

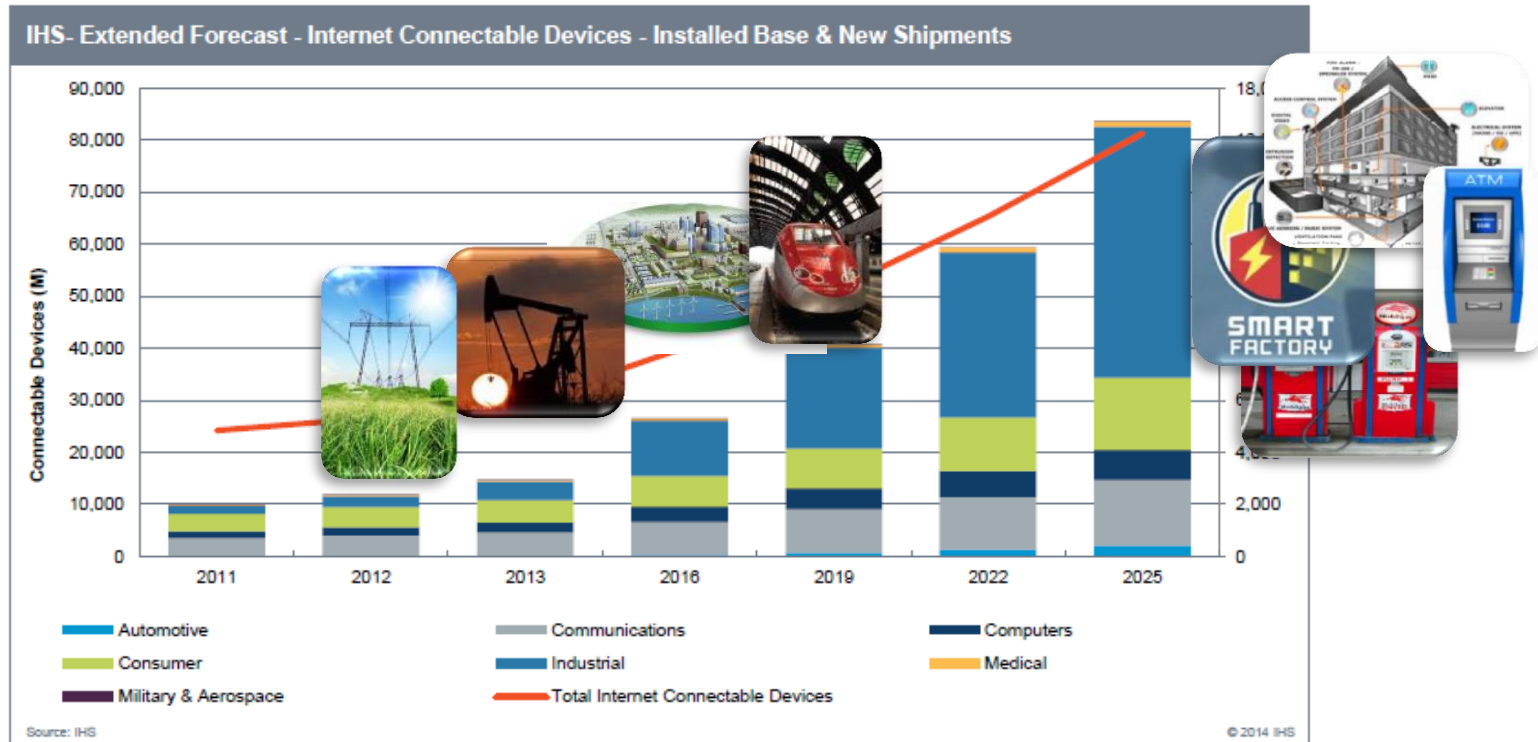
# Service-Aware Security for Distributed Automation



Ilan Barda  
GRIPS SciREX Symposium  
February 2<sup>nd</sup> 2015

**radiflow**  
Secure your Assets

# The market – Securing the Industrial IoT



## Industrial Control System (ICS) Security Market worth \$8.73 Billion by 2019

Source: MarketsandMarkets, December 2014

The report "**Industrial Control System (ICS) Security Market by Technology (DDOS, IDS/IPS, Firewall, SIEM, SCADA Encryption, UTM, Application, Whitelisting, DLP, Database Activity Monitoring), by Services, and by Verticals - Global Forecast to 2019**", segments the global ICS security market into various sub-segments with in-depth analysis and forecasting of revenues. It also identifies drivers and restraints for this market with insights into trends, opportunities, and challenges.

