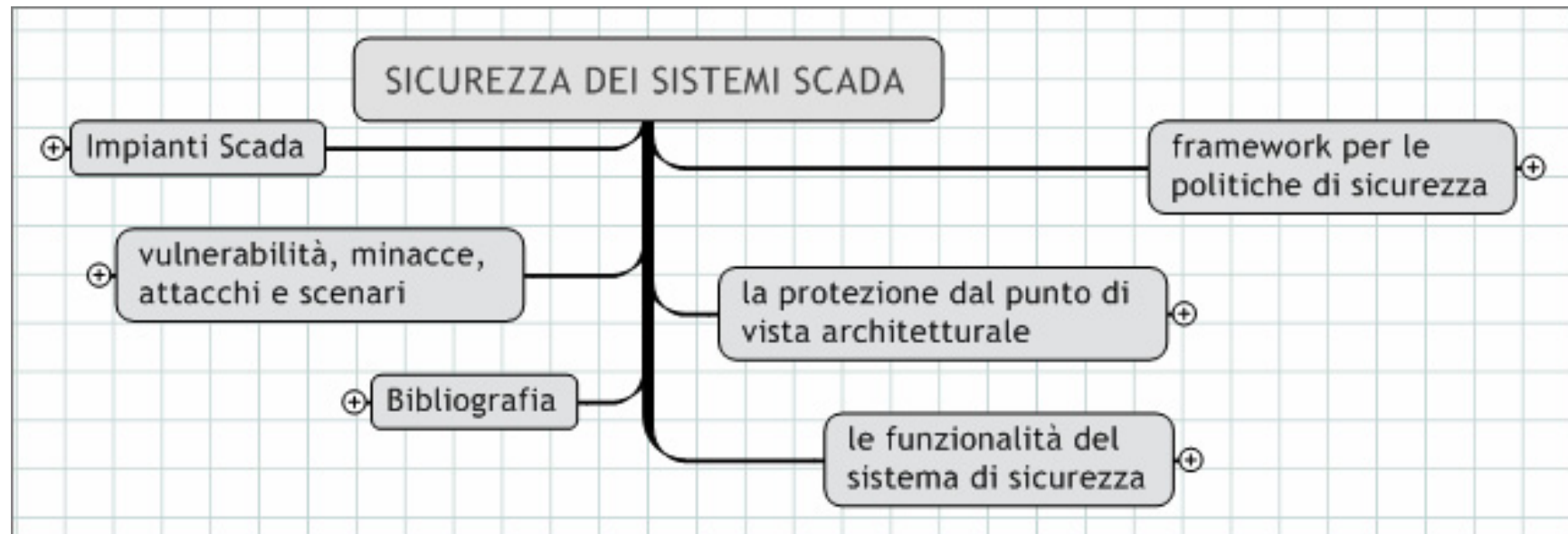


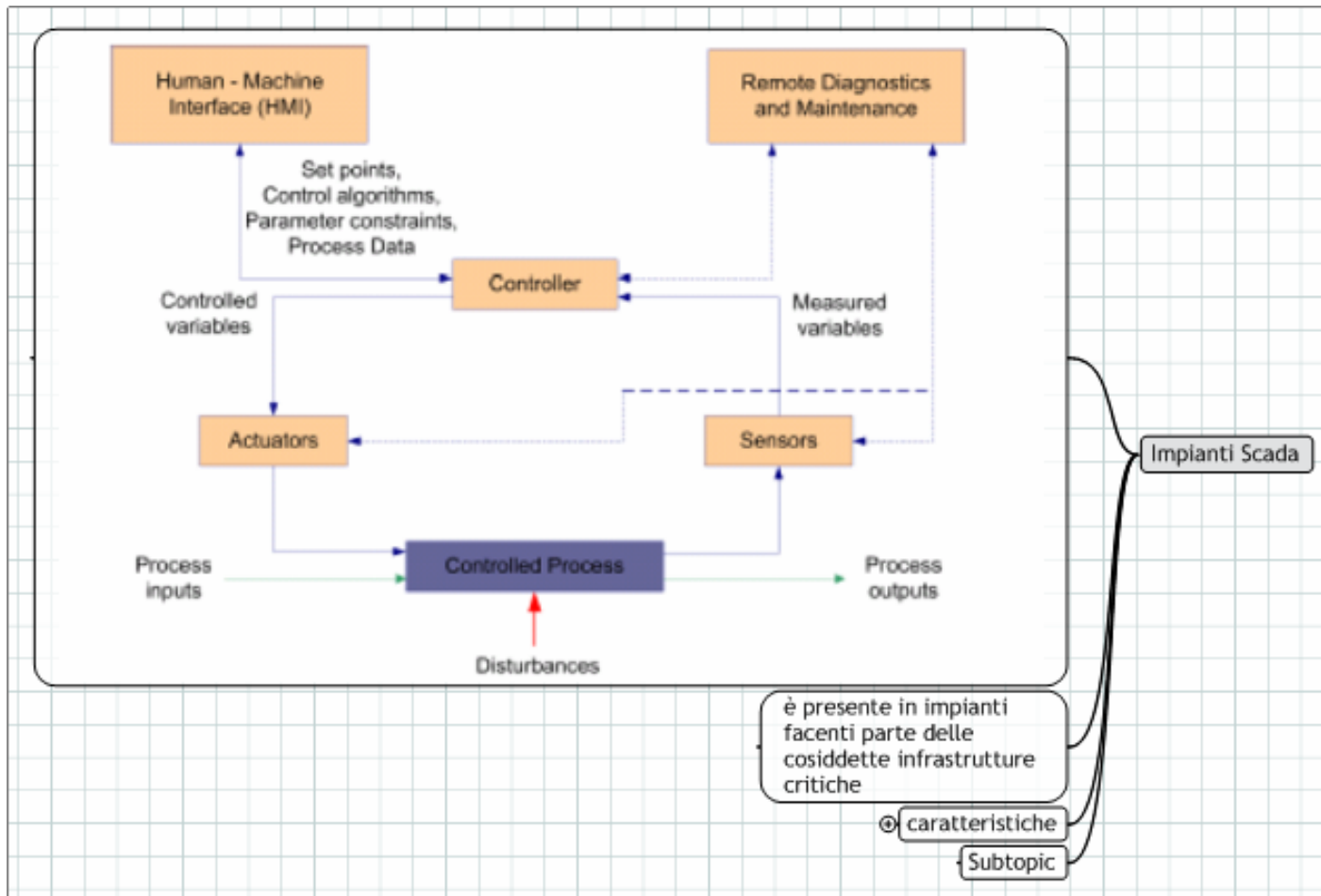
SICUREZZA DEI SISTEMI SCADA

Bozza per Dibattito

SICUREZZA DEI SISTEMI SCADA



Impianti Scada



Definizione

System

Control

And

Data

Acquisition

controllo industriale di
attrezzature di diverso tipo

registrazione dei relativi dati

Ambiti d'uso

Controllo del traffico

- Aereo
- Ferroviario
- Automobilistico



Controllo della gestione dei sistemi di trasporto dei fluidi

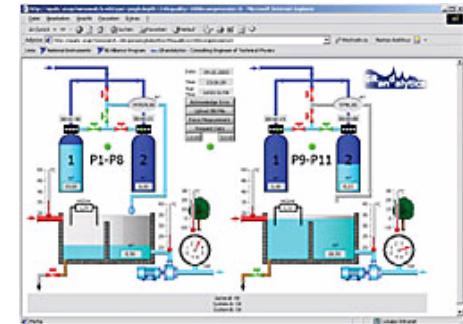
- Acquedotti
- Gasdotti
- Oleodotti



Controllo della distribuzione dell'energia
Reti di trasmissione dell'energia elettrica



Controllo della gestione delle linee di produzione
Processi industriali



Telerilevamento ambientale

Piattaforme

In passato:

- DOS
- VMS
- UNIX

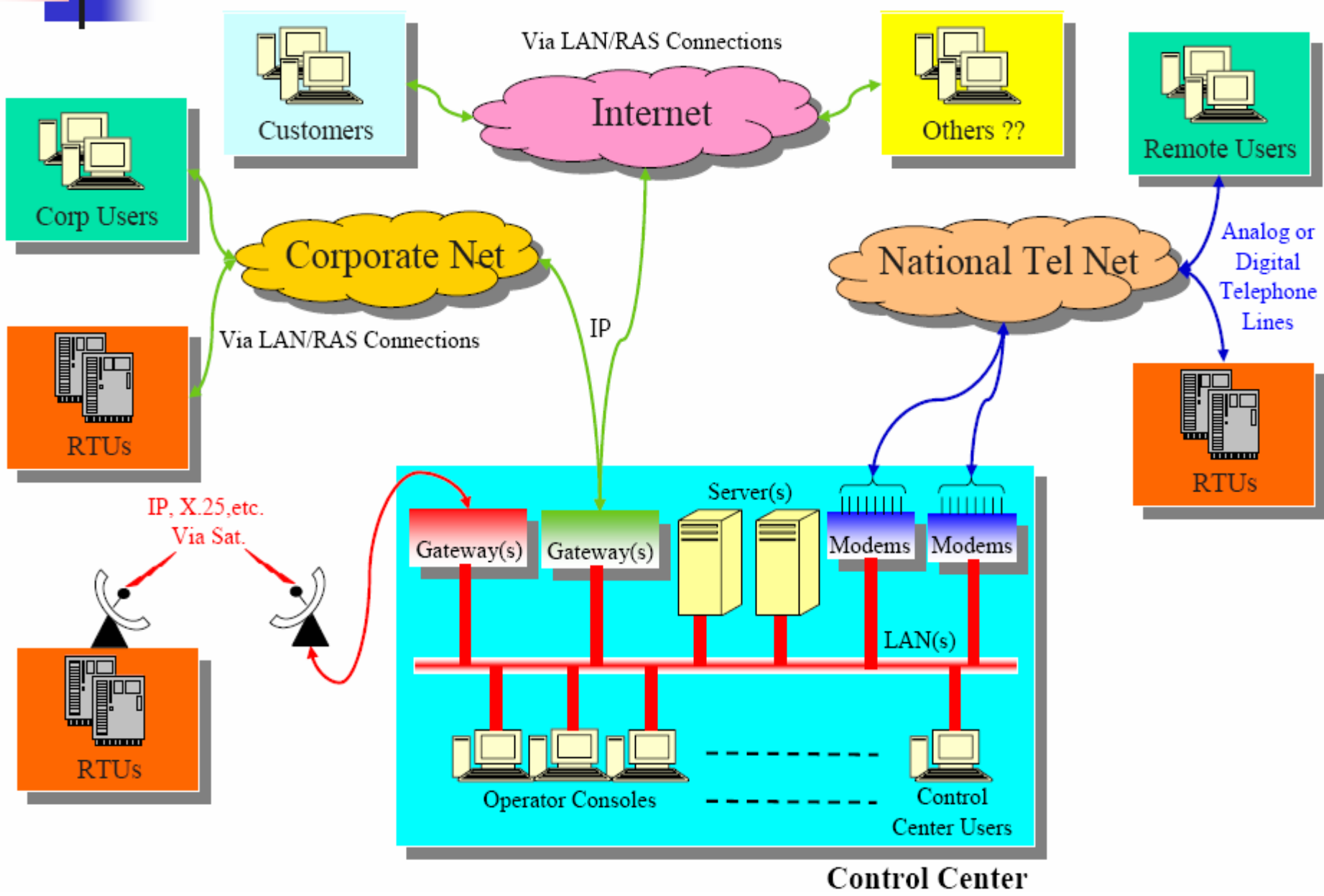
Più recentemente:

- MS Windows (NT e 2k)
- Linux

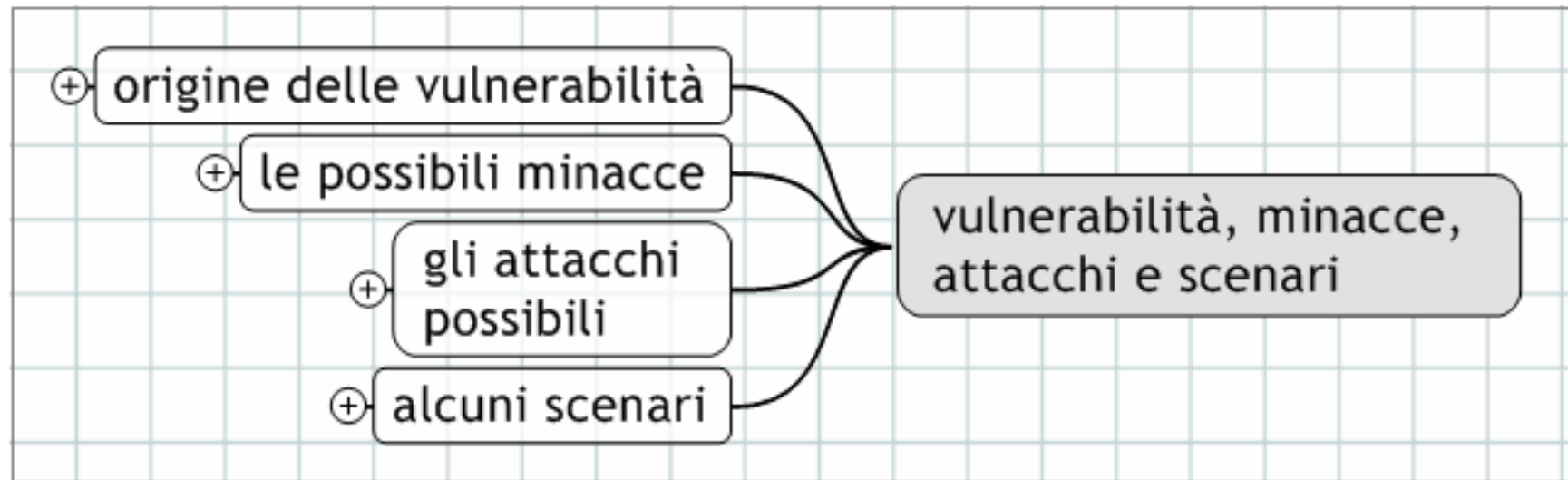
- Web technology, ActiveX, Java, etc

Caratteristiche

- complessità elevata
- forti interdipendenze
- costi elevati
- Sistemi legacy difficilmente rimpiazzabili
- Recente introduzione di tecnologie IP based
- Accesso remoto da siti distanti



vulnerabilità, minacce, attacchi e scenari



Origine delle vulnerabilità

- Connessioni con altri sistemi
- Accesso remoto
- Sicurezza fisica
- Protezione anti-virus
- Controllo degli Accessi
- Account e password
- Patch di sicurezza
- Monitoraggio dei sistemi
- Resilienza e continuità
- Codice prodotto da terze parti

Le possibili minacce

- Hackers
- Attacchi interni
- Criminalità
- Illegal information brokers
- Disgruntled staff
- Staff undertaking unauthorised actions (e.g. accessing the Internet)
- Corporate intelligence
- Contractors
- Foreign intelligence services
- Organised crime
- Terrorists
- Protesters and activists (e.g. environmental, political, animal rights)

Gli attacchi possibili 1

- attacchi old school
 - password guessing
 - SQL injection
 - port scanning
 - SNMP MIB walking
 - FTP anonymous
 - SMB null sessions
 - telnet senza password
 - sistemi non aggiornati
 - sniffing
 - trojans e backdoors

Gli attacchi possibili 2

- complessi
 - Known-key attack where an adversary obtains some keys used previously and then uses this information to determine new keys.
 - Replay attack where an adversary records a communication session and replays the entire session, or portions thereof, at some later point in time.
 - An impersonation attack where an adversary assumes the identity of the legitimate entities.
 - An attack against passwords. Where typically: a password is stored in a computer file as the image of an unkeyed hash function; when a user logs on and enters the password, it is hashed and the image is compared to the stored value; or when an adversary can take a list of probable passwords, hash all the entries in this list, and then compare this to the list of true encrypted passwords with the hope of finding matches.
 - A forward search attack, similar in spirit to the password attack, which is used to decrypt messages.
 - Interleaving attack using some form of impersonation in an authenticated protocol.

