Reliability of Communication

in the INSPIRE Project

MICIE – Final Workshop
Rome, Italy, Feb 28, 2011

Marcello Antonucci, SELEX Sistemi Integrati

PRESENTATION PLAN

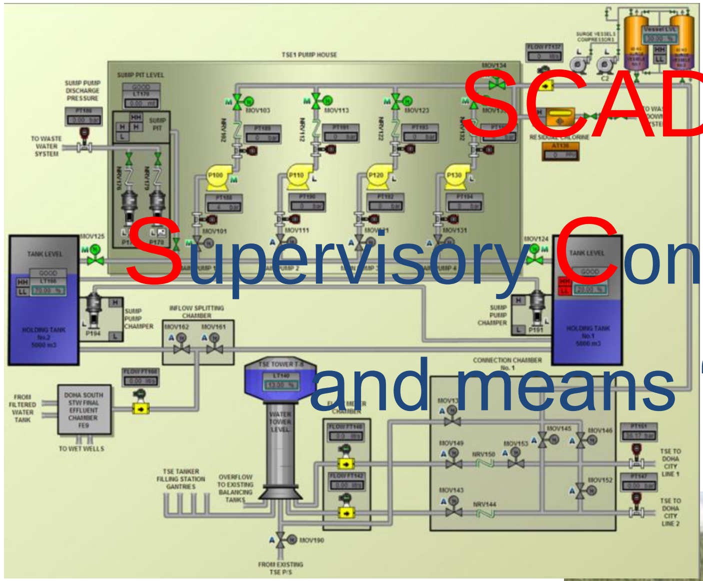
1. What are SCADA systems

2. How they put Critical Infrastructures at risk

3. Objectives of the INSPIRE project

4. Results of the INSPIRE project

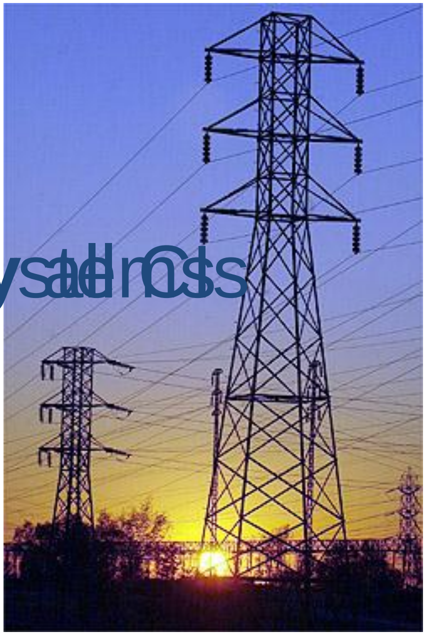
SCADA systems and Critical Infrastructures



SCADA stands for

Supervisory Control And Data Acquisition

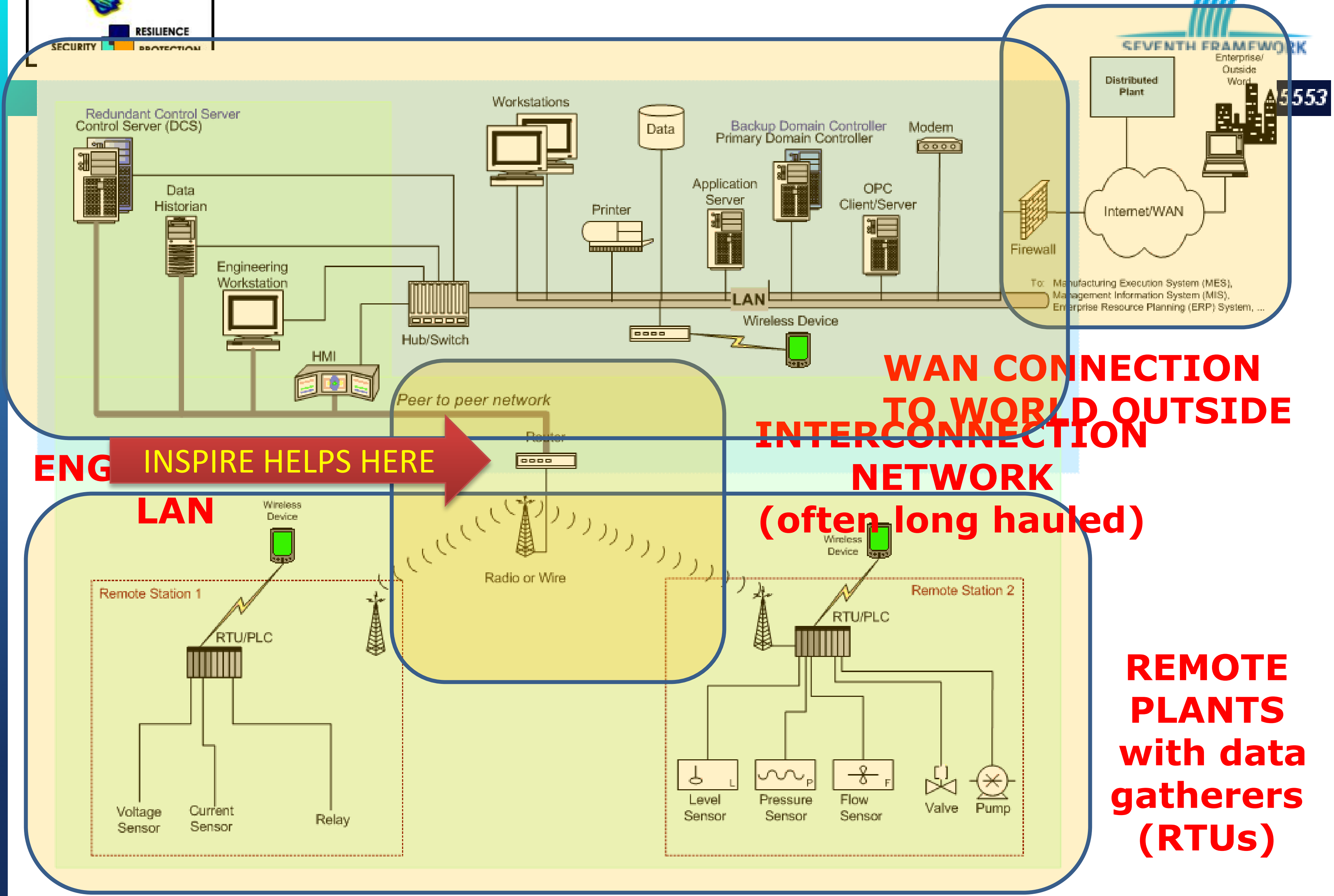
and means "Remote Monitoring"



