Cybersecurity Institute
Univ. Grenoble Alpes

Cybersecurity of industrial systems.
Cybersecurity guidelines

Stéphane Mocanu,

Laboratoire d'Informatique de Grenoble/INRIA

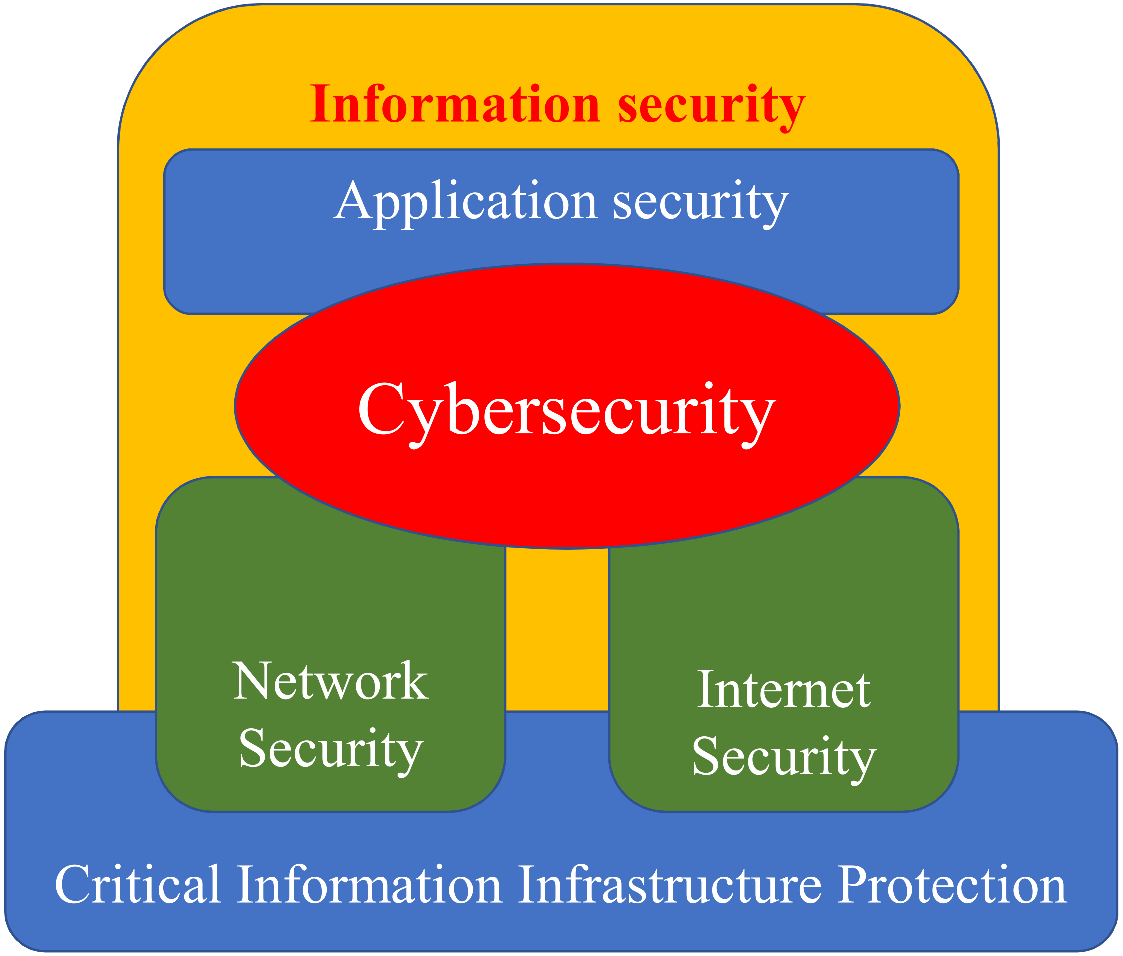
CTRL-A

stephane.mocanu@inria.fr

Some preliminary questions about cybersecurity

- What do you have to secure ?
    - Physical process, computers, networks, applications, data, people ?
- What do you mean by secure ?
    - Have to define a policy.
- Against which threats ?
    - There is no “absolute security”.
        - Vulnerabilities
        - Threat available resources
- What to do ? (choice of controls)
- How to do ? (security management)

General cybersecurity guidelines – ISO 27032



- CIIP : protection of critical industrial systems
- IS : General information security
- Application security : manage risk associated with application use (code, data, users)
- Network security : secure external and internal communication within organizations
- Internet security : protection of Internet-related services

Basic information security

- ISO 27000
- Information security : preservation of confidentiality ,integrity and availability of information CIA Triad
- In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved

- Resilience may also be of interest

CIA Triad

- Confidentiality: property that information is not made available or disclosed to unauthorized individuals, entities, or processes
  - Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information
- Integrity : property of accuracy and completeness
  - Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity
- Availability property of being accessible and usable on demand by an authorized entity
  - Ensuring timely and reliable access to and use of information.

- Proof :
- Authenticity property that an entity is what it claims to be
- Non-repudiation : ability to prove the occurrence of a claimed event or action and its originating entities
- Reliability property of consistent intended behavior and results

CIA Triad in use

Audit example for an asset using a 4 level scale (Low, Average, High, Very High)

Asset availability level	very high
Asset integrity level	average
Asset confidentiality level	very high
Asset proof level	low

What will you conclude ? Is the security level good enough ?

CIA Triad example continued

- The required CIAP level depends on the asset type.
- Example : a simple enterprise advertising web server (static web pages)

Availability = **Very High** ✓

A very high availability level is required to allow public access to the enterprise products presentation.

Integrity = **Very High** ✓

A very high integrity level is required. Data tampering with fake information published on the web server may damage enterprise image and business.

Web server

Confidentiality = **Low** ✓

Low confidentiality level is enough. All the data present on this server is public.

Proof = **Low** ✓

Low proof level is enough. No interactivity is available on the server pages (static web pages).

Security controls for CIA-P

Detailed description in NIST Special Publication 800-53

		D	I	C	P
Anti-virus	Allows to detect any virus already known by the security community	✓	✓	✓	
Cryptography	Allows the implementation information encryption and authentication		✓	✓	✓
Firewall	Equipment that allows networks zones confinement. It will authorize only specific network flows to cross between the zones.	✓		✓	
Access control	Allow privileged access (read/write/delete) to data only for authentified users.		✓	✓	✓
Physical security of equipements and rooms	Protects the physical integrity of assets.	✓	✓	✓	

Security controls continues

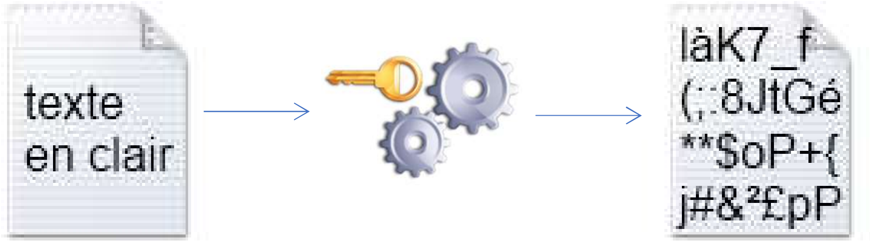
		D	I	C	P
Audit and Accountability	(i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; (ii) (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.	✓	✓	✓	✓
Awareness and Training	(i) ensure that managers and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures related to the security of organizational information systems; (ii) ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities	✓	✓	✓	✓

Cryptography basics

a. Definitions

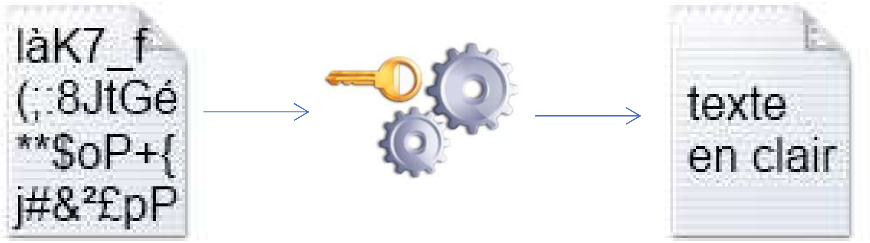
Encryption

Transform data such that it became unreadable. Only authorized entitiesmay read the ecrypted data.