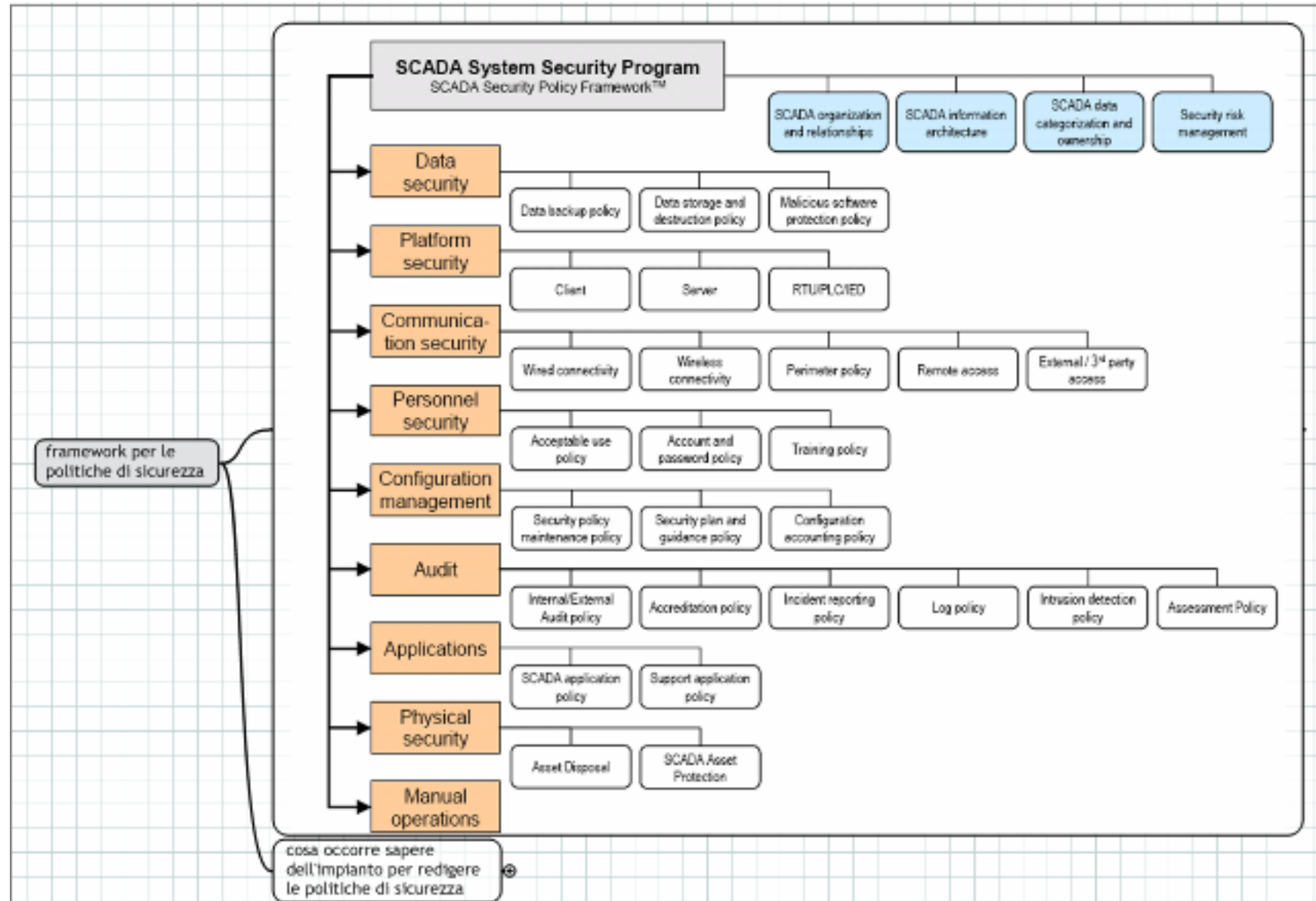
Alcuni scenari

- Systemic loss of all machines based on a particular operating systems (e.g. Windows, Unix, VMS etc.)
- Systemic loss of Ethernet/IP networking technologies
- Loss (or reduction) of functionality of process control systems
- Loss of connectivity between the process control systems and:
 - Corporate networks
 - Other systems (e.g. supply chain, laboratory systems or other companies)
 - Remote field devices
- Unauthorised change of setpoints or configuration by malicious or inadvertent actions
- Accidental change of system configuration by an authorised user
- Attack by disgruntled employee
- Loss of integrity or availability of historical data
- Loss of confidentiality of process and related information