SCADA systems are used in all CIs

These are examples of SCADA [illegible]

BASIC ARCHITECTURE



WAN CONNECTION TO WORLD OUTSIDE

INTERCONNECTION NETWORK (often long hauled)

ENG LAN

INSPIRE HELPS HERE

REMOTE PLANTS with data gatherers (RTUs)

Figure 2: Generic Industrial Control System Network Architecture - SCADA

5553

A SOURCE OF TROUBLE

- Large infrastructures managed through SCADA systems have a very long lifetime
- So do the SCADA systems!
- Some early digital SCADA systems (70’s) are still in operation, although they have evolved
- Evolution is mostly done by slow adaptation: *rip’n’replace* is very rare

No rip'n'replace?

- *“Evolution is mostly done by slow adaptation: rip’n’replace is very rare”*
  - ⇨ Systems currently in operation implement **brand new technologies,** side-by-side with systems based on old design, old technology, **old assumptions**
- This coexistence is unavoidable but **it is extremely dangerous**. We’ll see why.

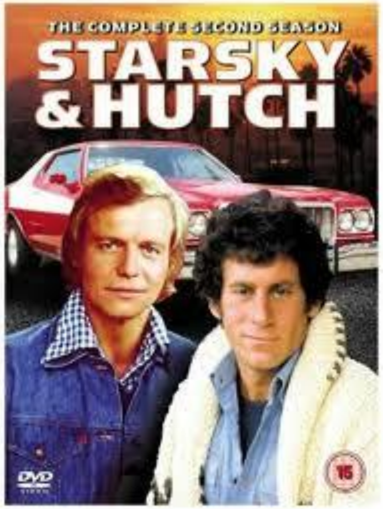
EARLY SCADA ARCHITECTURE

	70's	IMPLICATION ON SECURITY
COMPUTING EQUIPMENT	MAINFRAME	Secure by design. Service was performed by the manufacturer, so the hardware architecture was not documented and unknown to the mass.
SYSTEM SOFTWARE	PROPRIETARY	Secure by design. Industrial-grade by [illegible]n. [illegible] us[illegible] th[illegible]n.
COMMUNICATION LINES	LEASED (copper wire)	Eavesdropping required physical access to that wire, or to the PSTN switches.
APPLICATION SOFTWARE	AD-HOC CONTRACTED	Every system was unique. Flaws in [illegible] system could [illegible]t put a[illegible] th[illegible] at risk
STANDARDS AND PROTOCOLS	PROPRIETARY	[illegible]t [illegible] documented, not [illegible]able in consumer devices.

very secure, but... €xtremely €xpen$ive!

SCADA IN THE 70's

LIFE IN THE 70's



cr s

ea lo

ir The

b ata

a

No passwords: In case of an incident, an operator und e it or try it se on. That wou es!"

- **Peri** and are well ont door and doors".

EVOLUTION OF THE SCADA ARCHITECTURE

	70's	80's – 90's	00's – 10's
COMPUTING EQUIPMENT	MAINFRAME	MINICOMPUTERS (DEC, SUN, HP, IBM)	CONSUMER
SYSTEM SOFTWARE	PROPRIETARY	PROPRIETARY (VMS) TO OPEN (UNIXes)	UNIX, WINDOWS
COMMUNICATION LINES	LEASED (copper wire)	PACKET (X.25, frame relay)	INTERNET
APPLICATION SOFTWARE	AD-HOC BIG CONTRACTS	AD-HOC BASED ON COTS	COTS CONFIGURATION
STANDARDS AND PROTOCOLS	P	N OF RDS	MASSIVE USE OF OPEN STANDARDS

PRACTICALLY THE SAME TECHNOLOGIES THAT MILLIONS OF PEOPLE USE AT HOME

THE RISKS OF THE CURRENT ARCHITECTURE

	00's – 10's	WHAT'S THE RISK
COMPUTING EQUIPMENT	CONSUMER	Viruses
SOFTWARE	CONFIGURATION	
STANDARDS AND PROTOCOLS	MASSIVE USE OF OPEN STANDARDS	

VIRUSES

On mainframes and minicomputers, different disks were used for data and programs; the disks for programs were read-only, using a hardware switch. Then came Windows and the registry...

