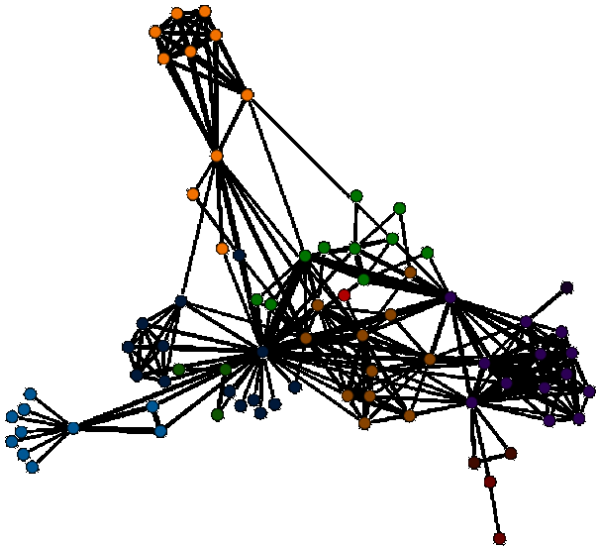
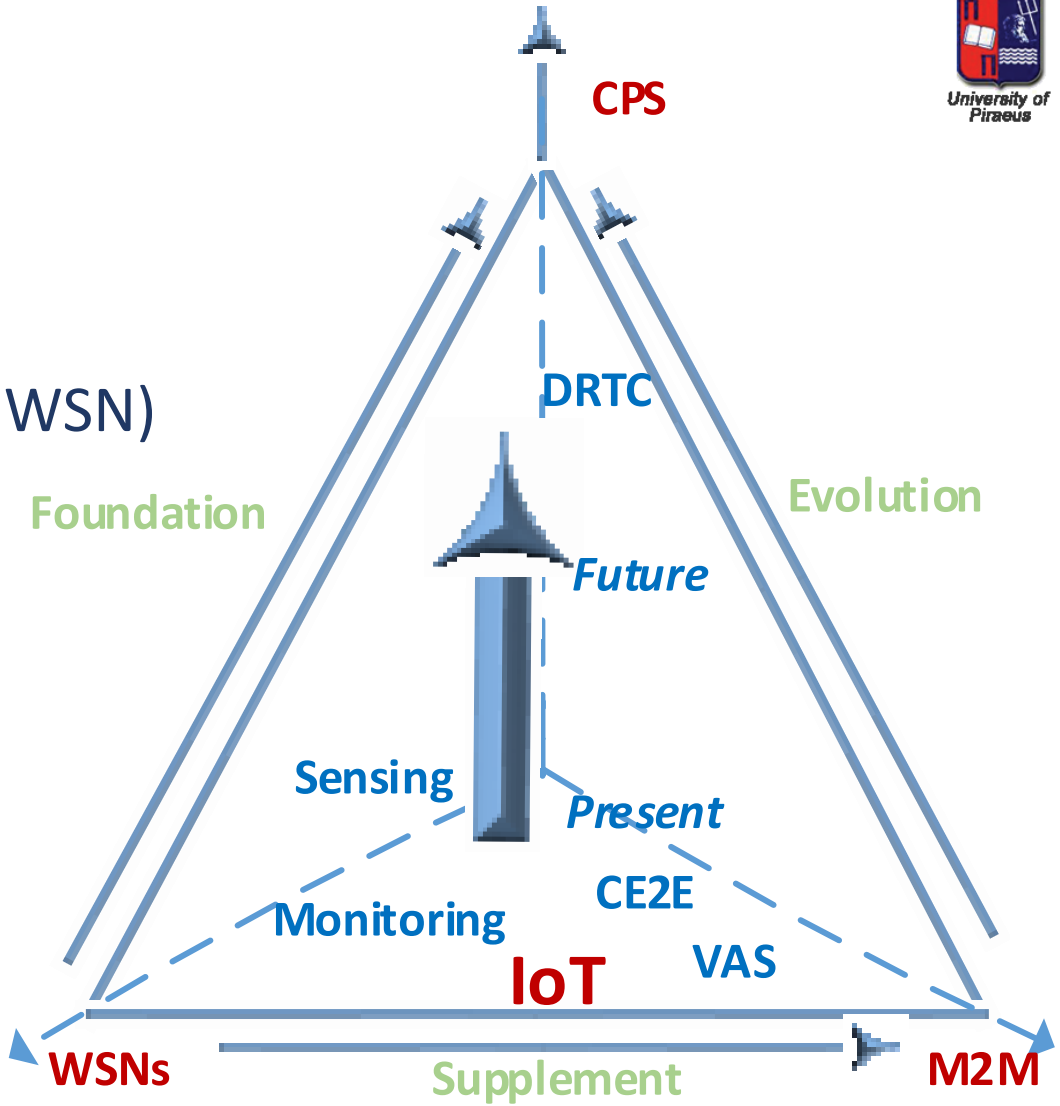
Ad-hoc & Sensor Networking for M2M Communications:
Threat Landscape and Good Practice Guide

Dimitrios Kallergis, Zacharenia Garofalaki
Department of Informatics, University of Piraeus, Greece
{d.kallergis, z.garofalaki}@unipi.gr



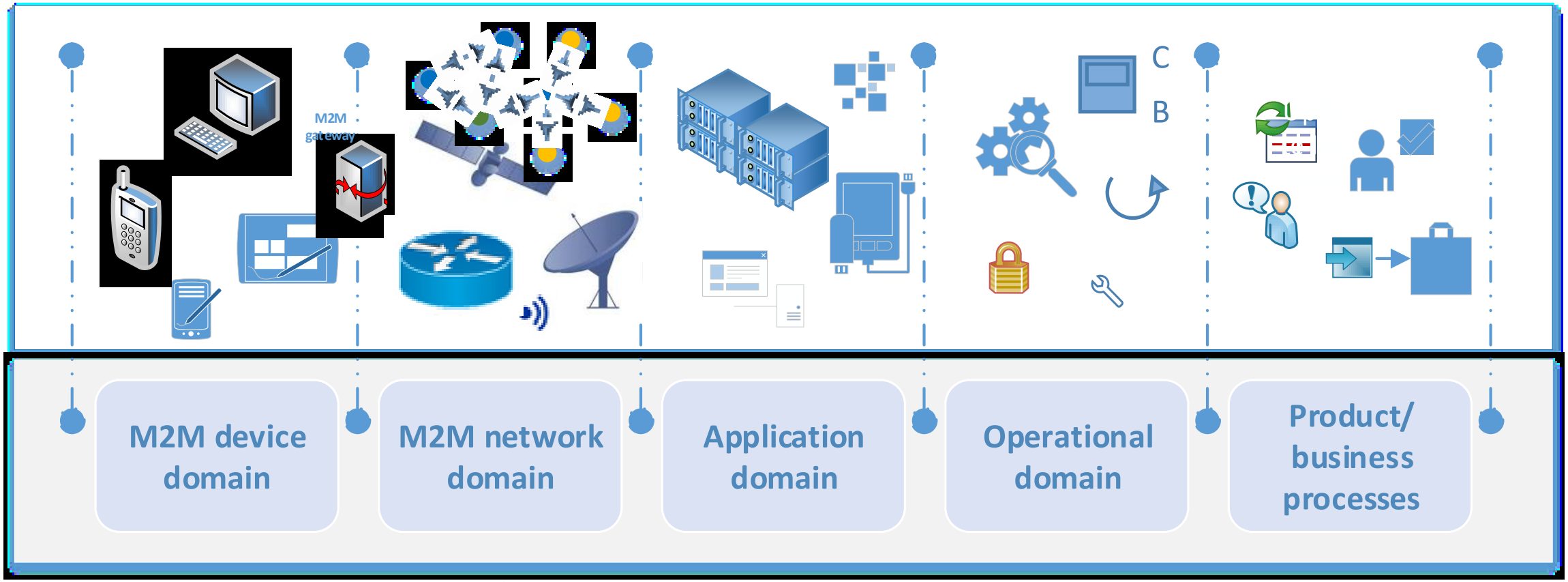
Terminology

- Machine-to-Machine (M2M)
- Ad-hoc and sensor networking (WMN, MANETs, WSN)
- Internet of Things (IoT)
- Cyber-Physical Systems (CPS)