# Radiflow Mission

- Utilities deploy modern **Distributed Automation** devices connecting **Remote locations** over large-scale **IP networks**
- Exposing **Critical applications** to **Cyber Security Attacks**



Radiflow provides Cyber Security solutions for Critical Distributed Automation networks

# Growing cyber-threat for SCADA networks

Some believe Stuxnet worm marks new age of super-cyber weapons

Published In: [Intelligent Utility](#)

MIT  
Technology  
Review

Friday, August 02, 2013

Chinese Hacking Team Caught Taking Over Decoy Water Plant

(AND WORST)  
[SEE WHAT'S NEW >>](#)

**Bloomberg**


Your world.  
**Ranked.**

## Russian Hackers Threaten Power Companies, Researchers Say

By Amy Thomson and Cornelius Rahn | Jul 1, 2014 3:05 PM GMT+0300 | [65 Comments](#) [Email](#) [Print](#)

A Russian group of hackers known as “Energetic Bear” is attacking energy companies in the U.S. and **Europe** and may be capable of disrupting power supplies, cybersecurity researchers said.

27 February 2014 Last updated at 00:26 GMT

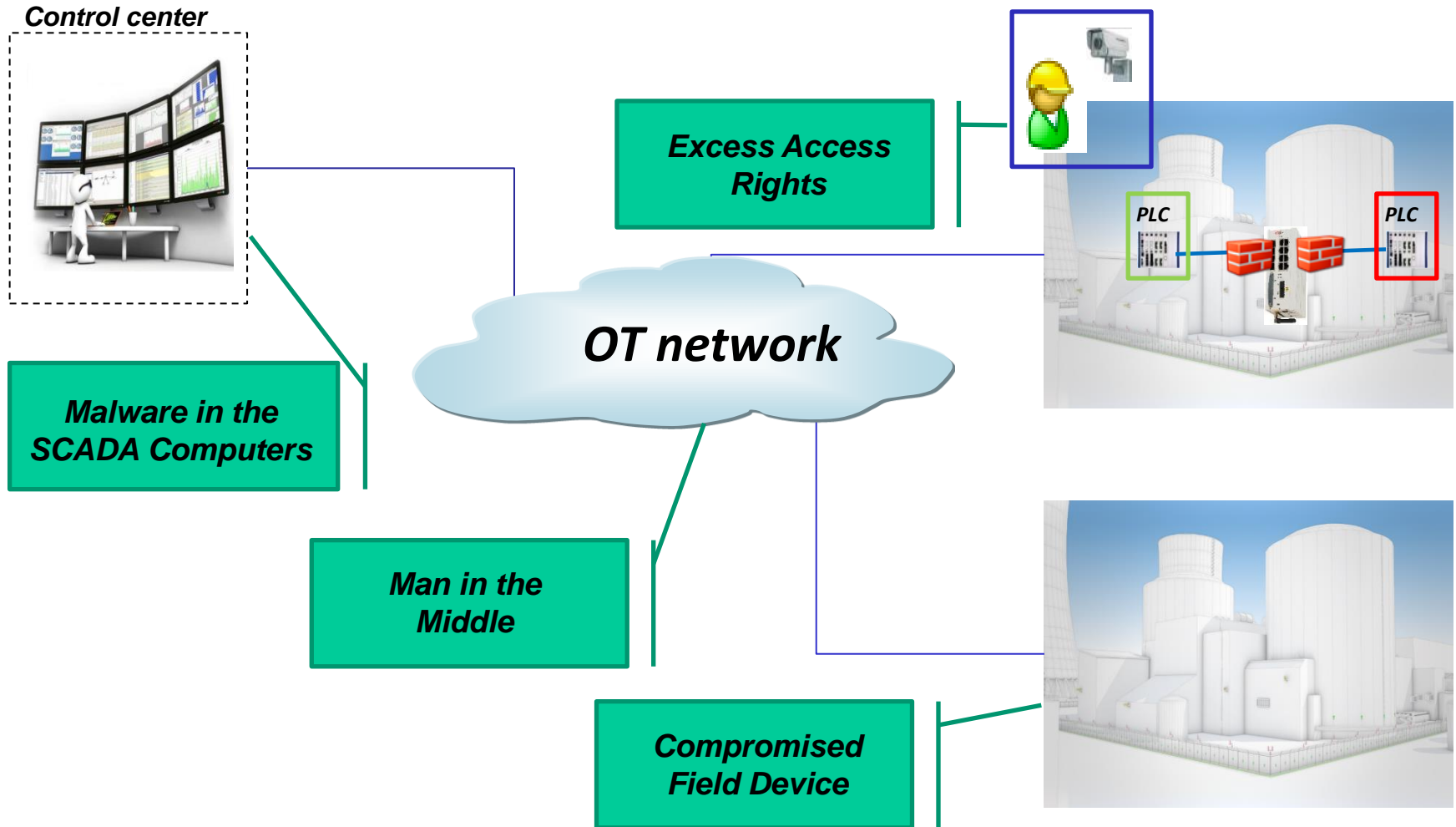
[Share](#) 