decryption

Transform data previousy encrypted such that it became readable. Only authorized entities may decrypt data

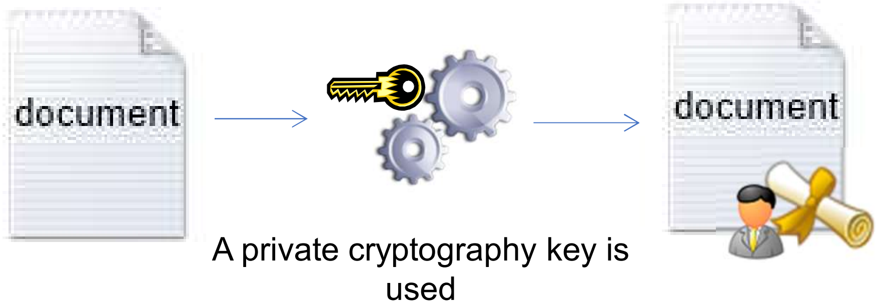


Cryptography basics

a. Definitions

Sign

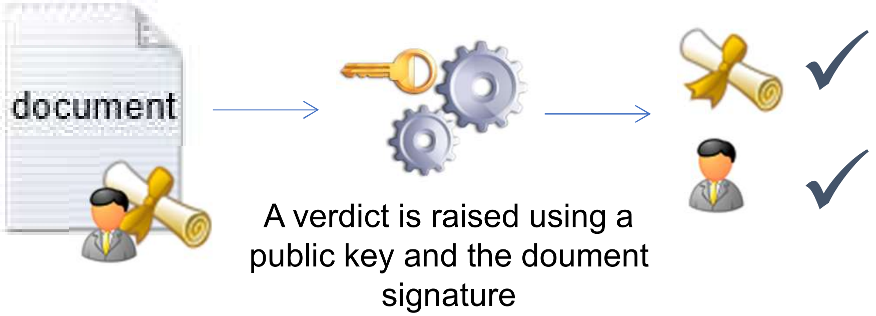
Create an electronic signature that uniquely identifyies data and sender.



A private cryptography key is used

Signature check

Checks that the data was not tampered and the sender is genuine.



A verdict is raised using a public key and the doument signature

Cryptography basics

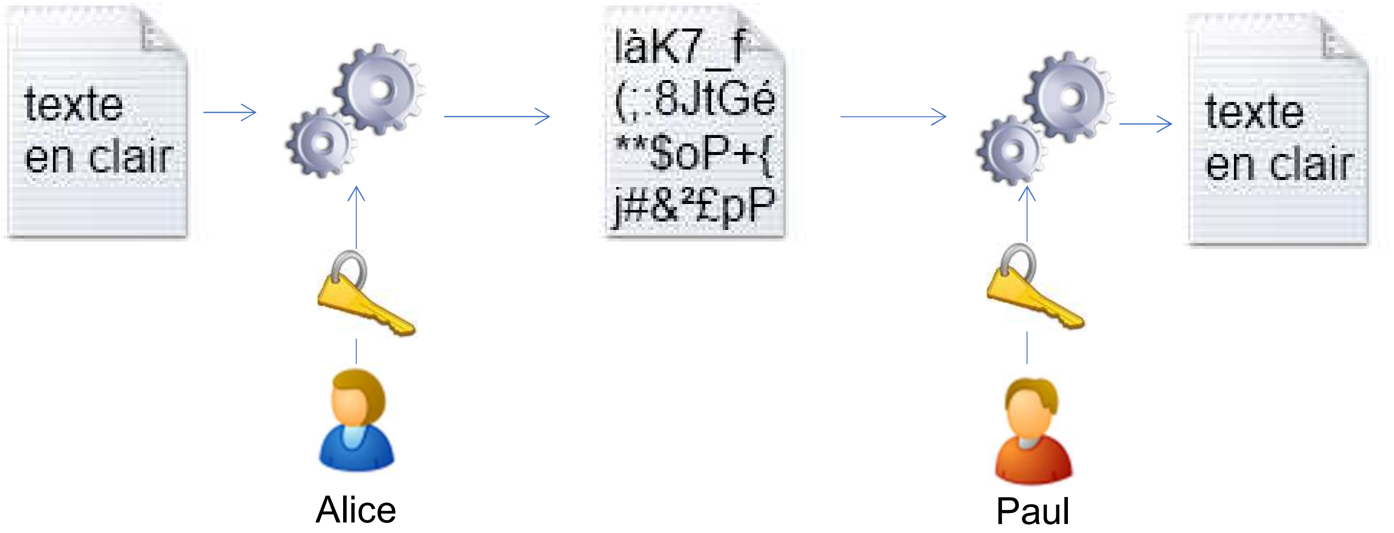
Symmetric encryption

- The same key is used to encrypt and decrypt the document
- The weak point is that key has to be kept secret !
- Faster than the asymmetric encryption

Cryptography basics

Symmetric encryption

- Alice wants to send a secure message to Paul



🔑 Shared secret key

Cryptography basics

Asymmetric encryption

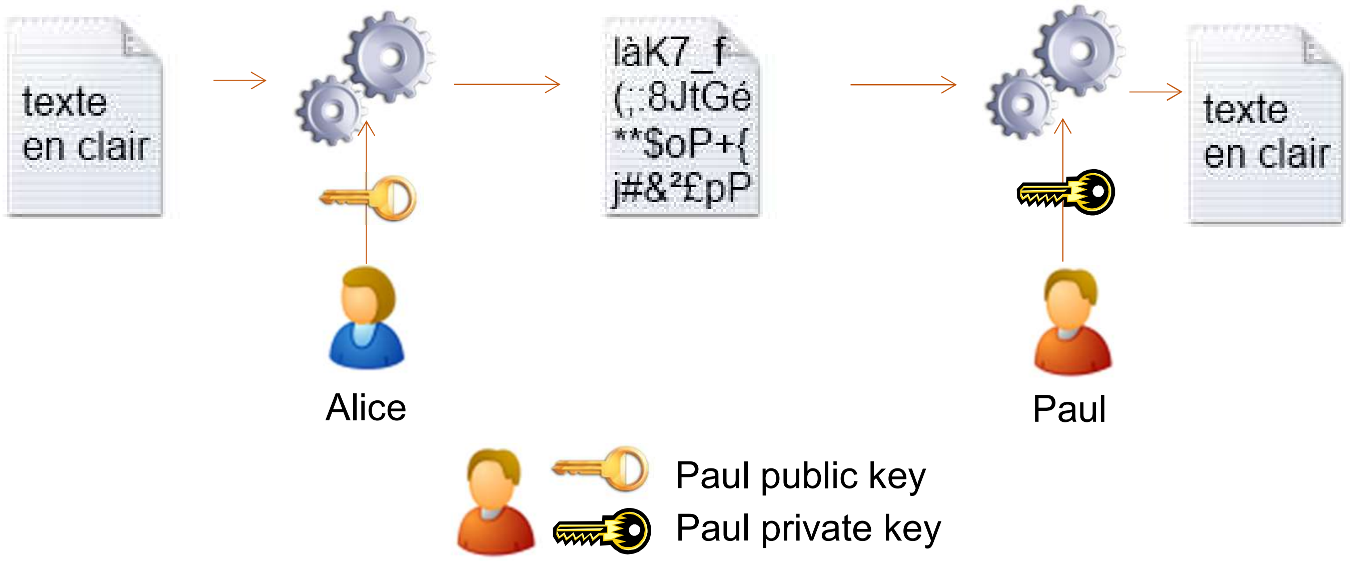
- Two dfiferent keys are used, one to encrypt the second one to decrypt:
  - Public key : anyone can obtain this key ;
  - Private key : only the owner has access, it has to be kept secret

- The two keys are mathematically related
  - Knowing the public key does not allow effective calculation of the private key
  - Each use owns two key : the private that must not be communicated and the public key which can be given to anyone.

3. Cryptography basics

Asymmetric encryption

- Alice wants to send an encrypted message to Paul
  - Alice encrypts the massage with Paul public key ;
  - Only Paul may decrypt the message using his private key;
  - Notes :
    - Alice never needs (and she cannot) use Paul’s private key !
    - Alice does not need to use her own keys in this example while she does not sign the message.