CPS: Cyber-Physical Systems
DRTC: Distributed real-time control
CE2E: Communicating end-to-end
VAS: Value added services

Extension of the ETSI M2M architecture



Usually embedded

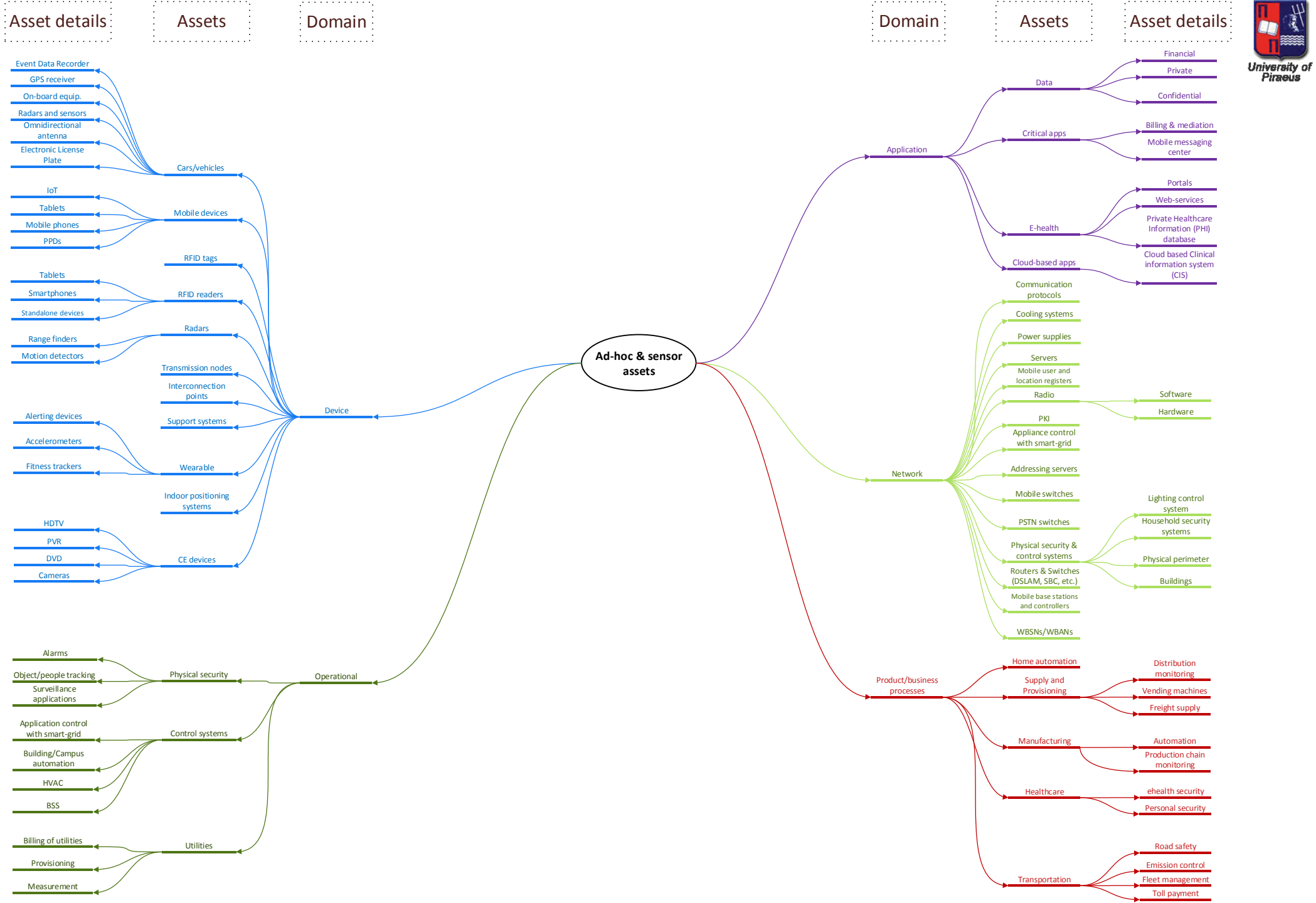
Connection between devices, sensors, gateways, networks

