

# “Piattaforme di telecontrollo capillare e sicuro per l’industrial Internet of Things”

*Cristian Sartori*

# SIEMENS

# Telecontrollo

## Scenario classico

- Raccolta e monitoring continuo di valori come livello di riempimento, pressione, temperatura ed altre variabili
- Grandi impianti con a disposizione logiche di automazione e allacciamento alla rete elettrica



# Telecontrollo

Driver per aumentare la competitività



Tempistiche sempre  
più veloci



Maggiore  
flessibilità



Maggiore  
efficienza

# Telecontrollo

## Esigenze - I

- Aumentare la capillarità dei punti di monitoring distribuiti sul territorio
- Problematiche legate all'infrastruttura / disponibilità della rete elettrica
- Facilità di utilizzo



# Telecontrollo

## Esigenze RTU

- Essere autonoma dal punto di vista energetico
  - Soluzione a batteria e/o pannello solare
  - Modalità risparmio energetico
- In grado di analizzare e implementare logiche di programmazione
- Inviare i dati alla centrale tramite protocolli standard
  - Connessione veloce alla rete mobile
  - Trasmissione dati sicura (VPN)





# Telecontrollo

Nuovi scenari: gestione acqua

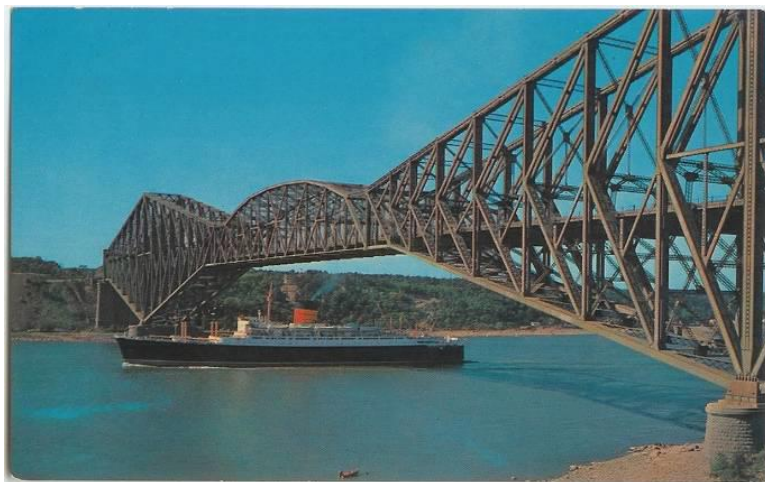
- Analisi distribuita sul territorio, aumentando la capillarità delle misure come:
  - Contabilizzazione portata (flusso)
  - Misurazione di pressione
  - Livello di serbatoi remoti



# Telecontrollo

Nuovi scenari: opere civili

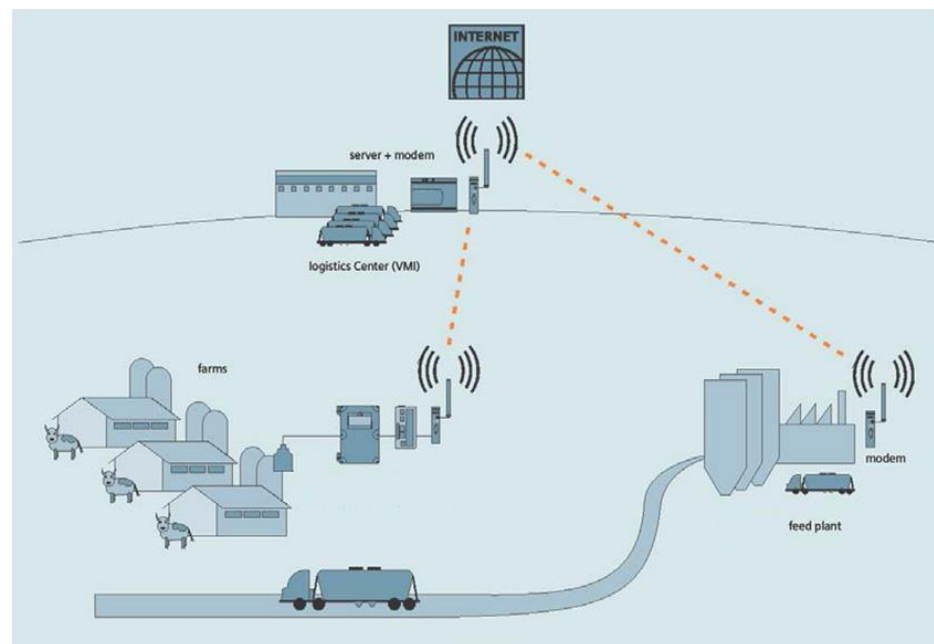
- Analisi di aree remote
  - Livello dei fiumi e torrenti
  - Livello altezza per le rotte marittime
  - Controllo slavine



