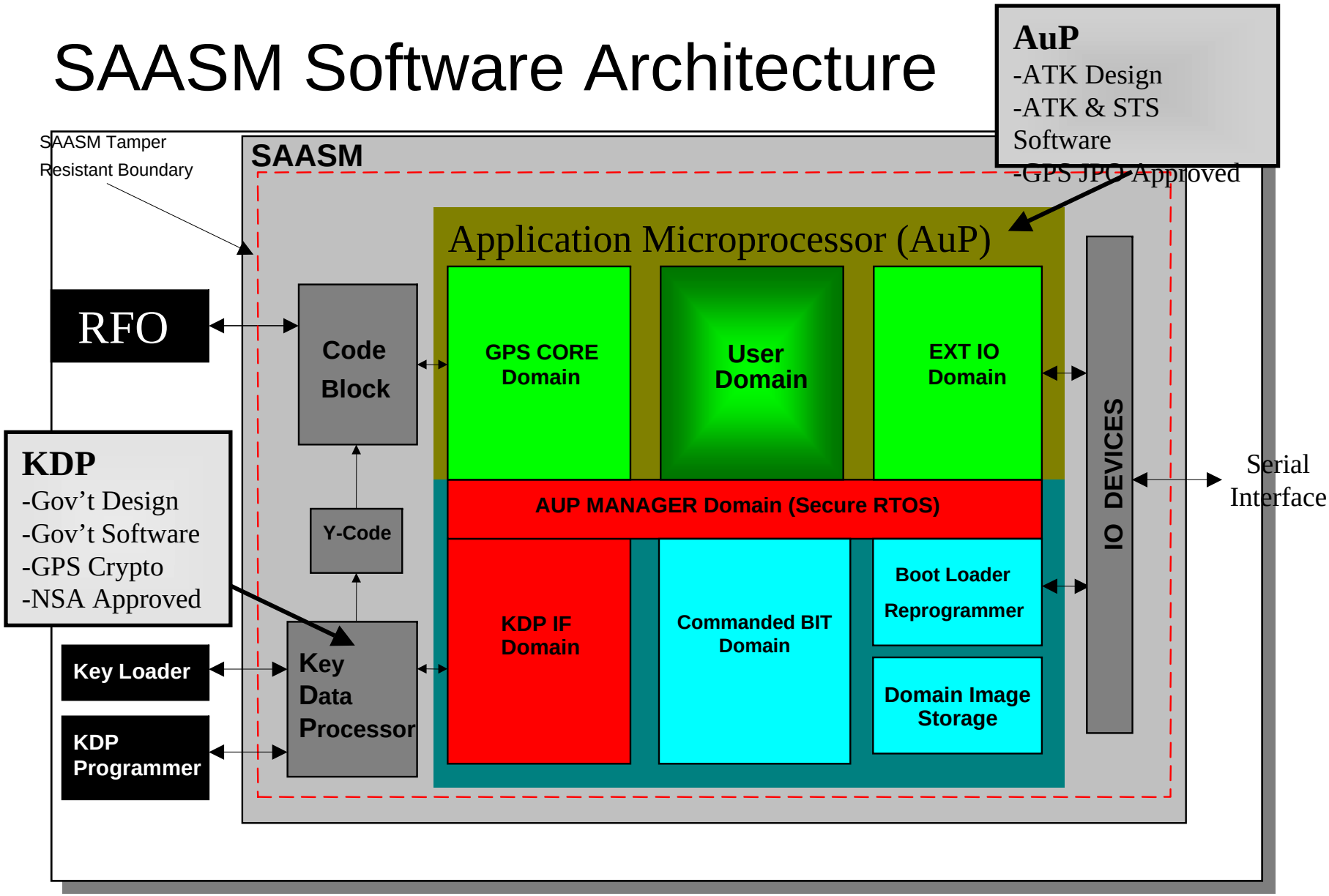
Each messages is filtered at its destination