Cryptography basics

Symmetric vs asymmetric encryption

	Symmetric encryption	**Asymmetric encryption**
Advantages	• Faster • Short keys (512 bits are enough)	• Keys are ease exchanged. Ony public keys hve to be exchanged
Disadvantages	• Keys are difficult to be exchaged as secrecy has to be kept.	• Operations are long • Needs longer keys (at least 4096 bits) ;
Some well known algorithms	• AES.	• RSA.

3. Cryptography basics

f. Electronic signature

Insures that data was not tampered and the sender is genuine. If the signature is not valid that means that the sender identity is missused or the the data was modifyed

Note :

- **Electronic signature does not insure confidentiality**, but integrity and proof;
- **When one encrypts a message it is recommended to sign it also** in order to grant the sender identity

3. Cryptography basics

Electronic signature

1. A hash (fixed size code) is generated from the message.;
   - Hash computing algorithm are public. The hash is not a secret. ;
   - The chance to obtain the same hash from two different message is very small.
2. The signature algorithm uses the hash and the <u>private</u> key to generate the authentication key (the actual signature) ;
3. The sender will send the message and the signature ;
4. The receiver computes the hash;
5. The receiver checks the authenticity using the public key of the sender, the hash and the signature

Cryptography basics

Security certificates

An important issue is related to the autheticity of the keys themselves

Anyone can obtain the public key of everybody using key servers. How may one be sure **that « Public key of Paul » actually belongs to Paul** and it was not generated by someone who missused Paul identity ?

Another point : when visiting a web site (a bank) how can one be sure that the web site is genuine and not a fake ?

- Solution : security certificates.

Cryptography basics

Security certificates

A security certificate (digital certificate, public key certificate, identity certificate) is **a file** containing :

- The **Public key** of a person (corporate of web site) ;
- Identity details of the owner (name, address) . ;
- The **digital signature** of a trusted entity that issued the certificate.;
- Information related to the validity of the key, allowed usage etc.

The trusted entity will :

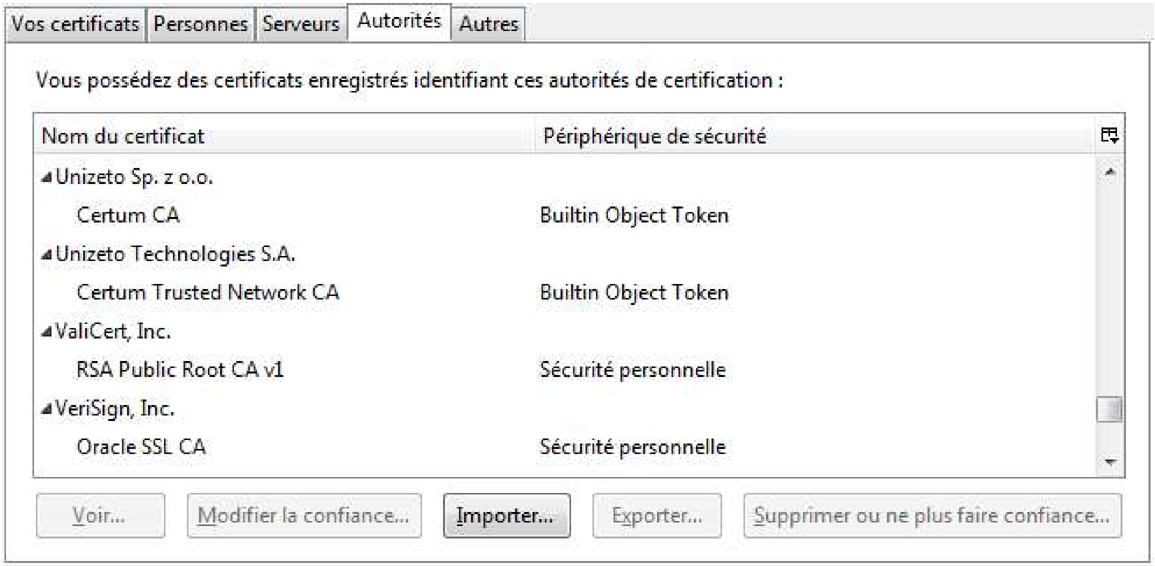
- **Check the identity** of the person asking for the certificate;
- **Creates the certificate** after verification, **and digitally signs it** (with the private key of the trusted entity) ;
- **Keeps up to date a list of certificates which were retired** (for example if the key was compromised).

Cryptography basics

Security certificates

How to recognize a trusted entity ?

- Directly integrated by the editors in the operating system and browsers;
- User may add new certificates if it chooses to trust them.



Vous possédez des certificats enregistrés identifiant ces autorités de certification :

Nom du certificat	Périphérique de sécurité
◢Unizeto Sp. z o.o.	
Certum CA	Builtin Object Token
◢Unizeto Technologies S.A.	
Certum Trusted Network CA	Builtin Object Token
◢ValiCert, Inc.	
RSA Public Root CA v1	Sécurité personnelle
◢VeriSign, Inc.	
Oracle SSL CA	Sécurité personnelle

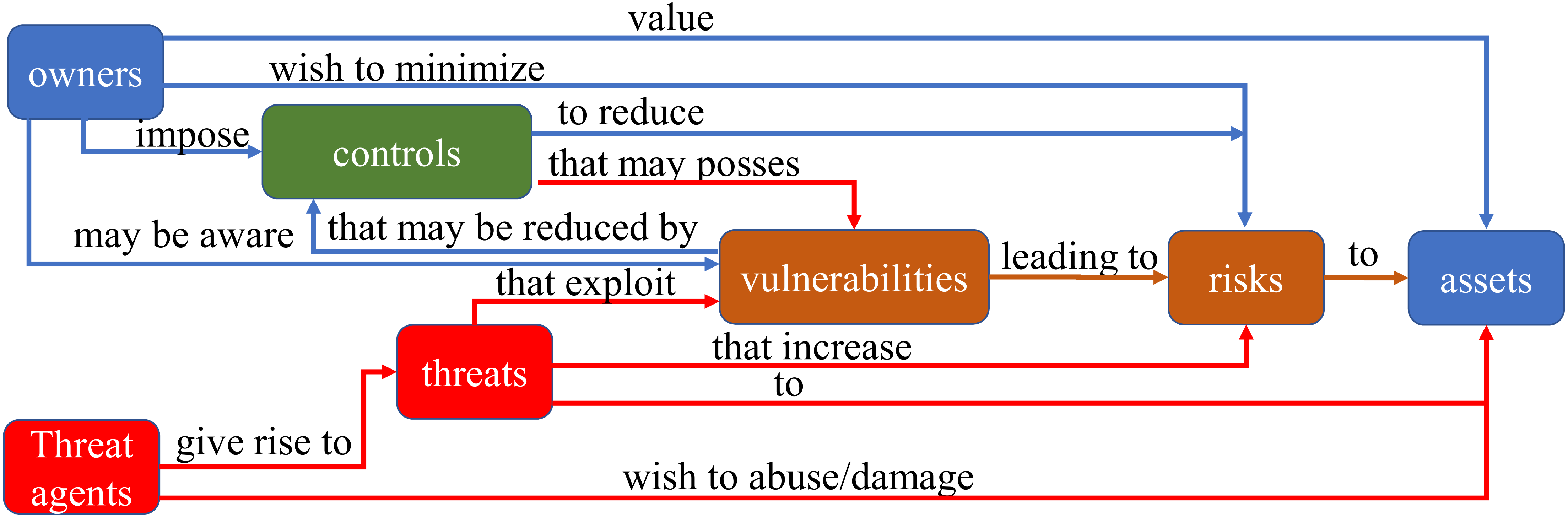
Image : magasin de certificats de Firefox

OpenPGP encryption exercise

- Install a pgp encryption suite. For windows : https://www.gpg4win.org/download.html
- I’ll send you a SIGNED message including my PGP public key
- Save the three documents : message, PGP signature, my public key
- Start Kleopatra and import my public key
- Use Kleopatra (with my key to check the signature) and SAVE the audit log
- Create a new pair of keys for your mail address
- Send me the audit log encrypted for me (i.e. with my public key) signed by you AND your public key
- You’ll received and encrypted answer from me (and you’ll have to decrypt)