## Energy firm cyber-defence is 'too weak', insurers say

By Mark Ward

Technology correspondent, BBC News

# Attack Vectors on the OT network



# Remote utility sites are the weakest link

- **SCADA networks were designed for security by obscurity**
  - Industrial automation devices utilize basic authentication methods
  - SCADA protocols do not support any role-based authorizations
- **Physical access to a remote site can be easily gained**
  - Remote sub-stations are unmanned
  - Authorized site visitors gain access to the local network
- **Inter-site sessions should not be considered trusted**
  - An insider in 1 site can gain unsupervised access to other sites
  - Man-in-Middle attacks can hack into the private network



***“smart grid cyber-security guidelines did not address an important element... risk of attacks that use both cyber and physical means”***

*Electricity Grid Modernization; Report to Congressional requesters, US GAO, January 2011*

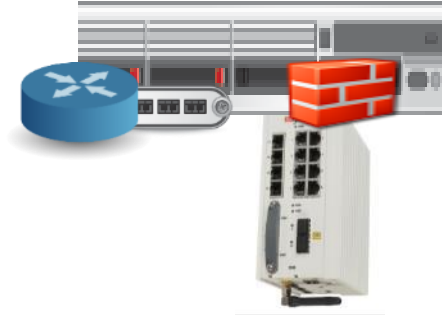


# Radiflow Portfolio Evolution



**Identity  
Management**

**SCADA Behavioral  
Detection Server**



**SCADA  
IPS/IDS**

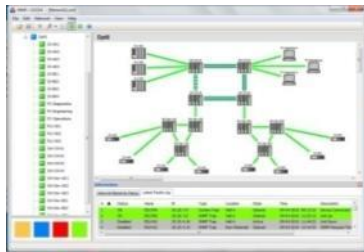
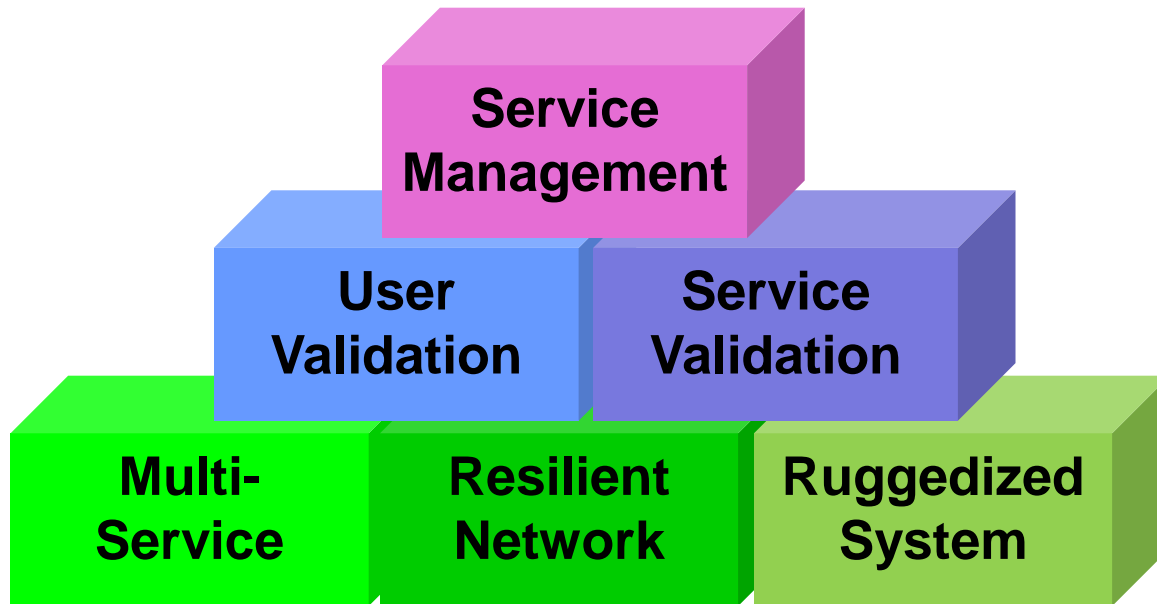