THE RISKS OF THE CURRENT ARCHITECTURE

	00's – 10's	WHAT'S THE RISK
COMPUTING EQUIPMENT	CONSUMER	Viruses **Standard peripherals (DVD, USB...)**
	N	
STANDARDS AND PROTOCOLS	MASSIVE USE OF OPEN STANDARDS	

MOUNTABLE MEDIA

On mainframes and minicomputers, external media were tape reels. No workstation operator could bring one from home and mount it. Actually, no operator had a tape reader at home. Now, reported SCADA incidents include operators mounting USB memory sticks or watching video on DVDs.

THE RISKS OF THE CURRENT ARCHITECTURE

	00's – 10's	WHAT'S THE RISK
COMPUTING EQUIPMENT	CONSUMER	Viruses Standard peripherals (DVD, USB...)
SYSTEM SOFTWARE	UNIX, WINDOWS	**Knowledge is widespread (incl. that of weaknesses!) Operators know how to (ab)use**
	ON	
	OF RDS	

AN EXAMPLE OF A WEAKNESS

SUN Microsystems, Inc.
Solaris 2.4 (SunOS 5.4)
patch # 102044-01
12 Sep 1994
*<<Bug in **mouse code** makes "**break root**" attack possible>>*

THE RISKS OF THE CURRENT ARCHITECTURE

11 Jan 2008

<<A teenage boy hacked into a Polish tram system and used it like "a giant train set", causing chaos and ***derailing four vehicles****. The* ***14-year-old****, a model pupil and an electronics "genius",* ***adapted a television remote control*** *so it could change track points in the city of Lodz.>>*

		WHAT'S THE RISK
		Viruses Standard peripherals (DVD, USB...)
		Knowledge is widespread (incl. that of weaknesses!) Operators know how to (ab)use
COMMUNICATION LINES	INTERNET	**Every teenager can try to break an IP address… and maybe succeed**
APPLICATION SOFTWARE	COTS CONFIGURATION	
STANDARDS AND PROTOCOLS	MASSIVE USE OF OPEN STANDARDS	

THE RISKS OF THE CURRENT ARCHITECTURE

14 Apr. 2008
US-CERT
Vulnerability Note VU#476345

CitectSCADA ODBC service buffer overflow

<<Citect CitectSCADA contains a remotely accessible buffer overflow vulnerability which may allow a remote attacker to ***execute arbitrary code****.>>*

		WHAT'S THE RISK
		Viruses Standard peripherals (DVD, USB...)
		Knowledge is widespread (incl. that of weaknesses!) Operators know how to (ab)use
		Every teenager can try to break an IP address... and maybe succeed
APPLICATION SOFTWARE	COTS CONFIGURATION	**Copies of the app s/w can be purchased, studied and broken**
STANDARDS AND PROTOCOLS	MASSIVE USE OF OPEN STANDARDS	

THE RISKS OF THE CURRENT ARCHITECTURE

	00's – 10's	WHAT'S THE RISK
		Viruses Standard peripherals (DVD, USB...)
		Knowledge is widespread (incl. that of weaknesses!) Operators know how to (ab)use
		Every teenager can try to break an IP address... and maybe succeed
		Copies of the app s/w can be purchased, studied and broken
STANDARDS AND PROTOCOLS	MASSIVE USE OF OPEN STANDARDS	**Every weakness discovered in a standard exposes some systems**

WEP "Security"

WEP = "**Wired-Equivalent(!) Privacy**"

The first encryption protocol for Wi-Fi networks, deemed "secure enough". Research (TUD, 2007) led to break it in **less than 60"**, with 3" of CPU time on a Pentium-M IV, 1.7GHz, 3MB memory (no, not *giga*: *mega*!).

It is still available as an option in most Wi-Fi devices and **might be still in use** somewhere.

THE RISKS OF THE CURRENT ARCHITECTURE

INSPIRE addresses this one

	00's – 10's	**WHAT'S THE RISK**
COMPUTI EQUIP		Viruses Standard peripherals (DVD, USB...)
SYSTEM SOFTWARE	NIX, WINDOWS	Knowledge is widespread (incl. that of weaknesses!) Operators know how to (ab)use
COMMUNICATION LINES	INTERNET	**Every teenager can try to break an IP address... and maybe succeed**
APPLICATION SOFTWARE	COTS CONFIGURATION	Copies of the app s/w can be purchased, studied and broken
STANDARDS AND PROTOCOLS	MASSIVE USE OF OPEN STANDARDS	Every weakness discovered in a standard opens some doors to some systems