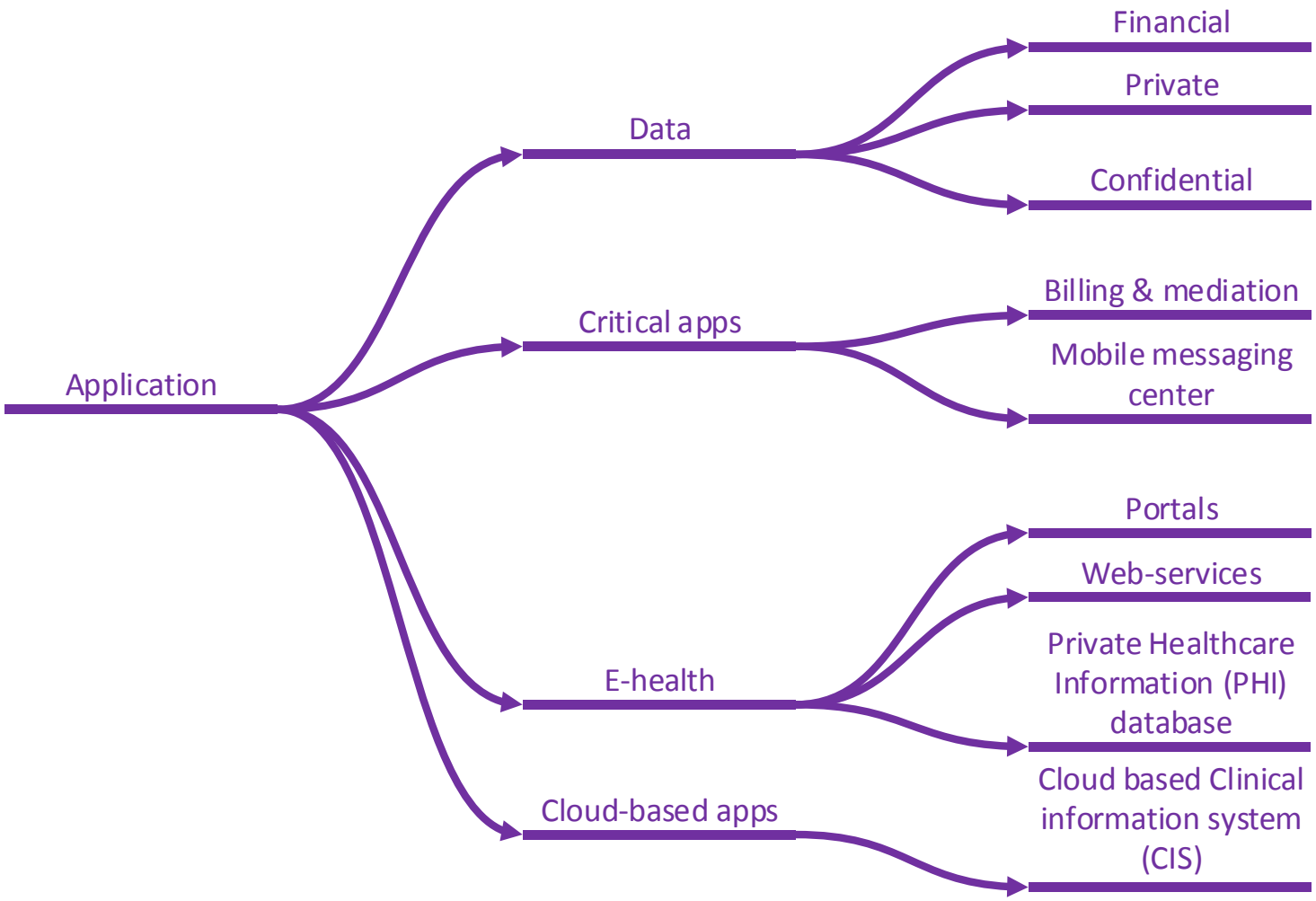
Data manipulation by business-apps

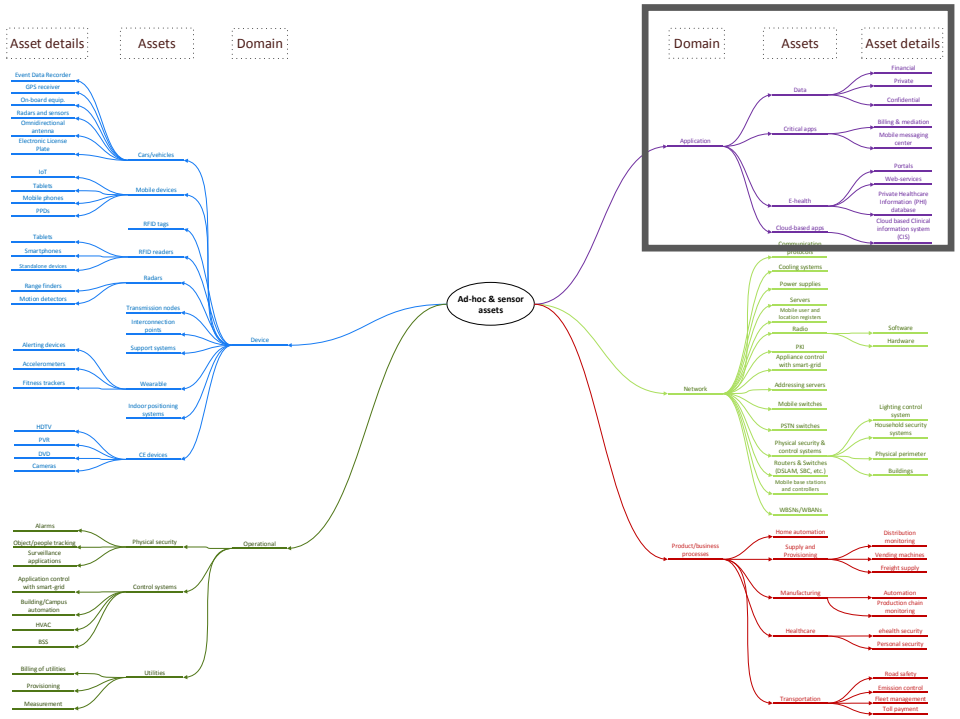
Physical security, control systems, utilities

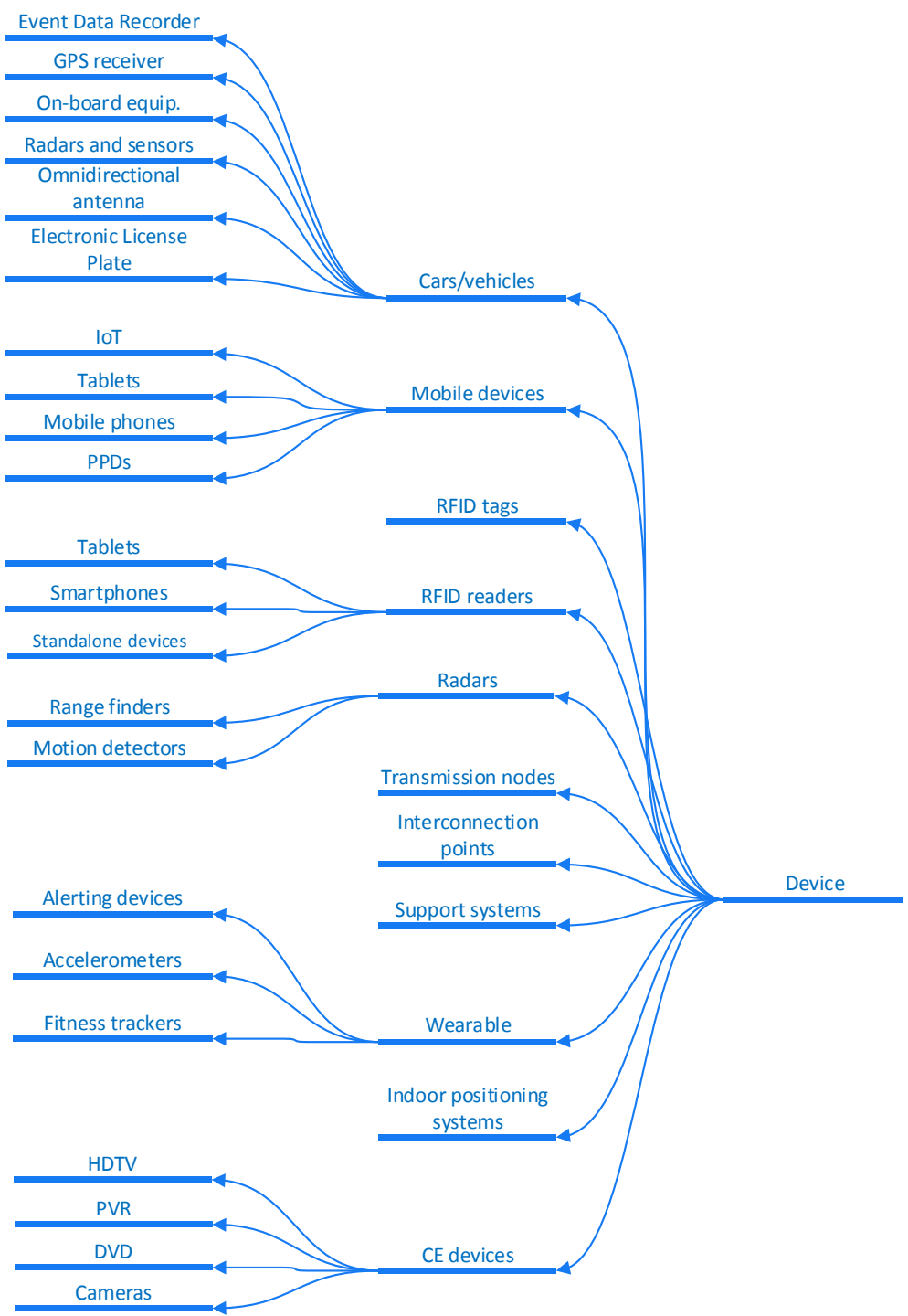
Transportation, healthcare, etc.