**Secure Utility  
Gateway/Router**



**Physical & Cyber  
Integration**

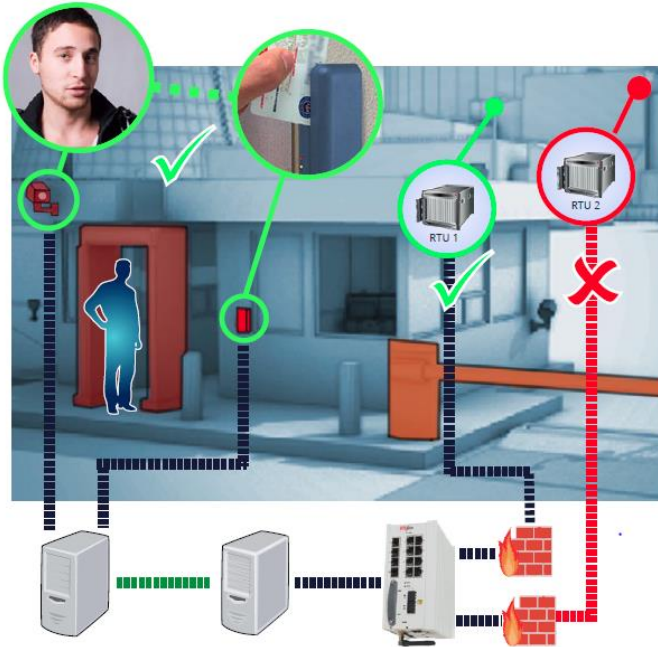
# Easy deployment using Secure Gateways/Routers



- Field deployment
  - Power Sub-stations
  - Railways/Highways
  - Explosive areas
- Variety of interfaces
  - Ethernet
  - Serial
  - Cellular
  - Discrete I/O
- Security tool-set
  - Application validation
  - User authentication
  - Data encryption



# Integrated Physical & Cyber security

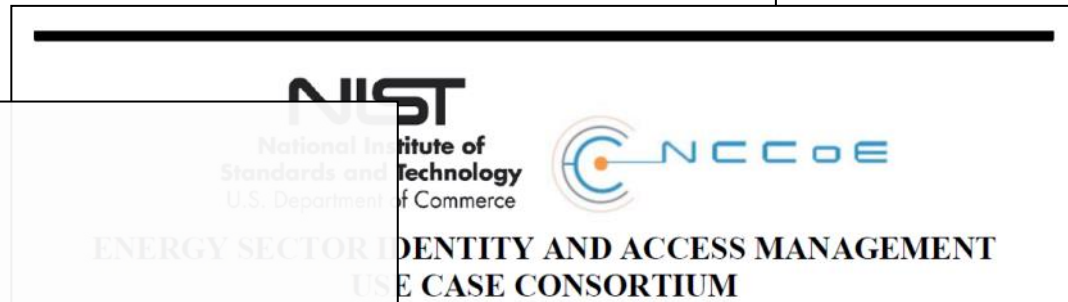
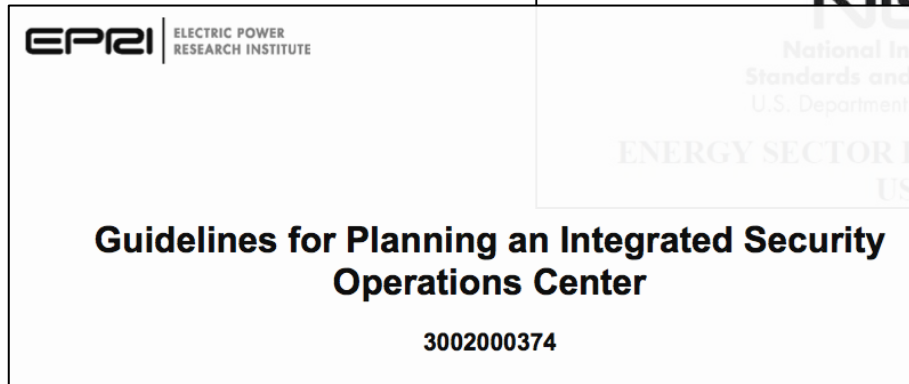
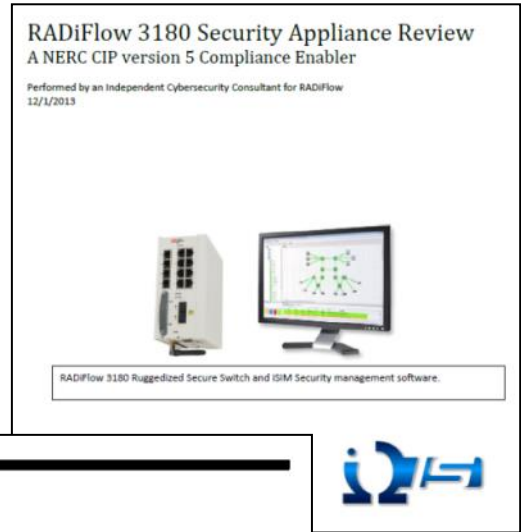