# Telecontrollo

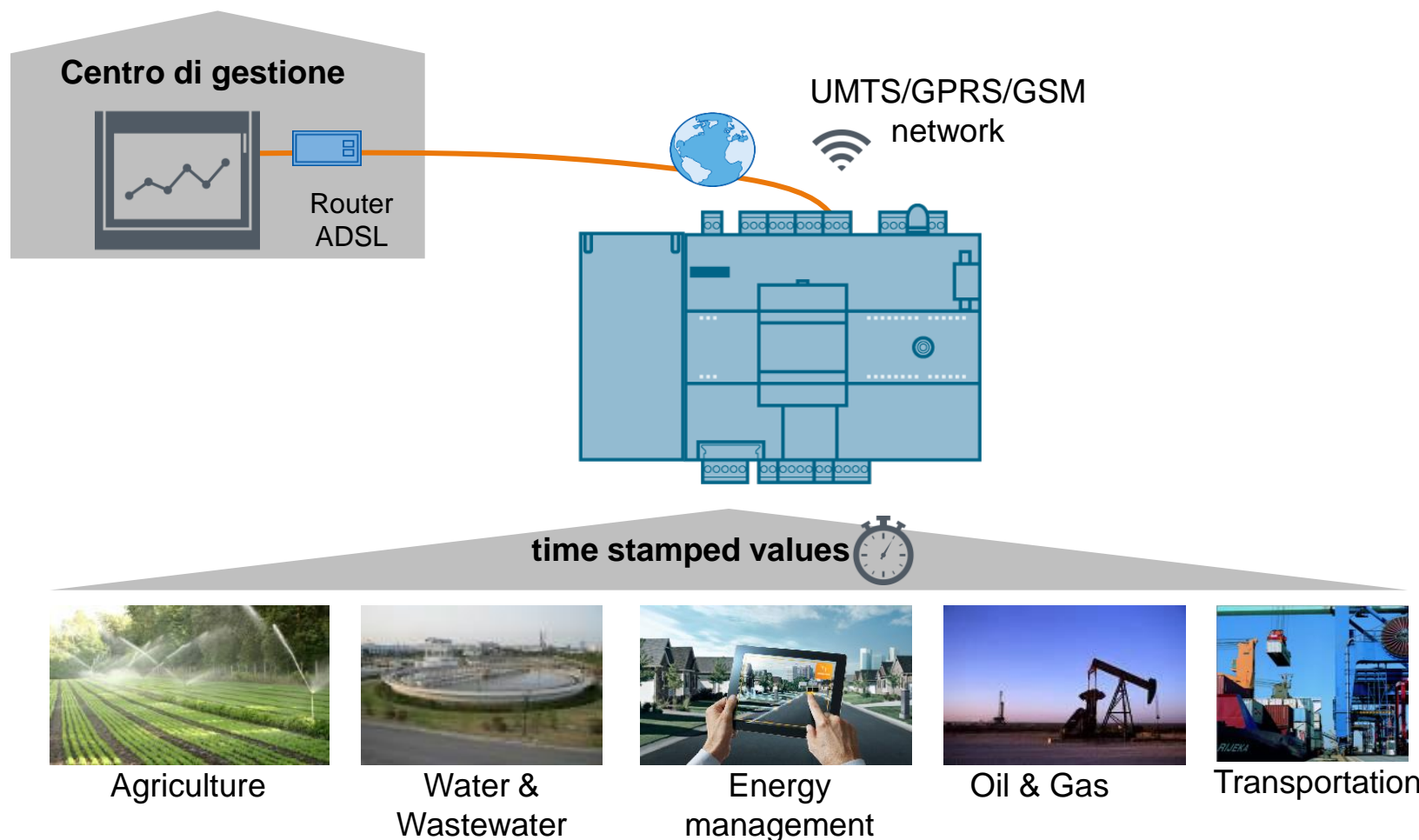
## Nuovi scenari: agricoltura

- Monitoring
  - Contabilizzazione e fatturazione sistemi di irrigazione
  - Livello dei silos
  - Vendor Management Inventory