Cybersecurity guidelines

General model



Threats will exploit vulnerabilities leading to risks for the assets

Stakeholders deploy countermeasures to control vulnerabilities and reduce risks

Some residual vulnerabilities may remain. A continuous management process is needed

Simplistic cybersecurity management

- Identify risks
- Identify vulnerabilities
- Find adequate controls and deploy
- Evaluate residual vulnerabilities
- Set-up a monitoring and correction process

But:

- Risks depends on threat complexity and skills
- Are you concerned by third party risks ?
- Control effect depends on resources/time/price/maintenance
- Some vulnerabilities may be hidden (0-day)
- Some vulnerabilities cannot be corrected (communication protocols)

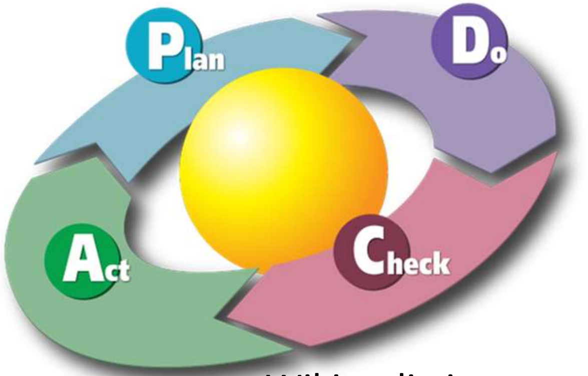
Real cybersecurity management

- Understand the organization
    - stakeholders
    - environment (social, cultural, political, legal, regulatory …)
    - contractual relationships
    - governance, structure, vision, mission, values
    - information systems and flows
    - interdependencies.
- Understand need and expectations of interested parties
    - Includes legal and regulatory requirement
- Determine the scope of the Information Security Management Systems (ISMS)
- Establish, Implement, Maintain an Improve ISMS
    - Leadership
    - Planning
    - Support
    - Operation
    - Performance evaluation
    - Improvement

Leadership (cybersecurity management)

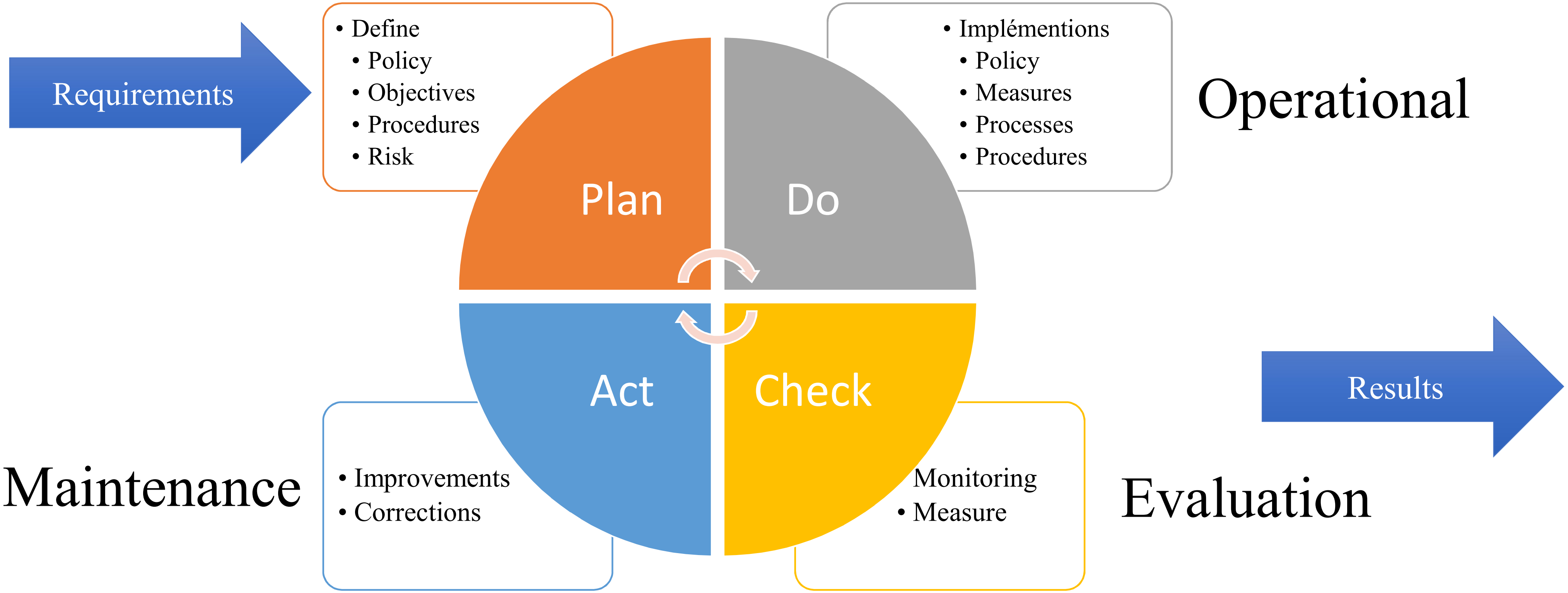
- Top management shall ensure that
  - Security policy and objectives are established an conform to the global strategy
  - ISMS is part of organization processes
  - Needed resources are available
  - ISMS achieves intended outcomes
  - Communication on the importance of effective ISMS is achieved
  - Continual improvement is promoted
  - Direction and support to persons contributing to ISMS is insured
- Top management establish information security policy
  - Appropriate to the purpose of the organization
  - Includes information security objectives
  - Includes a commitment to satisfy applicable requirements
  - Includes a commitment to continuous improvement
  - Documented
  - Available to interested parties (stakeholders)

Continual improvement process : Denning wheel (PDCA)