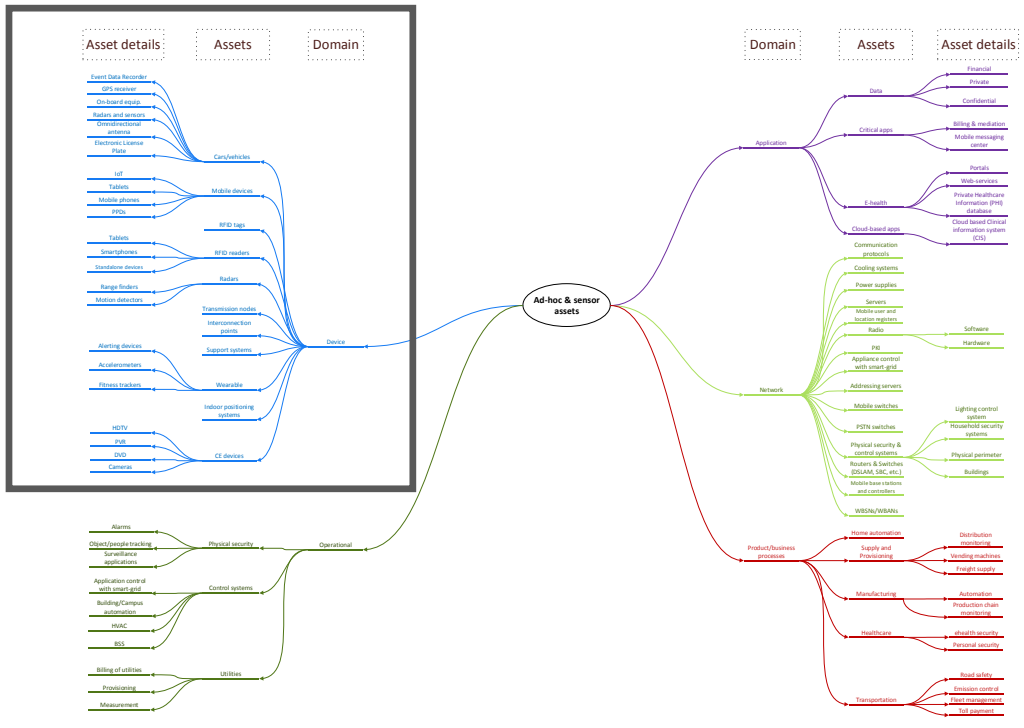
Assets

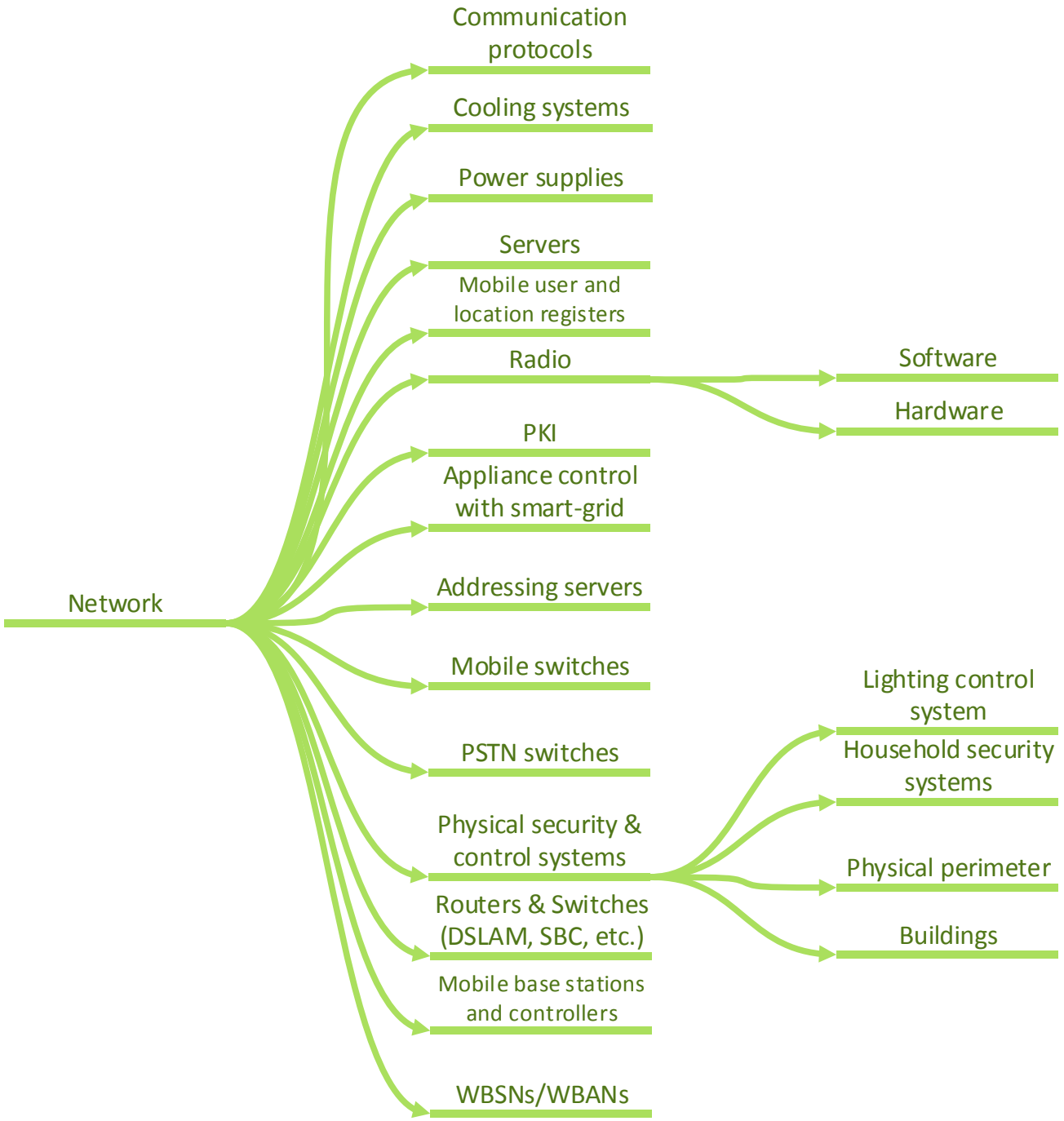

Asset details
Assets
Domain
Domain
Assets
Asset details
Ad-hoc & sensor assets
Device
Event Data Recorder
GPS receiver
On-board equip.
Radars and sensors
Omnidirectional antenna
Electronic License Plate
Cars/vehicles
IoT
Tablets
Mobile phones
PPDs
Mobile devices
RFID tags
Tablets
Smartphones
Standalone devices
RFID readers
Radars
Range finders
Motion detectors
Transmission nodes
Interconnection points
Support systems
Alerting devices
Accelerometers
Fitness trackers
Wearable
Indoor positioning systems
HDTV
PVR
DVD
Cameras
CE devices
Operational
Alarms
Object/people tracking
Surveillance applications
Physical security
Application control with smart-grid
Building/Campus automation
HVAC
BSS
Control systems
Billing of utilities
Provisioning
Measurement
Utilities
Application
Data
Financial
Private
Confidential
Critical apps
Billing & mediation
Mobile messaging center
E-health
Portals
Web-services
Private Healthcare Information (PHI) database
Cloud-based apps
Cloud based Clinical information system (CIS)
Network
Communication protocols
Cooling systems
Power supplies
Servers
Mobile user and location registers
Radio
Software
Hardware
PKI
Appliance control with smart-grid
Addressing servers
Mobile switches
PSTN switches
Physical security & control systems
Lighting control system
Household security systems
Physical perimeter
Buildings
Routers & Switches (DSLAM, SBC, etc.)
Mobile base stations and controllers
WBSNs/WBANs
Product/business processes
Home automation
Supply and Provisioning
Distribution monitoring
Vending machines
Freight supply
Manufacturing
Automation
Production chain monitoring
Healthcare
ehealth security
Personal security
Transportation
Road safety
Emission control
Fleet management
Toll payment