- Distributed SCADA IPS in each site
- Correlation with physical security systems for dynamic user authentication
- Validate per-user SCADA operations
- Integration with central SIEM tool

***Task-based access control by dynamically allocating physical & logical security resources based on physical & logical triggers***

# Security solution validated by US Research Labs

- Role Based IPS/IDS for SCADA Protocols
- Securing Data Traffic (Legacy or IP)
- Secure Authentication
- Persistent, Reliable Logging



# Field-proven technology



# Focus applications

- Power T&D (Smart-Grid, Sub-station automation)



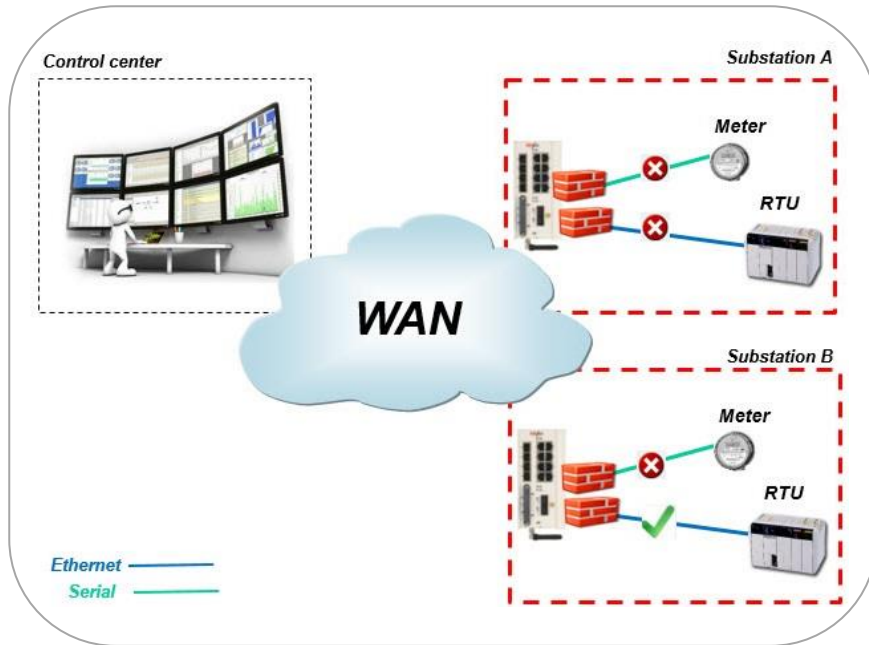
- Smart-City, Safety and Security

- Intelligent Transportation (Railways, Highways)

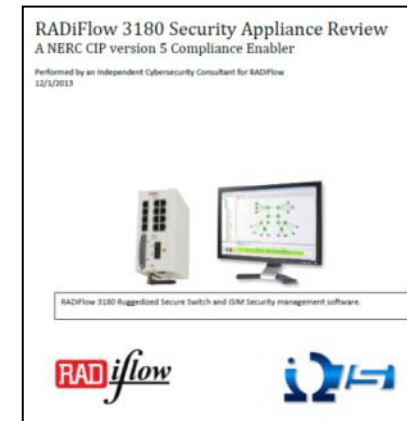


- Drilling and Pipelines (Water, Oil & Gas)