Wikipedia image

Strategy



Requirements

- Define
  - Policy
  - Objectives
  - Procedures
  - Risk

Operational

- Implémentions
  - Policy
  - Measures
  - Processes
  - Procedures

Plan

Do

Act

Check

Maintenance

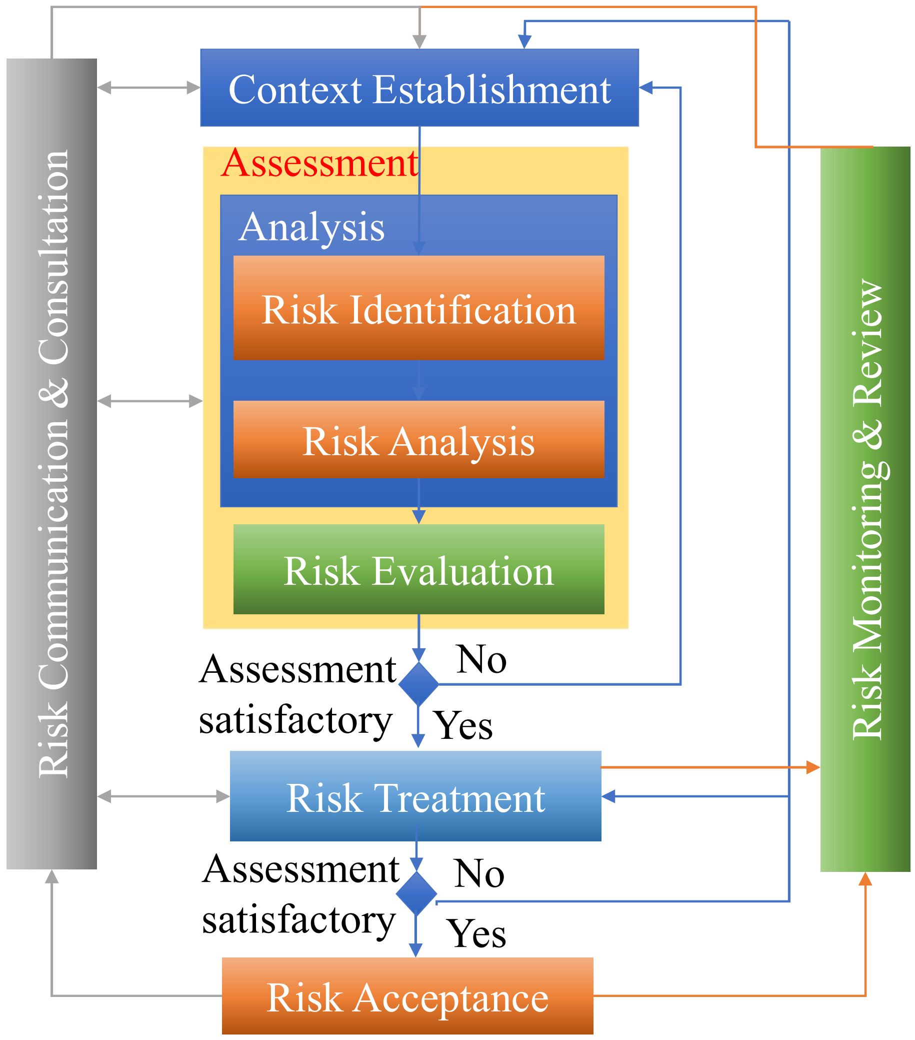
- Improvements
- Corrections

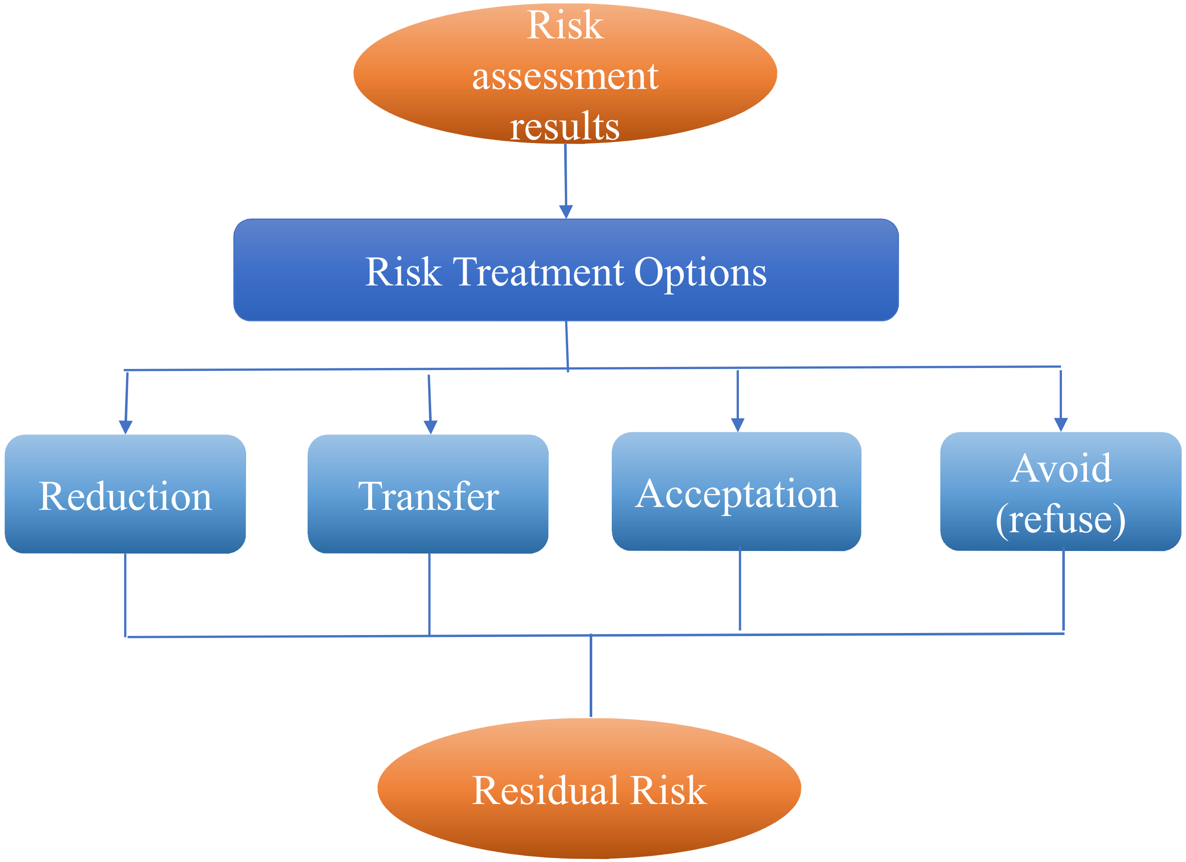
Monitoring
- Measure

Evaluation

Results

Risk Management (ISO 31010)



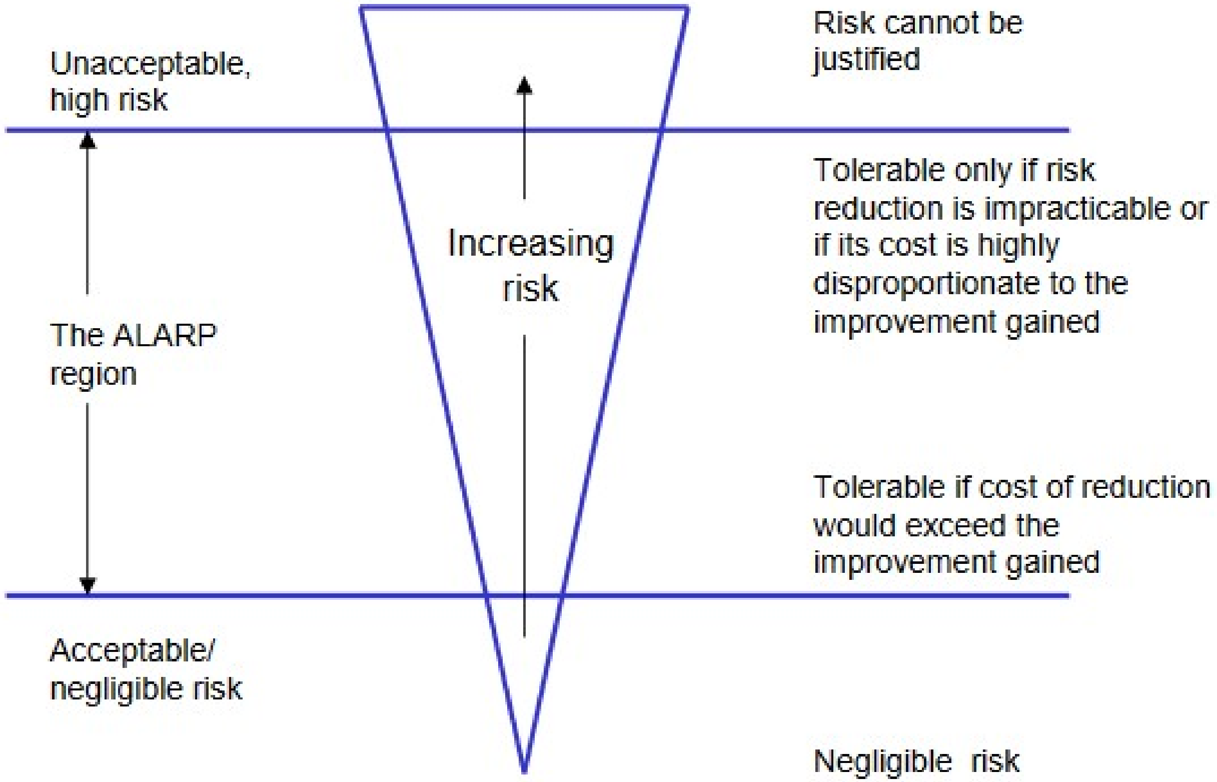


Preliminary risk assessment

- Plan
    - Risk assessment
        - Risk acceptance criteria
        - Identify information security risks and owner
        - Analyse information security risk
            - Asses potential consequences
            - Asses realistic likelihood
            - Determine the level of risk
        - Evaluate the information security risk
            - Compare the evaluation results with with risk acceptance criteria
            - Prioritize risks for treatement
        - Document
        - Select information security risk treatment options
        - Determine the necessary controls
        - Produce a Statement of Applicability (if ISO 27000 compliant)