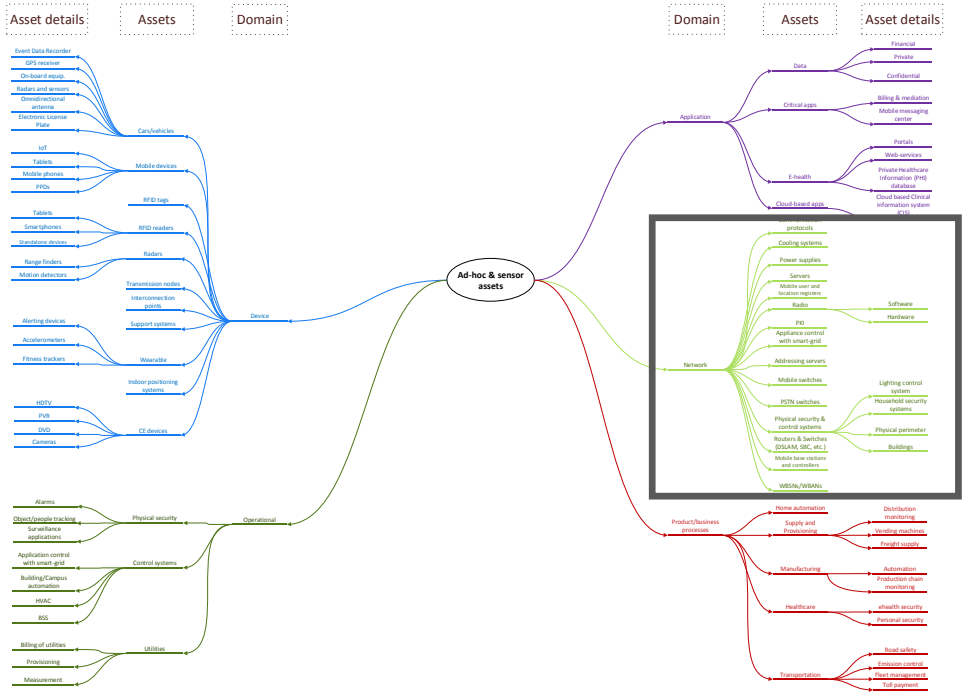

Application
Data
Financial
Private
Confidential
Critical apps
Billing & mediation
Mobile messaging center
E-health
Portals
Web-services
Private Healthcare Information (PHI) database
Cloud-based apps
Cloud based Clinical information system (CIS)

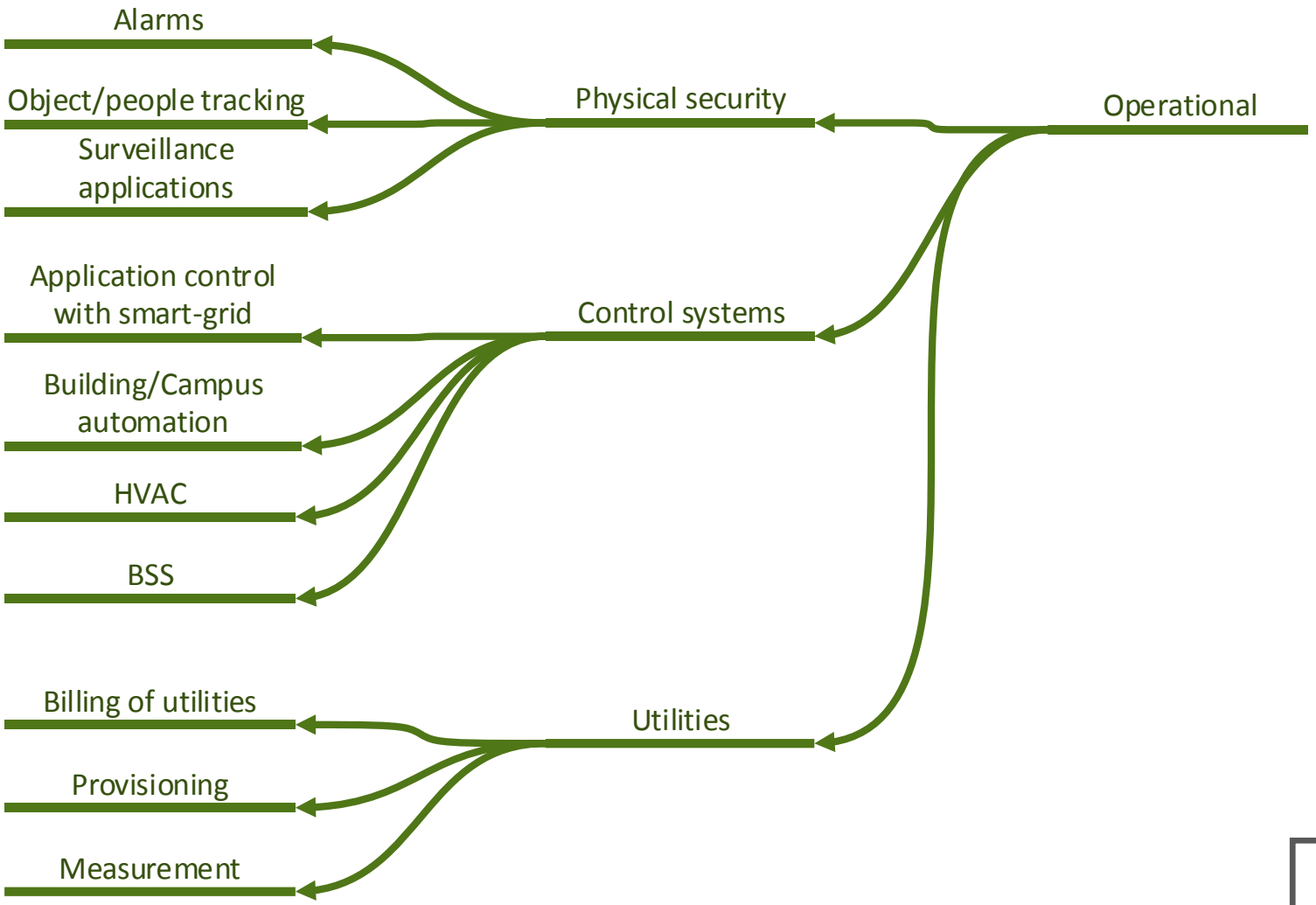

Asset details
Assets
Domain
Ad-hoc & sensor assets
Device
Operational
Network
Application
Product/business processes
Physical security
Control systems
Utilities
Data
Critical apps
E-health
Cloud-based apps
Financial
Private
Confidential
Billing & mediation
Mobile messaging center
Portals
Web-services
Private Healthcare Information (PHI) database
Cloud based Clinical information system (CIS)