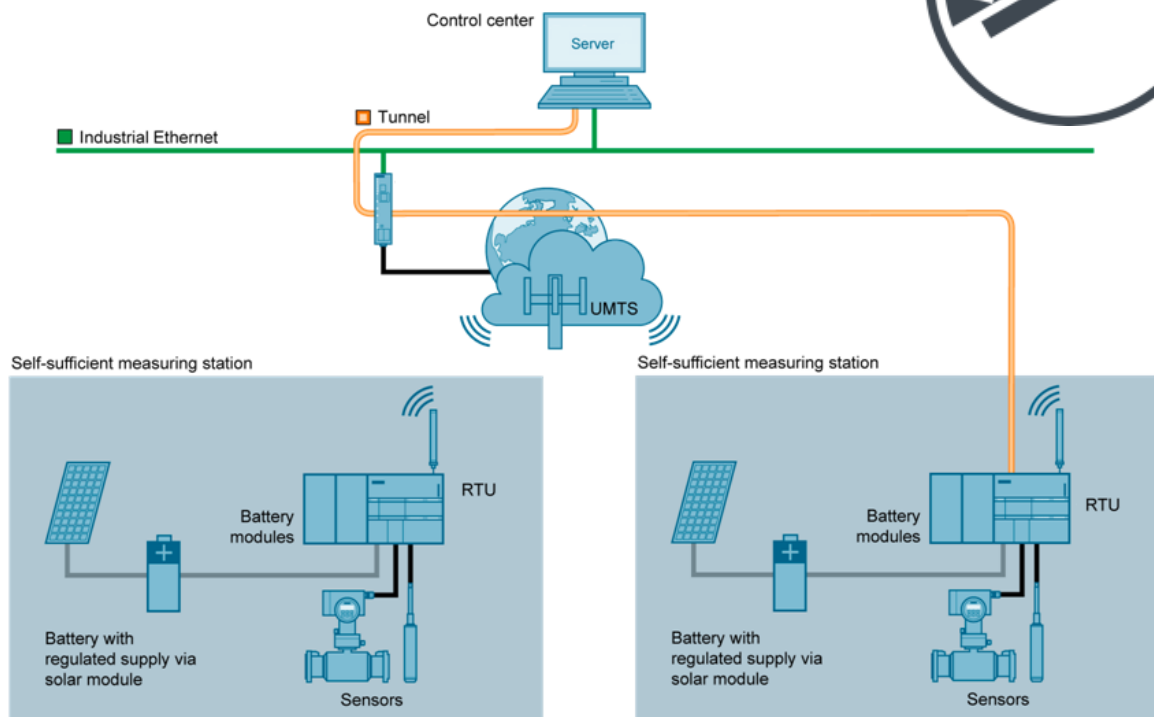
# Telecontrollo Architettura



# Telecontrollo

## Protocolli standard

- Per facilitare l'integrazione nei sistemi di telecontrolli è necessario adottare gli standard come:
  - IEC 60870-5-104
  - DNP3



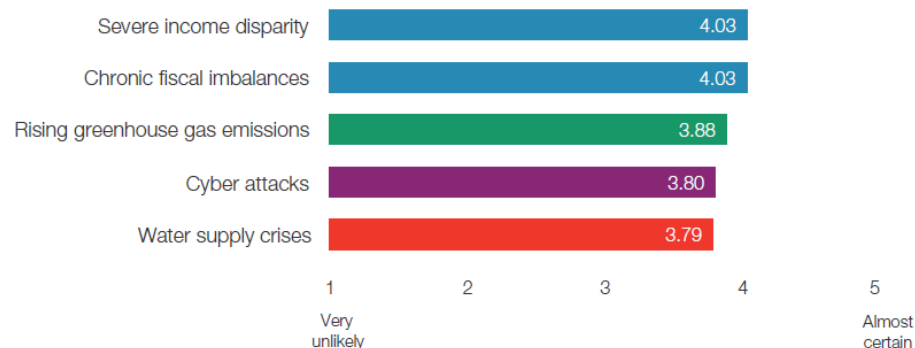
# Telecontrollo

## Cyber Security

### Trend che impattano la Security

- Incremento uso Smart Phone
- Approccio Cloud Computing
- Tecnologia Wireless
- Smart Grid
- IoT (Internet of Things)
- Industry 4.0
- **Teleassistenza per accesso ad aree remote**

### 5 rischi più probabili



Source: World Economic Forum 2014, 50 Global Risks

# Telecontrollo

Attacchi cibernetici sono una realtà anche per il telecontrollo

## Top 10 threats 2012

1. Unauthorized use of remote maintenance access
2. Online attacks via office/enterprise networks
3. Attacks against standard components used in the ICS network
4. (Distributed) denial-of-service ((D)DOS) attacks
5. Human error and sabotage
6. Introduction of harmful code via removable media and external hardware
7. Reading and writing messages in the ICS network
8. Unauthorized access to resources
9. Attacks on network components
10. Technical faults and acts of God

## Top 10 threats 2014

1. Infection with harmful software via the Internet and Intranet New
2. Introduction of harmful software via removable media and external hardware
3. Social engineering New
4. Human error and sabotage
5. Unauthorized use of remote maintenance access
6. Internet-connected control components New
7. Technical faults and acts of God
8. Compromised smartphones in the production environment New
9. Compromised Extranet and cloud components New
10. (Distributed) denial-of-service ((D)DOS) attacks

Source: BSI analysis on cyber security 2012

Source: BSI analysis on cyber security 2014

# Telecontrollo

Trasmissione dati tramite VPN