An(other) example of network intrusion

***Maroochy Shire Sewage Spill** incident, spring 2000.*

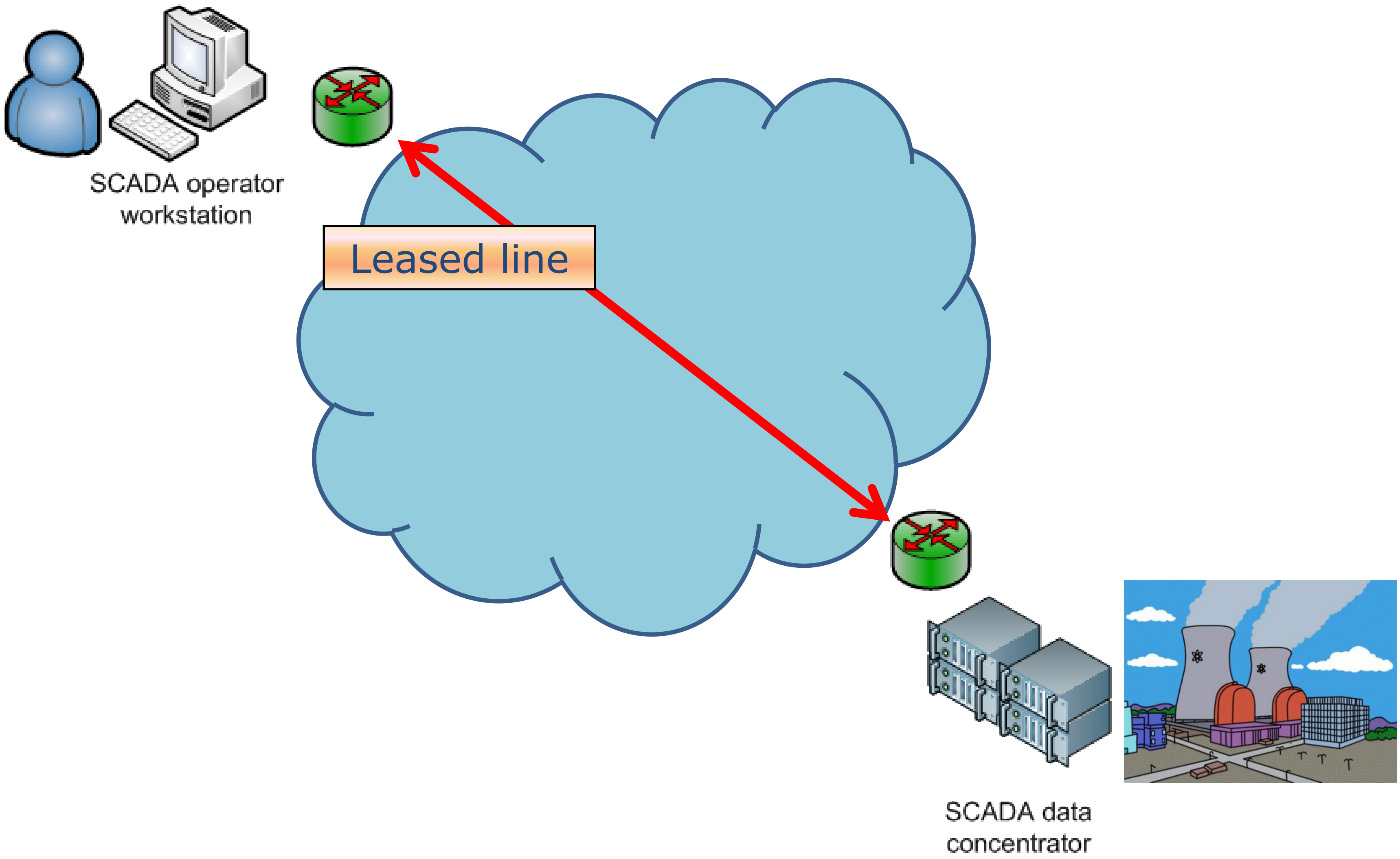
***Ingredients**: a disgruntled fired employee, his notebook and Wi-Fi coverage in the parking lot.*

***Action**:*

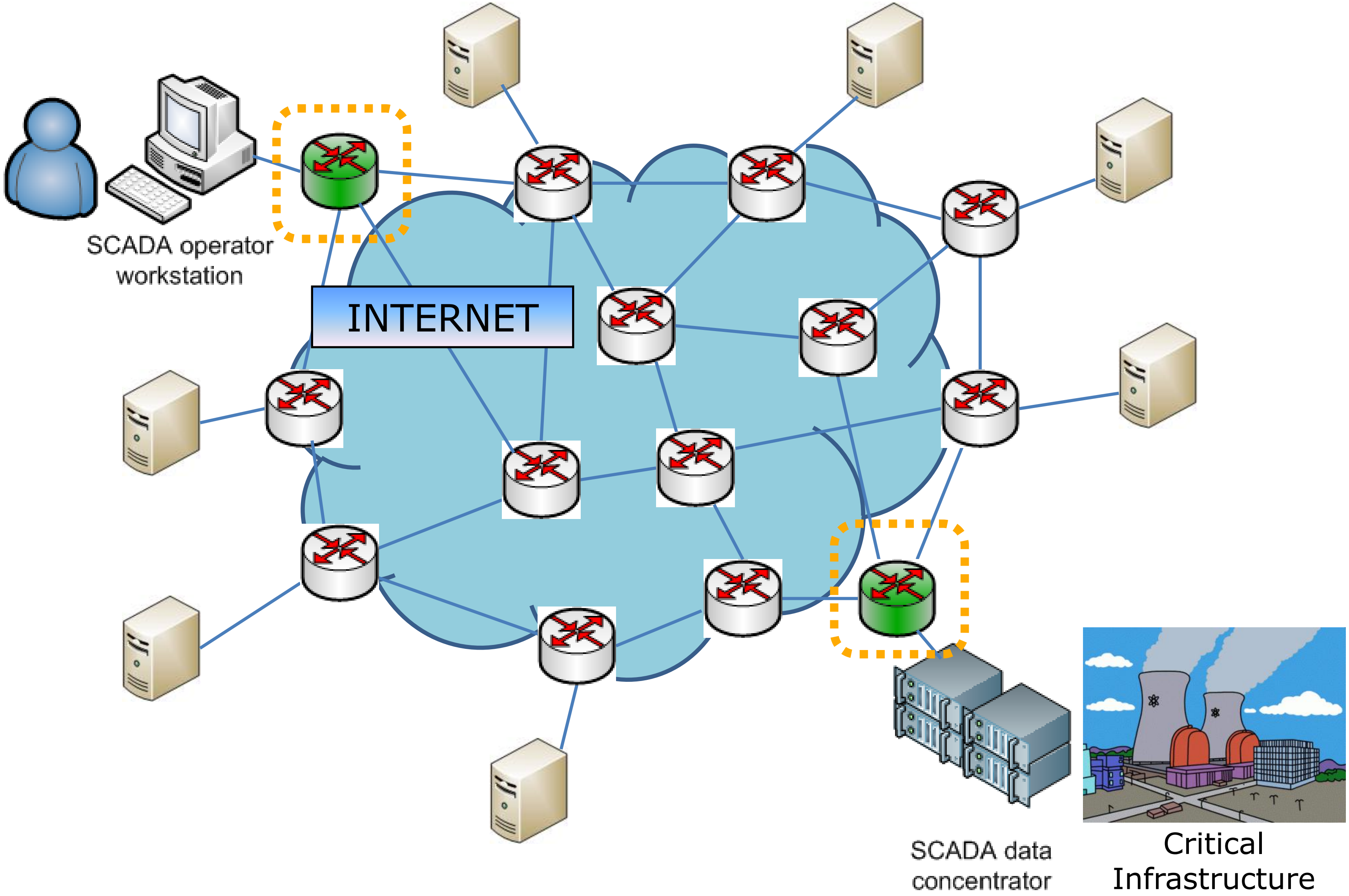
1. *park in the parking lot;*
2. *switch on the notebook;*
3. *switch on Wi-Fi;*
4. *connect to the WLAN of the plant;*
5. *run the SCADA client software;*
6. *show the bastards how's life without me...*