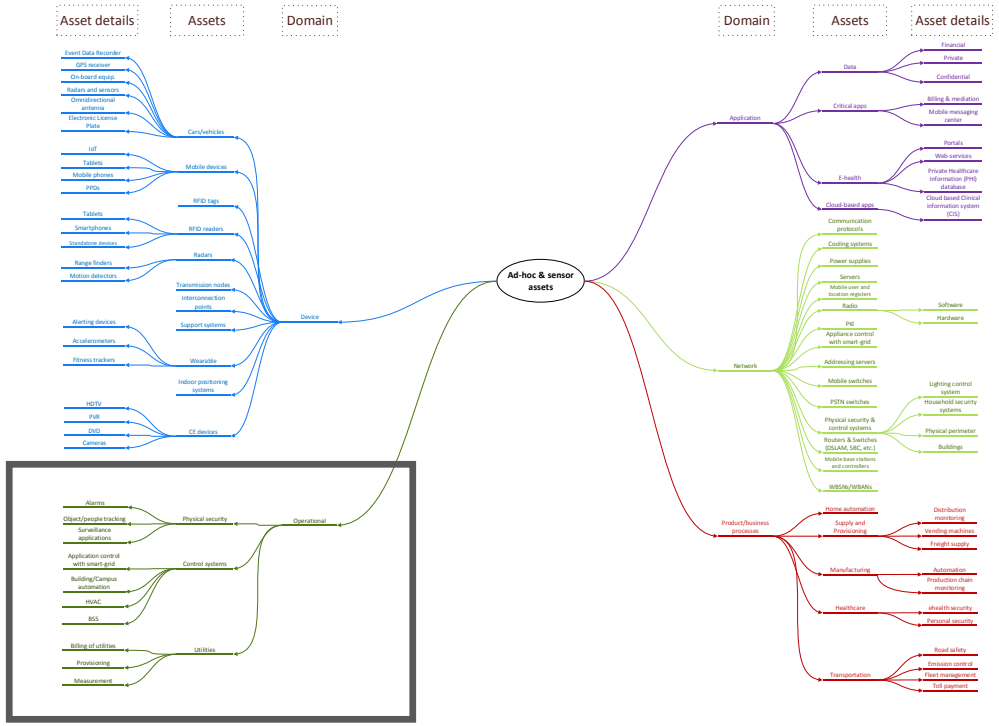

Event Data Recorder
GPS receiver
On-board equip.
Radars and sensors
Omnidirectional antenna
Electronic License Plate
Cars/vehicles
IoT
Tablets
Mobile phones
PPDs
Mobile devices
RFID tags
Tablets
Smartphones
Standalone devices
RFID readers
Radars
Range finders
Motion detectors
Transmission nodes
Interconnection points
Support systems
Device
Alerting devices
Accelerometers
Fitness trackers
Wearable
Indoor positioning systems
HDTV
PVR
DVD
Cameras
CE devices

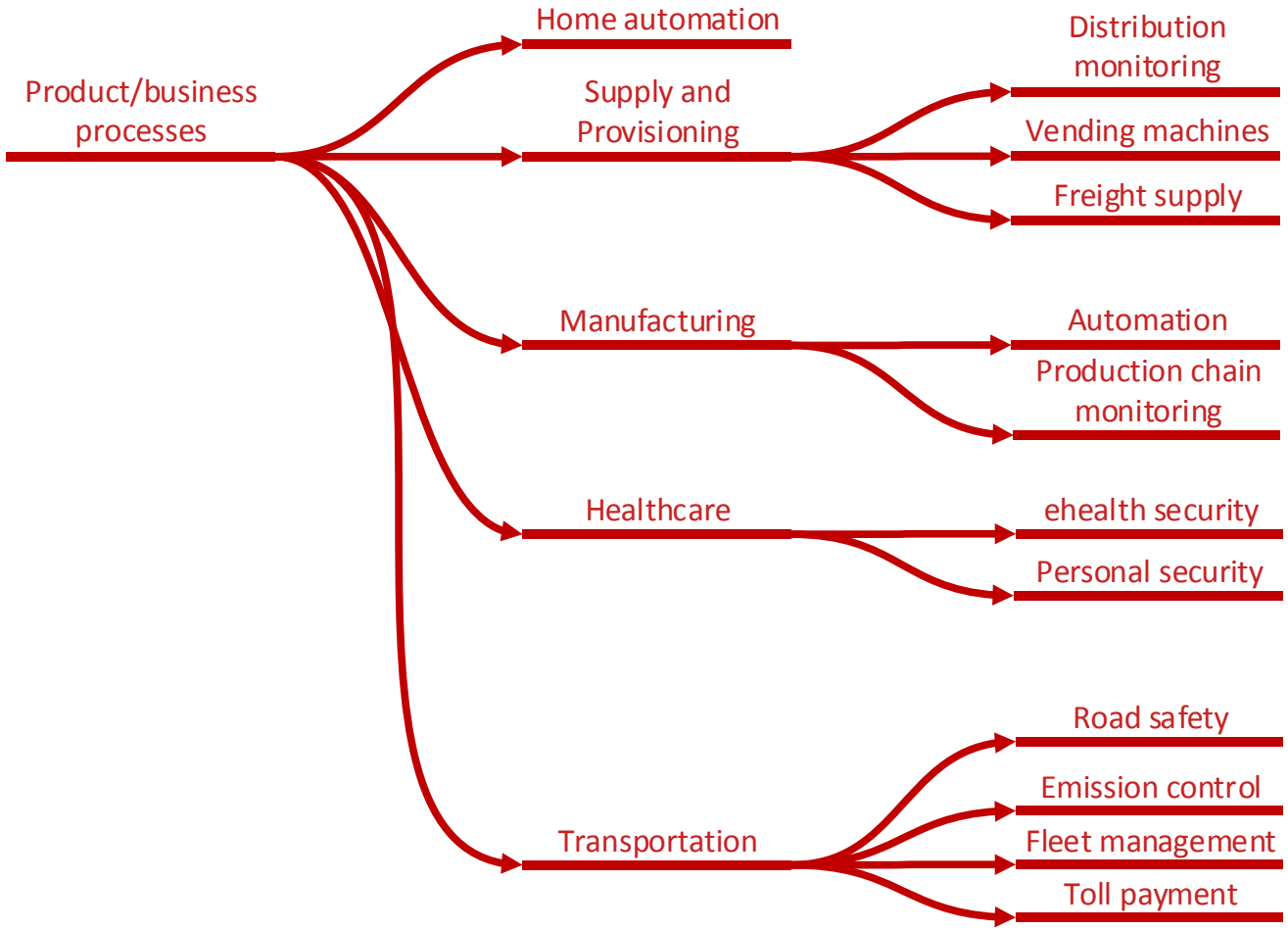

Asset details
Assets
Domain
Ad-hoc & sensor assets
Operational
Physical security
Control systems
Utilities
Application
Network
Product/business processes
Data
Critical apps
E-health
Cloud-based apps
Financial
Private
Confidential
Billing & mediation
Mobile messaging center
Portals
Web-services
Private Healthcare Information (PHI) database
Cloud based Clinical information system (CIS)
Communication protocols
Cooling systems
Power supplies
Servers
Mobile user and location registers
Radio
PXI
Appliance control with smart-grid
Addressing servers
Mobile switches
PSTN switches
Physical security & control systems
Routers & Switches (GSLAM, SRC, etc.)
Mobile base stations and controllers
W8SNs/WBANs
Software
Hardware
Lighting control system
Household security systems
Physical perimeter
Buildings
Home automation
Supply and Provisioning
Manufacturing
Healthcare
Transportation
Distribution monitoring
Vending machines
Freight supply
Automation
Production chain monitoring
ehealth security
Personal security
Road safety
Emission control
Fleet management
Toll payment