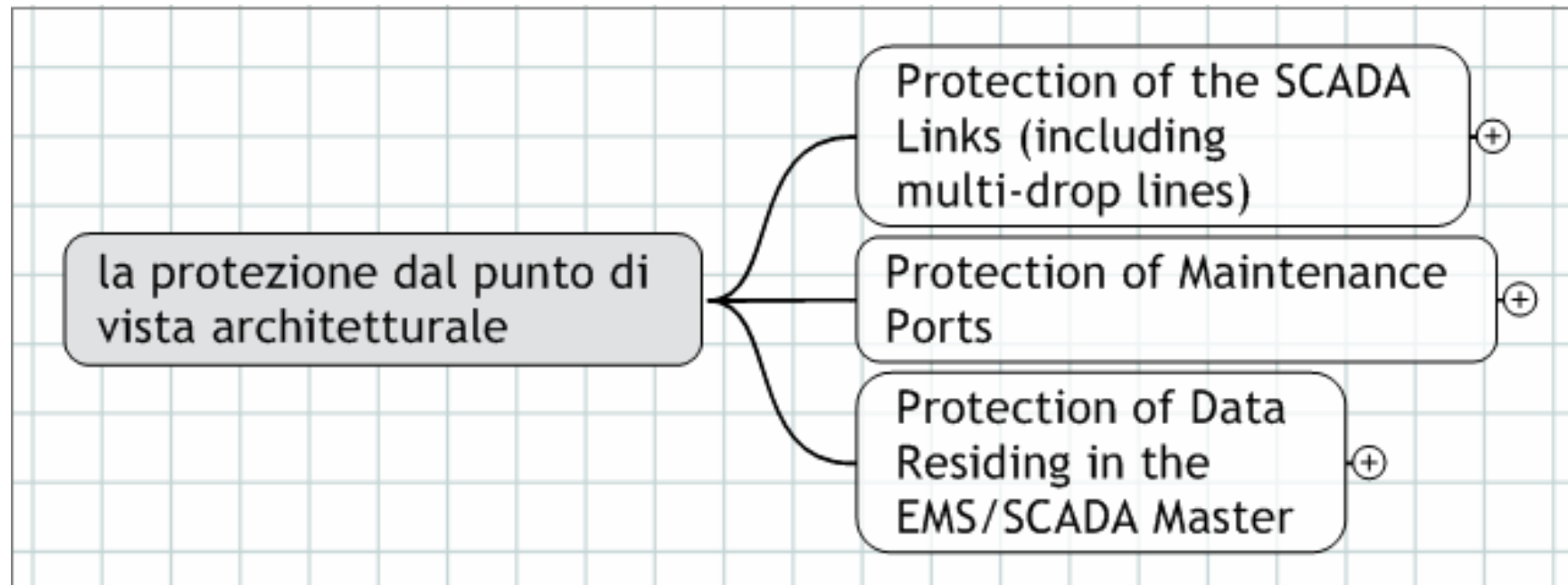
Cosa occorre sapere dell'impianto per redigere le politiche di sicurezza

- Quanti siti, sistemi e impianti correlati esistono?
- Quali e quanti sistemi risiedono su ogni sito?
- Come si collocano i singoli siti e sistemi nella catena del valore (value oppure supply chain)?
- Qual è la criticità in termini operativi e di business di ogni sito e sistema?
- What contributions do the systems make to process or personnel safety?
- What production and other operations are carried out by the site?
- Are there any Safety, Health and Environmental or regulatory implications?
- Are there any other regulatory requirements?
- Do the assets form part of the CNI (Critical National Infrastructure)? (For further information on what might constitute the CNI please consult www.nissc.gov.uk)
- Who is the single point of accountability (SPA) for each site, system and asset?
- Who are the key vendors and third parties relating to the systems?
- Who are the key support organisations at the site (IT, process control, off-site third party, on-site third party or in-house)?
- What are the site's critical system assets?
- What connections and data feeds are there to and from the control systems (include manual data feeds as well as electronic connections)?
- Are there any known issues with systems?
- What projects are underway or scheduled?
- What are the contact details for the local personnel and vendors?
- What are the dependencies relating to the site?
- Are there summary and detailed system and network diagrams?
- Is all documentation secure?