***Result**: 264,000 gallons (900 tons) of raw sewage released into nearby rivers and parks.*

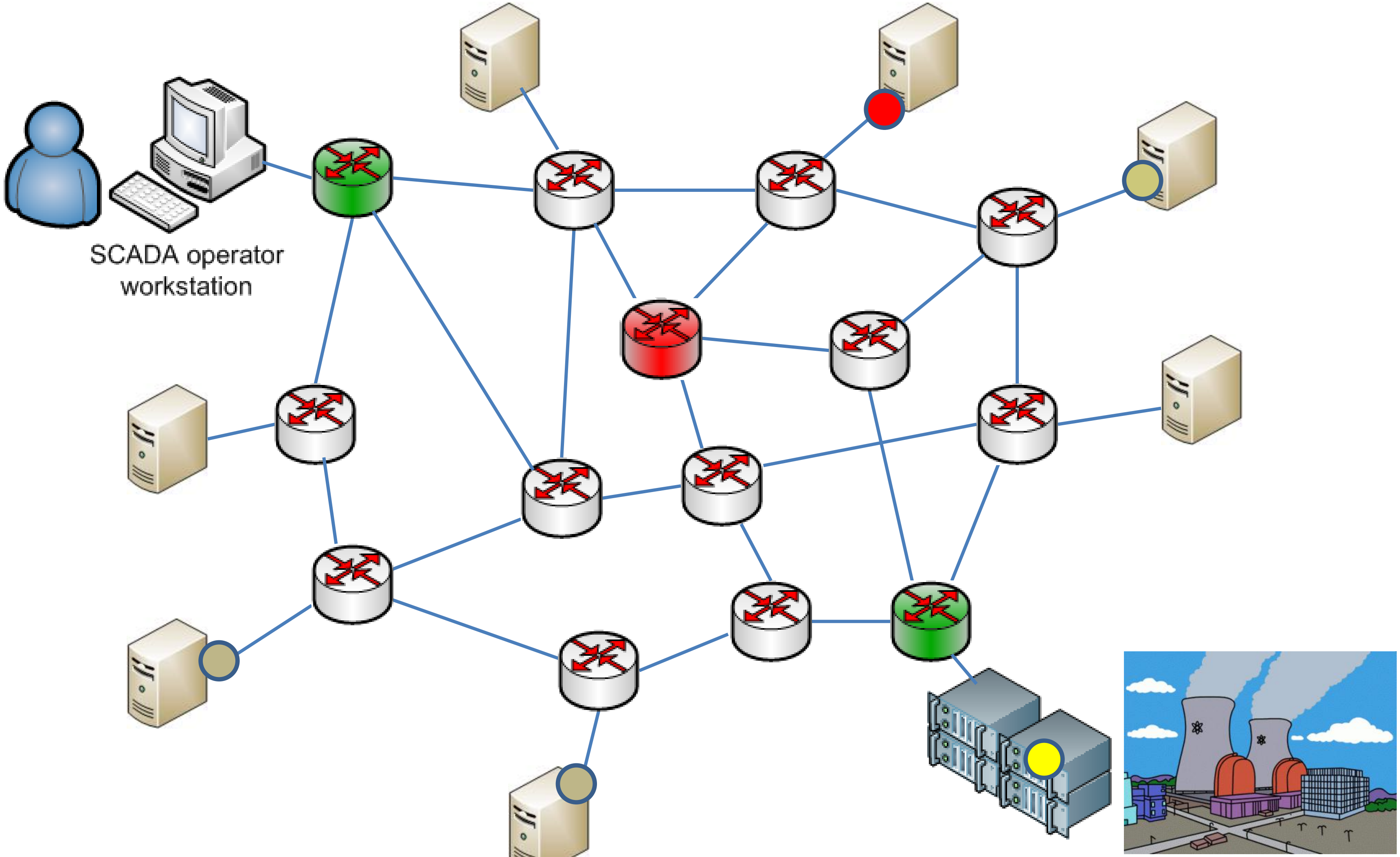
How Wide Area connections evolved: THEN...