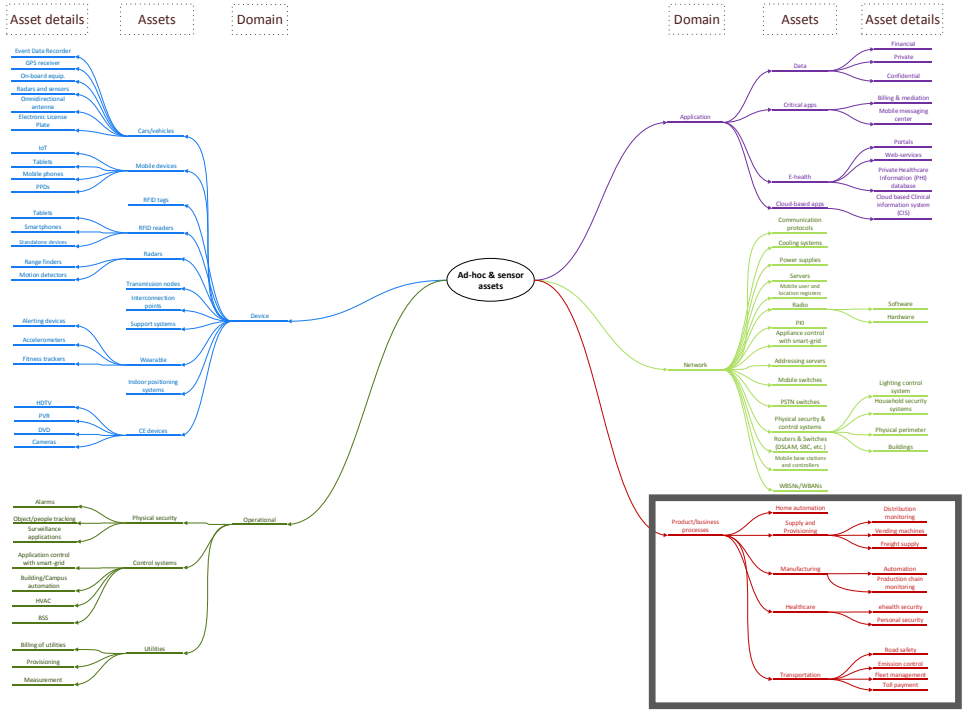

Network
Communication protocols
Cooling systems
Power supplies
Servers
Mobile user and location registers
Radio
Software
Hardware
PKI
Appliance control with smart-grid
Addressing servers
Mobile switches
PSTN switches
Physical security & control systems
Lighting control system
Household security systems
Physical perimeter
Buildings
Routers & Switches (DSLAM, SBC, etc.)
Mobile base stations and controllers
WBSNs/WBANs


Asset details
Assets
Domain
Ad-hoc & sensor assets
Device
Operational
Physical security
Control systems
Utilities
Application
Network
Product/business processes
Domain
Assets
Asset details

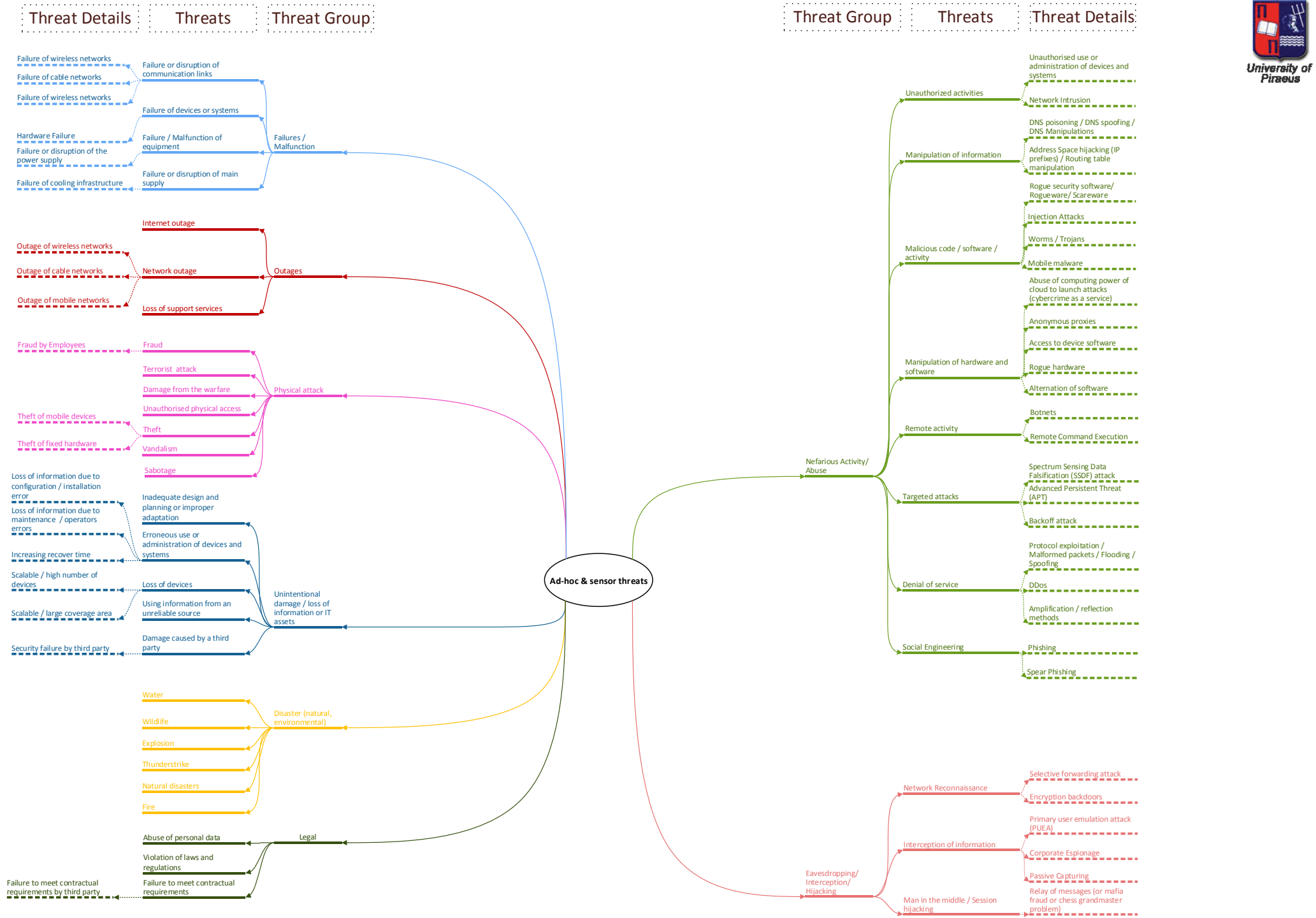

Alarms
Object/people tracking
Surveillance applications
Physical security
Operational
Application control with smart-grid
Control systems
Building/Campus automation
HVAC
BSS
Billing of utilities
Provisioning
Measurement
Utilities