Framework per le politiche di sicurezza



La protezione dal punto di vista architettonurale



Protection of the SCADA Links (including multi-drop lines)

- 1. Provide cryptographic modules suitable for installation on existing communication lines and in substation environments.
- 2. Use cryptographic keys to provide secure login identification (ID) of the cryptographic modules. Once established, communications between the computer and the SCM shall be encrypted.
- 3. Use login IDs at each terminal to establish a cryptographic session for communicating SCADA messages.
 - Cryptographic algorithm shall be as transparent as possible to SCADA protocols, but the cryptographic modules installed at the master stations shall be able to determine destination addresses for mixed mode operation.
 - Algorithm shall not impose more than a 20% decrease in SCADA polling frequency.
 - Final selected algorithm shall meet the requirements of AGA Report 12.
- 4. Provide a means for mixed mode operation from the master station (with some RTUs equipped with SCMs on their communication ports and some with no SCM) on multi-drop lines.
- 5. The SCM shall provide an external alarm output if the device fails to function, if tampering is detected, or if its power supply is lost.
- 6. Retrofit of SCADA links shall require no software changes in either the master station or in the RTUs.

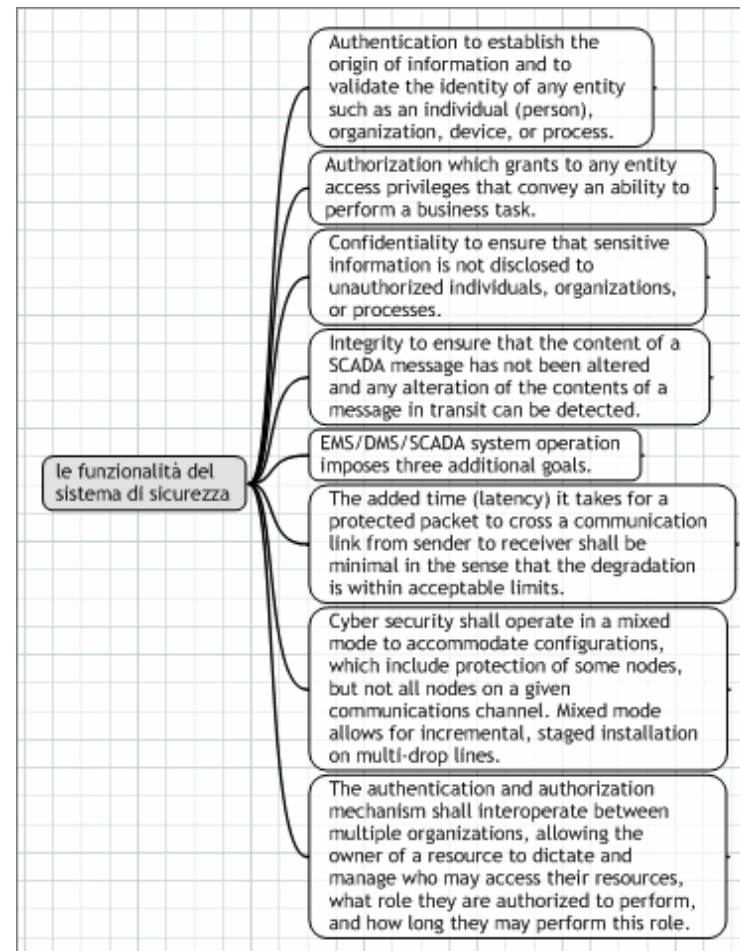
Protection of Maintenance Ports

- 1. Remote access shall be usable over dial-up connections from a computer (notebook or desktop) to an IED's maintenance port.
- 2. Access shall use two factor authentication; e.g., cryptographic authentication key (or Smart Card) in a Universal Serial Bus (USB) port and Personal Identification Number (PIN) to establish secure ID before allowing remote access from the computer to the maintenance port via an MCM.
- 3. Once communication is established between the computer and the MCM, messages shall be encrypted.
- 4. Once access is permitted, MCM shall allow use of existing passwords in the IED and require minimal changes in the computer's existing remote access software.
- 5. MCM shall terminate the access if the USB authentication key (or Smart Card) is removed.
- 6. MCM shall terminate the access if no activity is detected for a configurable period of time.
- 7. The MCM shall provide an external alarm output if the device fails to function, if tampering is detected, or if the power supply is lost.

Protection of Data Residing in the EMS/SCADA Master

- 1. External access to the SCADA database (access other than by the SCADA operator) shall be allowed only to authenticated users with access rights.
- 2. Authentication shall be two factor; e.g., cryptographic authentication key in a USB port (or SmartCard) and PIN.
- 3. Access rights shall include read only, write only, and read/write and shall include an expiration date/time.

Le funzionalità di un sistema di sicurezza per Scada



Bibliografia