Risk acceptance criteria

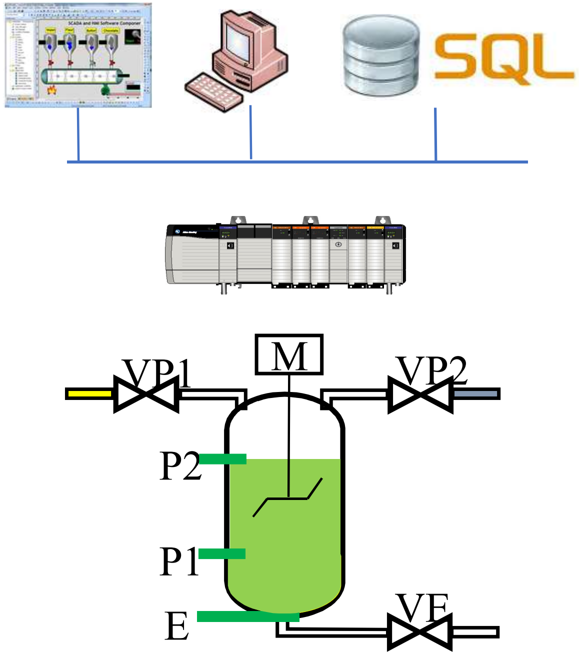
- ALARP (As Low As Reasonable Practicable) – cost/benefit analysis



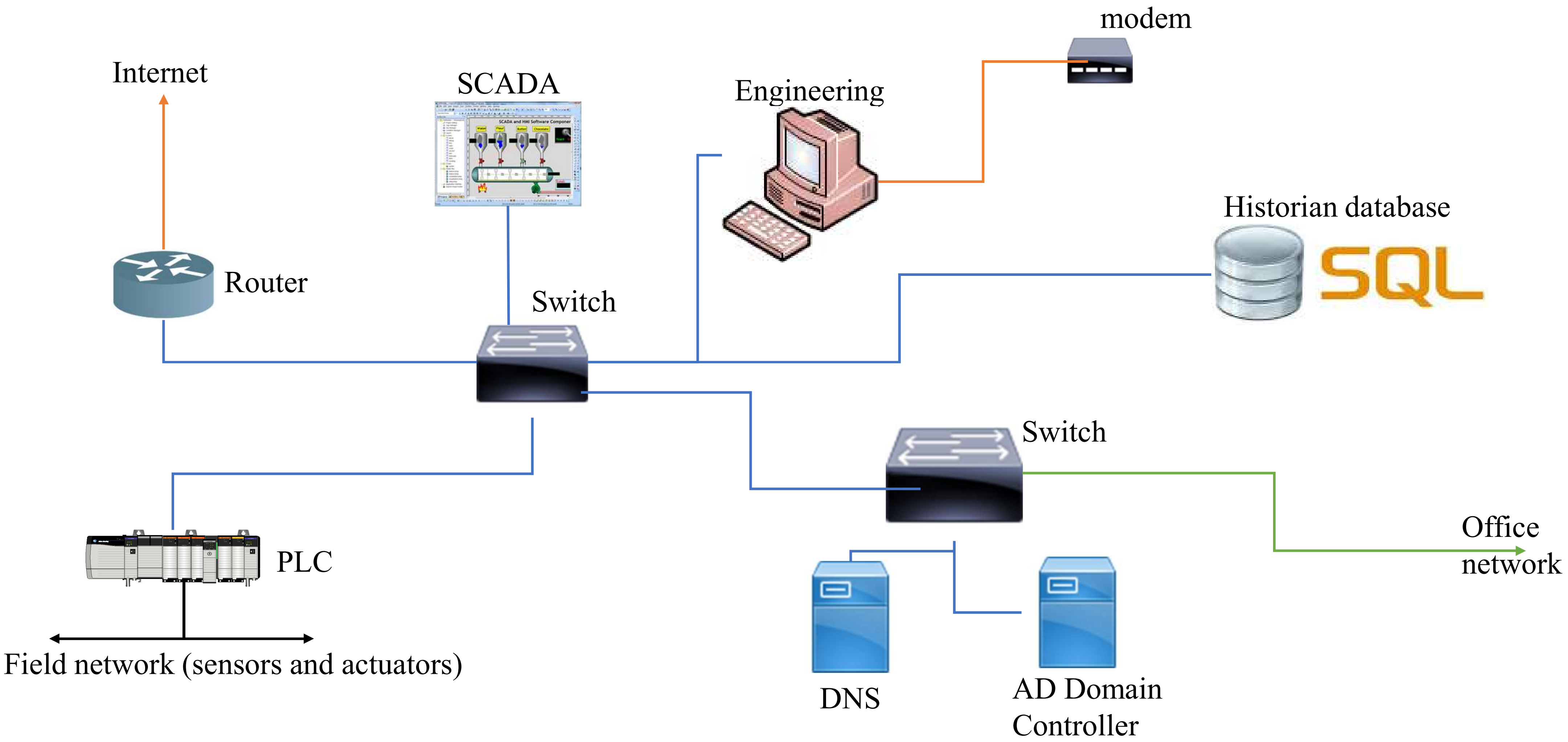
Unacceptable, high risk
Risk cannot be justified
Increasing risk
The ALARP region
Tolerable only if risk reduction is impracticable or if its cost is highly disproportionate to the improvement gained
Tolerable if cost of reduction would exceed the improvement gained
Acceptable/ negligible risk
Negligible risk

Chemical plant example

- Simple plant (chemical product mixer)
- Controller : PLC connected to a local LAN
- Internet connected SCADA
- Internet connected SQL historian
- Local or remote maintenance



Network infrastructure



Risk identification examples

- Need to identify risk sources, events, their causes and their potential consequences
- Event-based approach

Event	Threat	Vulnerability	Consequence	Owner
disruption of PLC program	Internal threat	Weak PLC Access control	potential chemical pollution	IT
	Program fault	No program testing	potential chemical pollution	Maintenance

- Asset-based approach

Asset	Threat	Vulnerability	Consequence	Owner
PLC	Data tampering	Internet accessible	potential chemical pollution	IT
SCADA	Impersonation	Weak password	potential chemical pollution	IT, Operations
Engineering computer	Malware	Outdated OS	data loss, operations disrupted	IT, Maintenance

Risk evaluation

- Objective : rank risks (threat/vulnerability pairs)
- Have to consider
    - Asset values
    - Risk consequences
        - For the company
        - Third parties
        - Environment
- Generally a consequence/likelihood matrix is used

Asset oriented evaluation

	Threat Likelihood	**Low**			**Medium**			**High**		
	Ease of exploitation	**L**	**M**	**H**	**L**	**M**	**H**	**L**	**M**	**H**
Asset value	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

- Example. Asset: historian, Threat : network sniffing

Consequence oriented

	Likelihood of incident scenario	**Very low** **(Very unlikely)**	**Low** **(Unlikely)**	**Medium** **(Possible)**	**High** **(Likely)**	**Very high** **(Frequent)**
Bussines impact	Very low	0	1	2	3	4
	Low	1	2	3	4	5
	Medium	2	3	4	5	6
	High	3	4	5	6	7
	Very high	4	5	6	7	8

- Example: Environment pollution due to an external threat taking control on SCADA

Cross asset value/threat likelihood

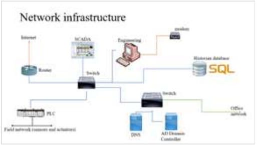
For each threat compute risk score as a product of asset value and threat likelihood

Threat descriptor (a)	**Consequence or asset value** (b)	**Likelihood of threat occurence** (c)	**Measure of risk** (d)	**Threat ranking** (e)
PLC disruption	5	2	10	3
SCADA compromission	5	4	15	1
Eng computer fail	3	5	15	1
Data breach on historian	2	4	8	4
DNS poison	1	5	5	5

Choice of controls

- General threats: conformity approach
  - Good practices
  - Regulations
    - France : RGS, RGPD
    - USA : NIST regulations
  - Standards
    - ISO 27000 - Information technology - Security techniques
    - IEC 62443 - Industrial communication networks – Network and system security
    - IEC 62351 - Power systems management andv associated information exchange – Data and communications security
    - ISO 27019 - Information technology - Security techniques – Information security controls for the energy utility industry
- Specific threats
  - Scenario analysis, specific in depth defense policy