# Secure Access for Substation Automation

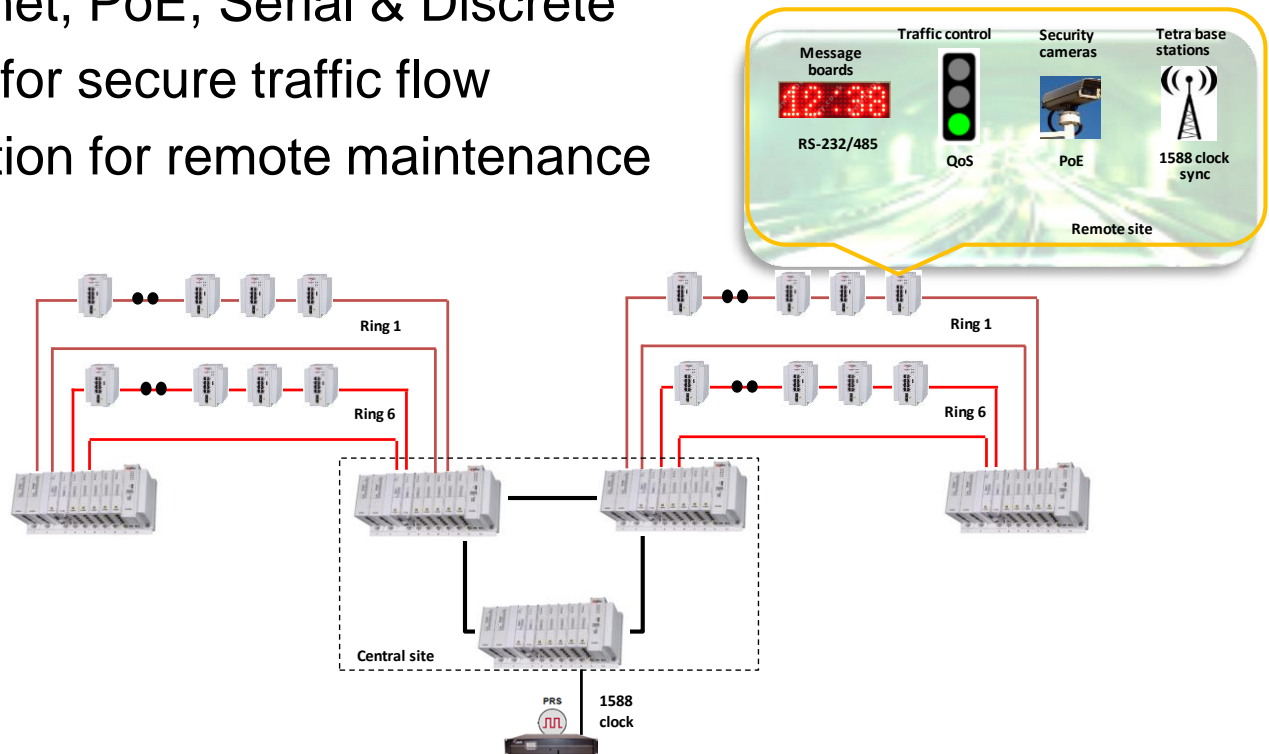


- Identity management for detailed per user authorizations
- Validation of SCADA behavior per user
- Automatic learning of SCADA behavior
- Detailed log of user activities
- IPsec VPN for inter-site connectivity
- Support Ethernet and Serial devices



# Large scale control for Intelligent Transportation

- Modern Railway/Highway control applications require
  - Ethernet rings for reliable networking
  - Mixture of Ethernet, PoE, Serial & Discrete
  - ModBus firewall for secure traffic flow
  - User Authentication for remote maintenance





# Summary

---

- Modern distributed automation applications use IP networks
  - Intra-network security is mandatory
- Radiflow Service-aware Industrial security solution
  - Integrated defense-in-depth tool-set
  - Optimize CapEx and OpEx

For more details:

[info@radiflow.com](mailto:info@radiflow.com)

[www.radiflow.com](http://www.radiflow.com)