...AND NOW


SCADA operator workstation
INTERNET
SCADA data concentrator
Critical Infrastructure

Routers are exposed



INSPIRE overview

- Two-year small or medium-scale focused research project (STREP)
- Work programme topic addressed:
  - Objective ICT-SEC-2007.1.7: Critical Infrastructure Protection (CIP)
- Start/End date:
  - 1/11/2008 to 31/1/2011
- Total cost / EC contribution:

  € 3,697,402 / € 2,400,000

INSPIRE Consortium

ACADEMY

- Consorzio Interuniversitario Nazionale per l’Informatica (Coordinator) (ITA)
- Technische Universität Darmstadt (GER)

INDUSTRY

- SELEX Sistemi Integrati (ITA)
- Thales Communications (FRA)
- ITTI (SME) (POL)
- S21sec Information Security labs (SME) (SPA)
- KITE Solutions (SME) (ITA)
- Centre for European Security Strategies (GER)

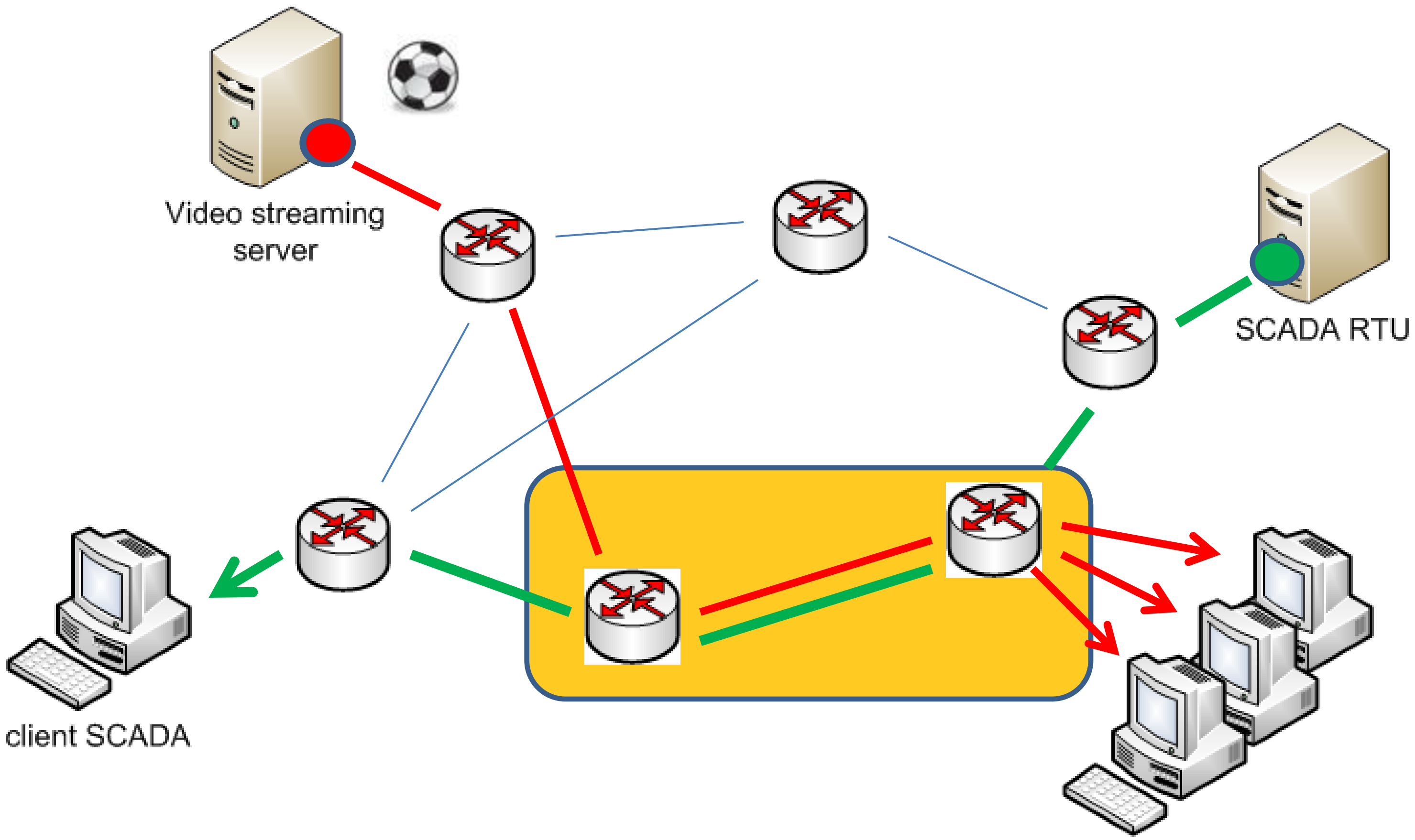
INSPIRE Objectives

- To analyse the dependencies of critical infrastructures from the underlying communication networks
- To develop diagnosis and recovery techniques for SCADA systems
- To exploit peer-to-peer overlay routing mechanisms to improve the resilience of SCADA systems
- To define a self-reconfigurable architecture for SCADA systems