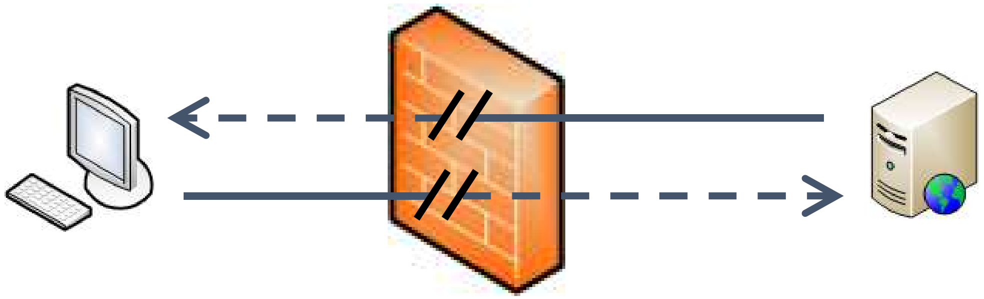
ISO 27000 security control classes



- Legal
  - Compliance
- Organizational
  - Information security policies
  - Organization of information security
  - Human Resources Security
  - Asset Management
- Partner relationship
  - System acquisition, development and maintenance
  - Supplier relationships
- Incident management
  - Information security incident management
  - Information security aspects of business continuity management
- Technical
  - Access Control
  - Cryptography
  - Physical and Environmental Security
  - Operations security
  - Communications security

Firewall

- **Passthrough device for network flows between 2 or more networks**
- Deep packet inspection for input and output flows.
- **Rule-based filtering :** only network packet compliant with rules will be transmitted.
- May include an anti-virus



For each input or output flow the firewall will check the rules do decide if packets are allowed to go

IDS and IPS

IDS **I**ntrusion **D**etection **S**ystem

IPS **I**ntrusion **P**revention **S**ystem

Devices designed for network flow analysis and **detection of intrision attempts** :

- Either analyzing the behavior of the network flows;
- Either using patterns or signatures of harmful data flows

When an intriusion is detected :

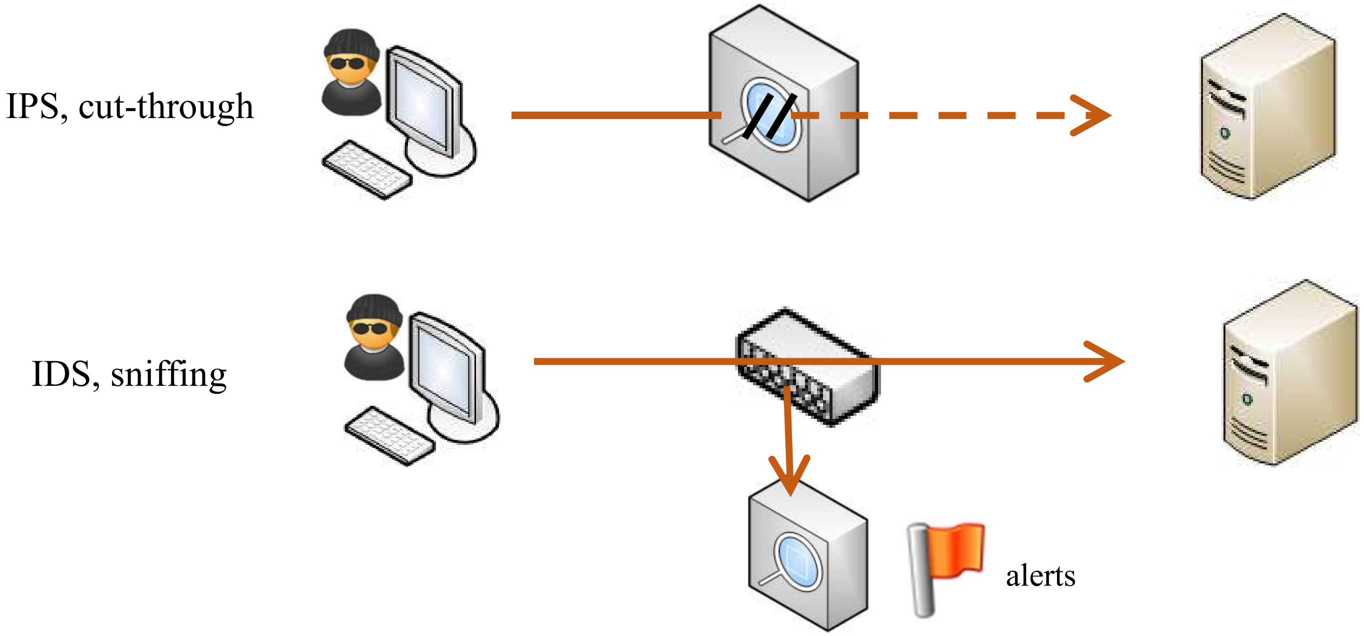
- The **IDS will raise alerts** to the administrators who take the decisions;
- The **IPS will block** lhe harmful network flows.

IDS/IPS need a detailed and maintained configuration :

- They might raise false positives (i.e. they will wrongly alert a legitimate traffic);
- Signature based IDS/IPS can detect only intrusions whose caracteristics re already known.

Free IDS

- Pattern-oriented
  - SNORT https://www.snort.org/ (can also be configured as IPS)
  - Suricata https://suricata-ids.org/
- Mixed
  - Zeek https://zeek.org/

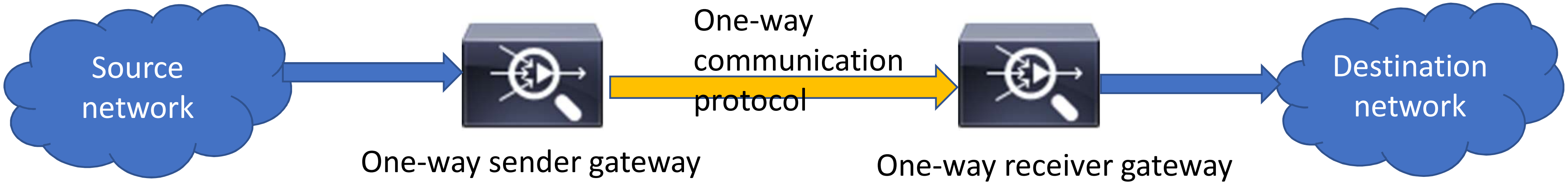


Data diode

- Passive (no IP), one-way transmission device
- Cannot be attacked through the network (no IP)
- Can be used successfully for one way UDP transmission
- Breaks TCP protocols (no ACKs)
- Breaks routing protocols
- Alone can be used only for traffic monitoring

One-way gateway

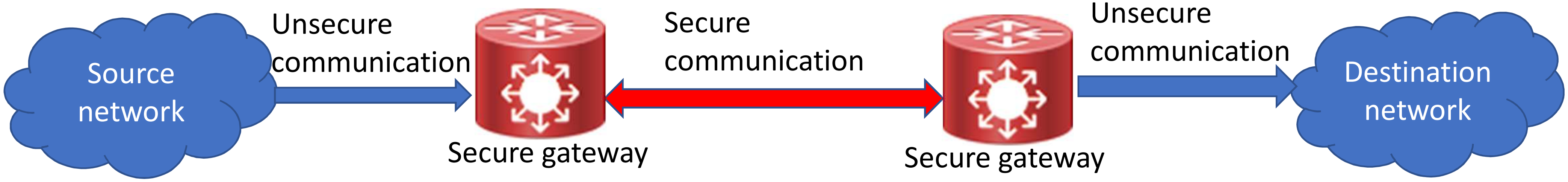
- Active device used for “one way” communication.