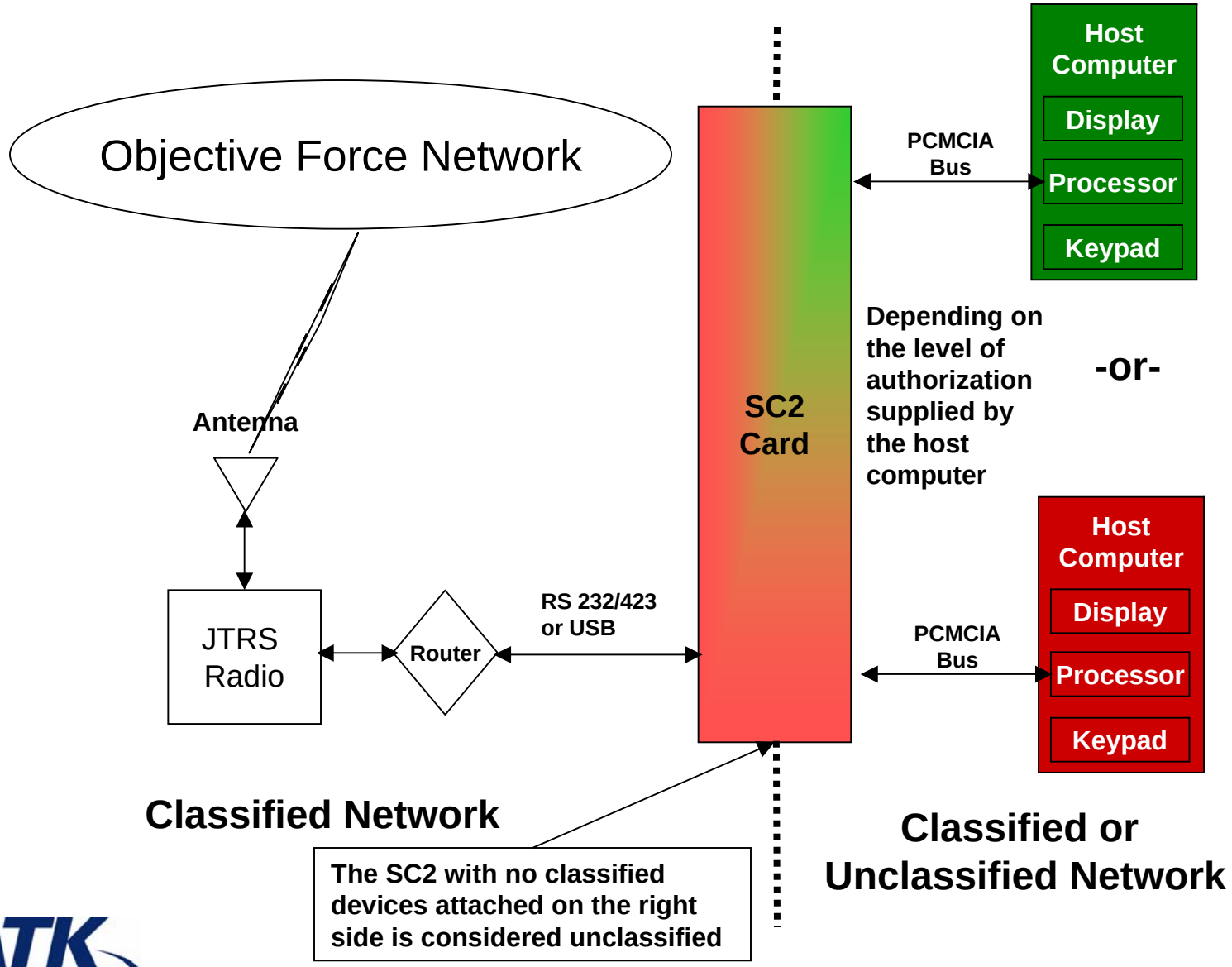
Secure Computer Card (SC2) Background

- **During early development of the Spider APLA system, there was a requirement for the manned portion of the system to contain/protect classified information while being operated by an unclassified user**
- **The proposed solution to meet the above requirement was to use the Secure Computer Card (SC2), which used the same technology used by the Selective Availability Anti Spoofing Module (SAASM), the security module for the emerging military GPS systems**
  - **The SAASM module uses physical and software protective measures that allowed it to contain and process classified information, while the module itself remains unclassified**
- **Due to Landmine Security Doctrine change, the SC2 functionality is no longer required by Spider**
  - **A prototype exists that will filter messages based on format and JVMF message header**

SAASM Software Architecture



SC2 Functional Architecture



MITRE

Summary

- The protective measures of the SC2 would allow for it to be handled as an unclassified device based on the level of the authentication
  - It can maintain segregation of data of multiple classification levels and release that data only with the appropriate authorization
- Network, radios and SC2 would be MLS while host computer would operate in a single level of security
- Would require interaction with NSA and CIO/G6 to approve connection (authentication) between network radio and SC2 card, unless SC2 handles the encryption / decryption
  - Additional Authentication may be required between radio and SC2
- SC2 concept still needs to be certified and accredited

Acronyms

- AES – Advanced Encryption Standard
- APLA – Anti Personnel Landmine Alternative
- CCI – Controlled Cryptographic Item
- JTRS – Joint Tactical Radio System
- JVMF – Joint Variable Message Format
- MLS – Muli Level Security
- NSD-A - Non Self Destruct Alternative
- NSA – National Security Agency
- SAASM – Selective Availability Anti Spoof Module
- SC2 – Secure Computer Card
- UAV - Unmanned Air Vehicle
- UGS – Unmanned Ground Sensors