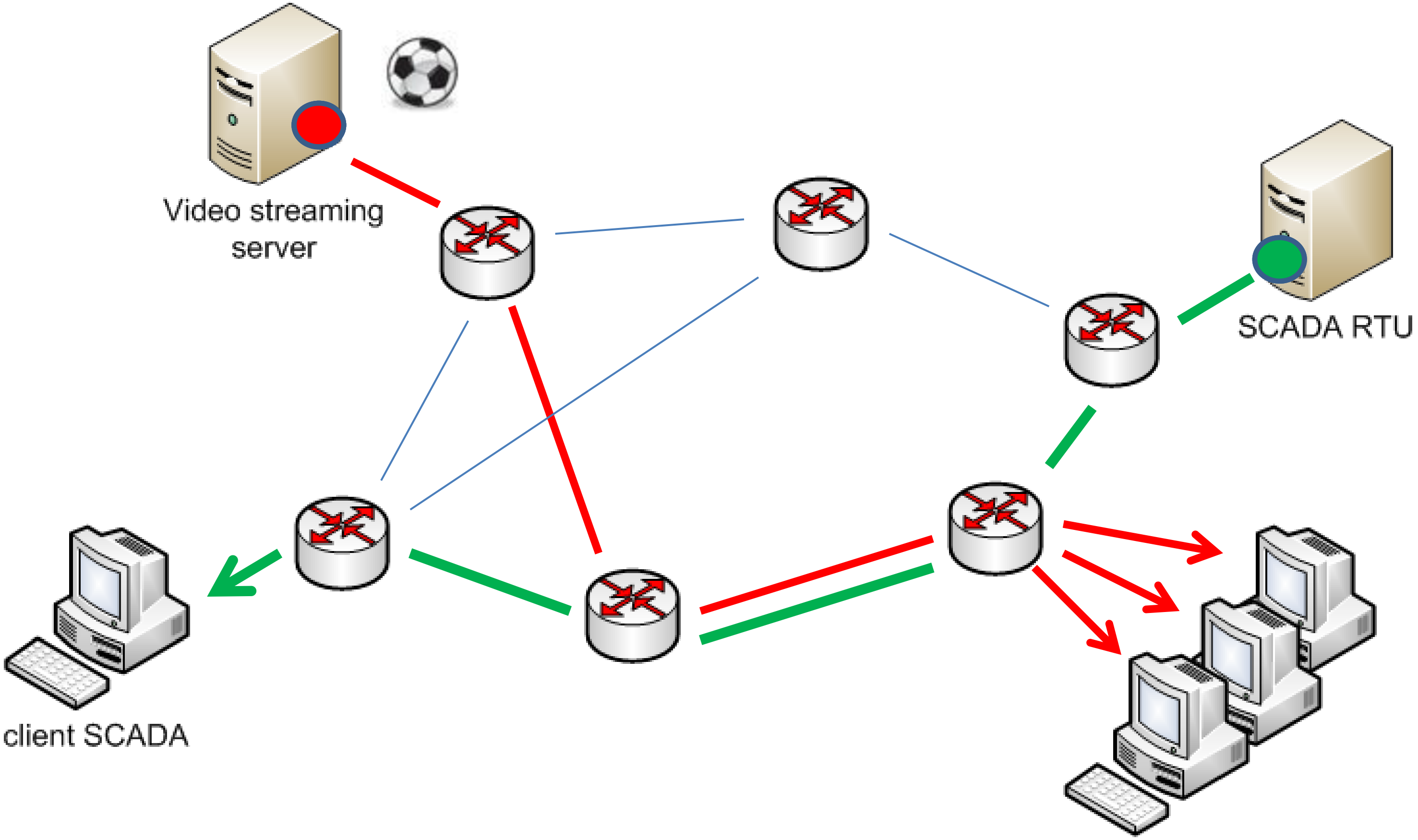
Main techniques investigated by INSPIRE

- Using MPLS protocol to defend SCADA traffic
  - – reroute to avoid congestion or DoS
  - – prioritize to avoid congestion or DoS
  - – split traffic to preserve confidentiality
- Using P2P networks to defend SCADA traffic
- Integrating a comprehensive Security assessment framework (from the vulnerability databases to patching and what-if’s)