- Do not break TCP
- Allows routing
- Can be attacked thru the network (has an IP)
- May be enforced with a diode

Secure gateway

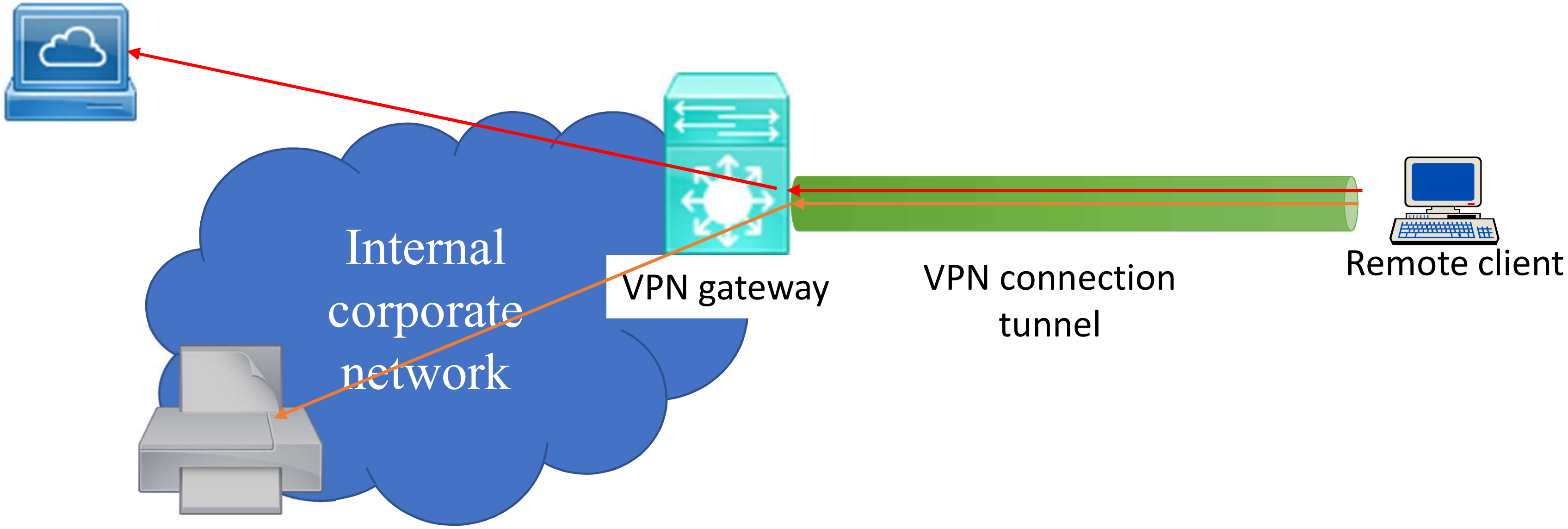
- Protocol translation gateway



- Allows bi-directional communications
- Do not break protocols
- Allows routing

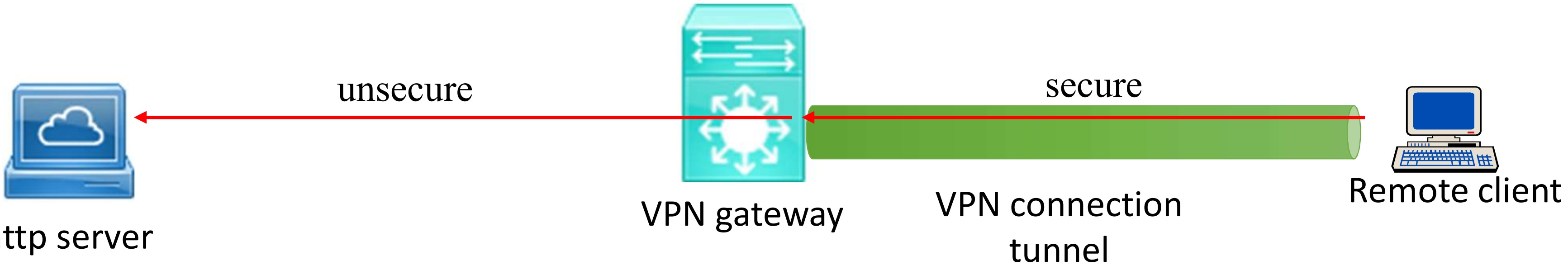
VPN Virtual Private Network

- Originally used to allow access to internal network resources
- Once connected (tunnel) ALL connection goes thru the VPN gateway and uses a corporate IP number
- VPN Gateway:
  - Authenticates the user
  - Provides a new IP number (corporate internal)



VPN and security

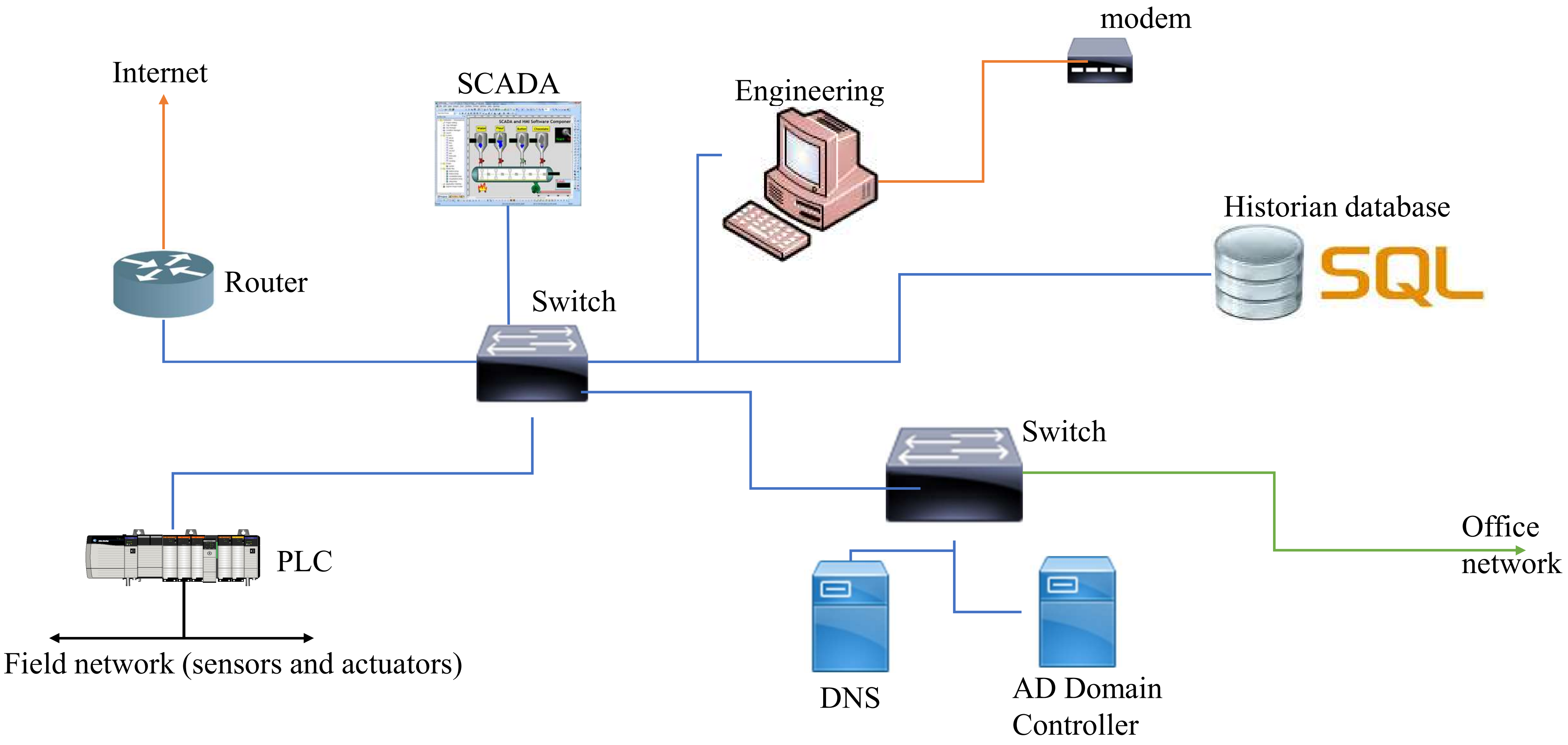
- Tunnel protocol is secure : IPsec or TLS
- VPN will :
  - Secure communications between mobile client and VPN gateway (or between two VPN gateways)
- VPN will not :
  - Provide Internet anonymity (the gateway knows who you are)
  - Provide secure end to end connection



Remainders

- CISCO Certificates
- Lab reports : supervisory control

Exercise : securing the example network


modem
Internet
SCADA
Engineering
Historian database
SQL
Router
Switch
Switch
Office network
PLC
Field network (sensors and actuators)
DNS
AD Domain Controller