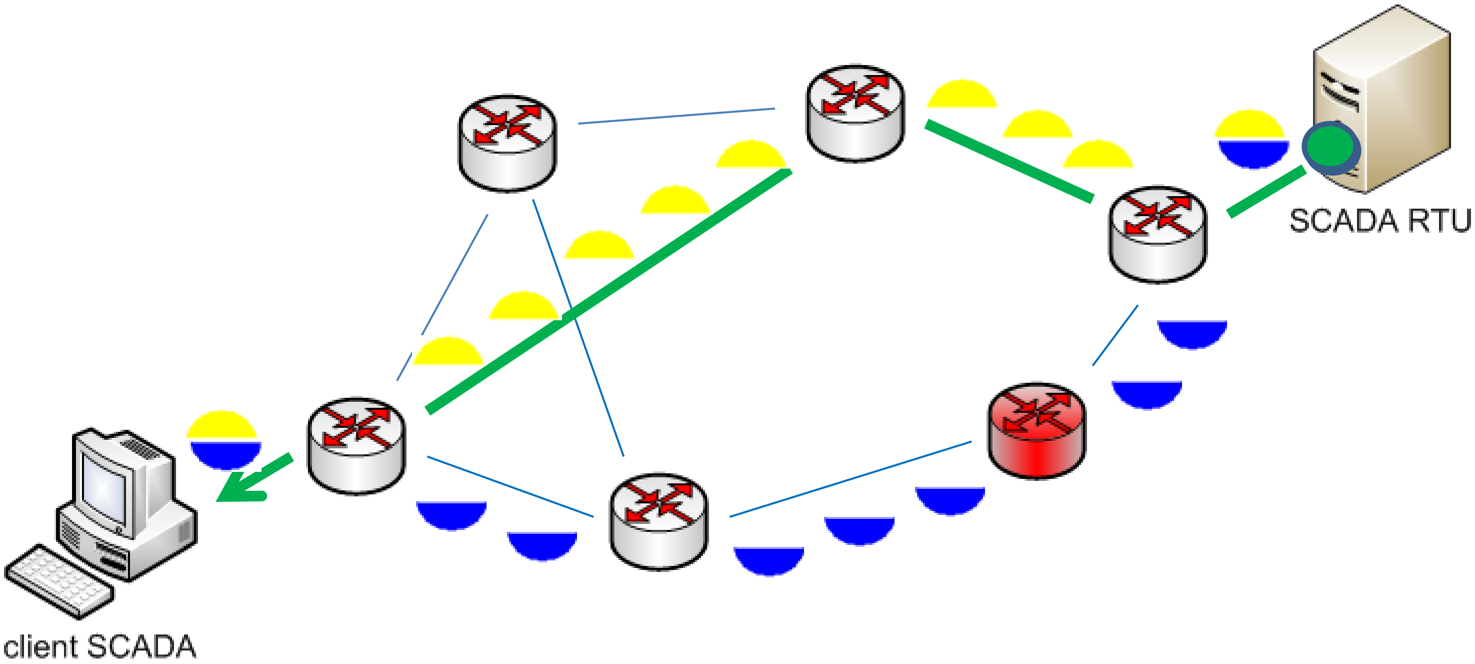
Using MPLS to prioritize



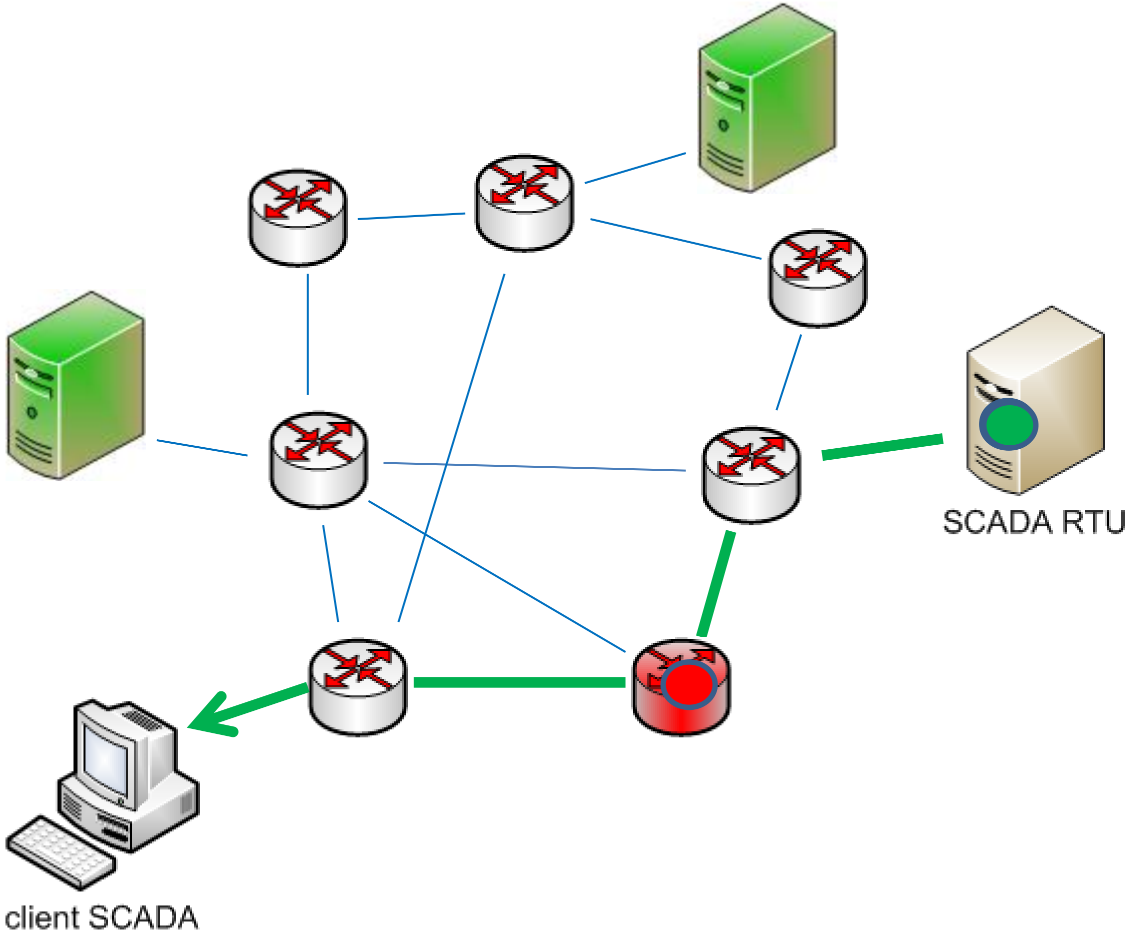
Using MPLS to reroute



Path splitting with MPLS



P2P-based protection



More info on INSPIRE

http://www.inspire-strep.eu
info@inspire-strep.eu

Project Coordinator:

Salvatore D’Antonio (CINI)

salvatore.dantonio@uniparthenope.it

For SELEX Sistemi Integrati:

Fabrizio Margaresi

fmargaresi@selex-si.com