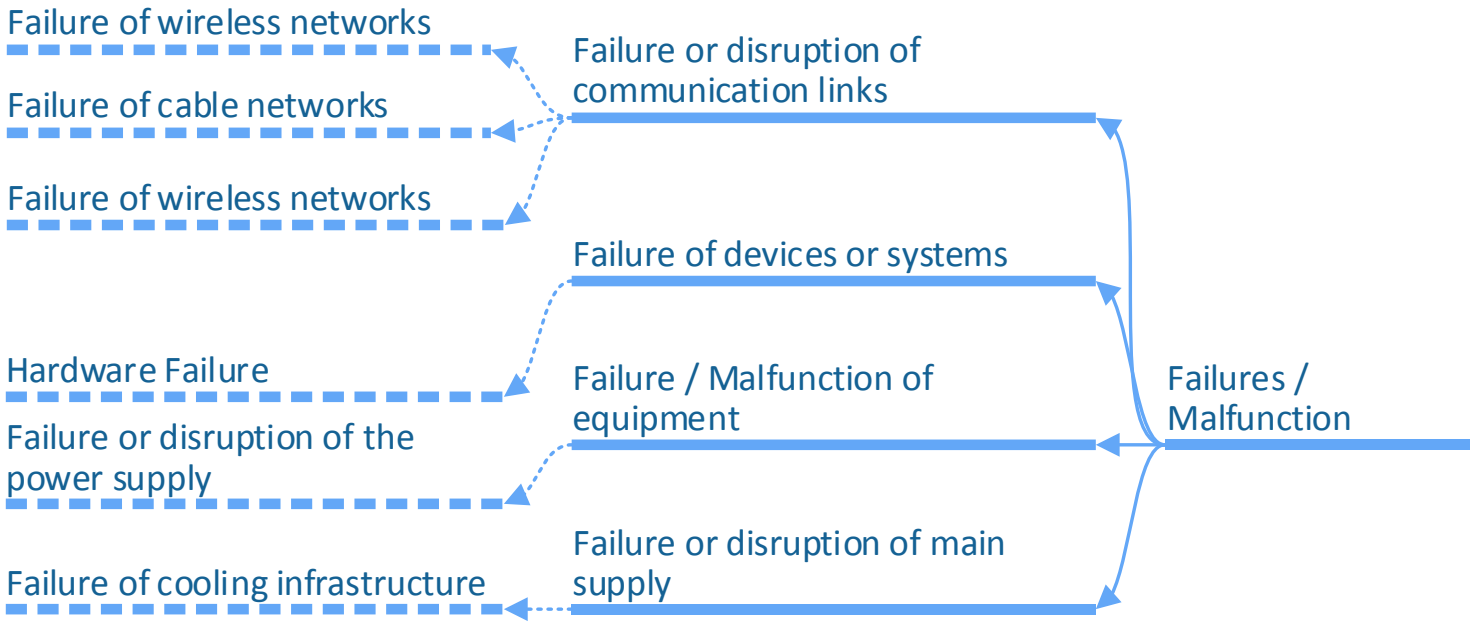

Asset details
Assets
Domain
Ad-hoc & sensor assets
Domain
Assets
Asset details
Application
Network
Product/business processes
Alarms
Object/people tracking
Surveillance applications
Physical security
Operational
Application control with smart-grid
Building/Campus automation
HVAC
BSS
Control systems
Billing of utilities
Provisioning
Measurement
Utilities

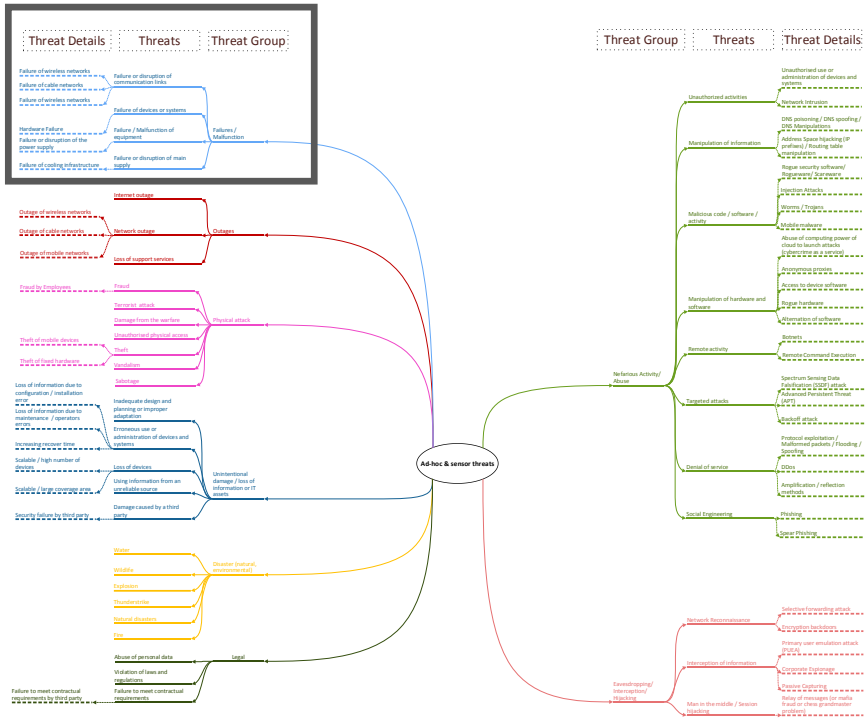

Product/business processes
Home automation
Supply and Provisioning
Distribution monitoring
Vending machines
Freight supply
Manufacturing
Automation
Production chain monitoring
Healthcare
ehealth security
Personal security
Transportation
Road safety
Emission control
Fleet management
Toll payment

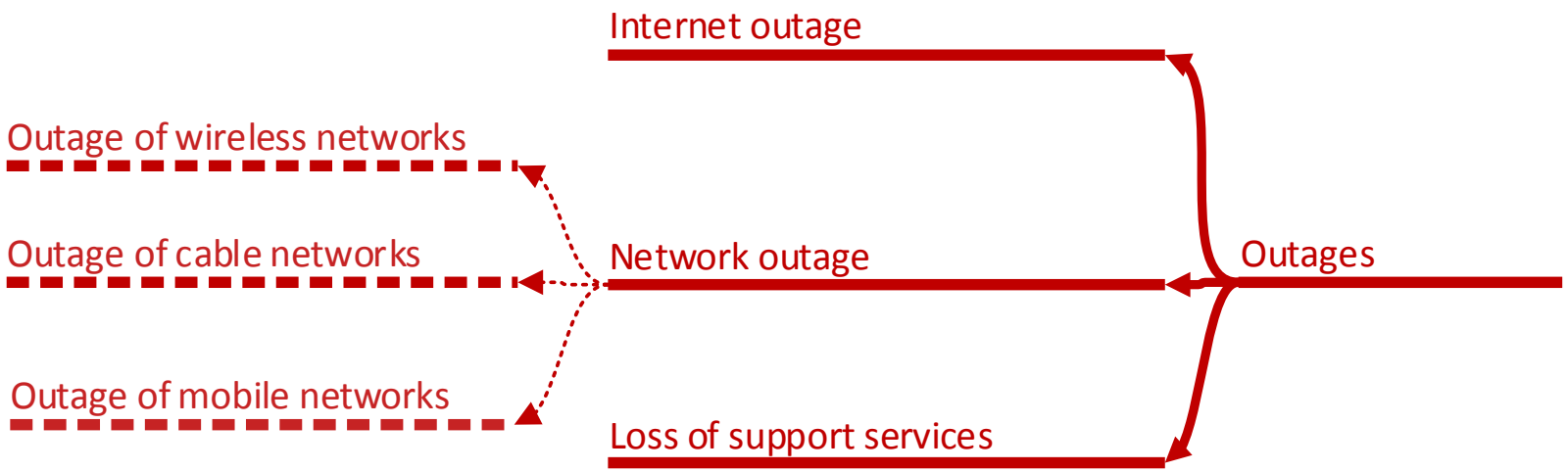

Asset details
Assets
Domain
Ad-hoc & sensor assets
Application
Network
Operational
Device
Physical security
Control systems
Utilities
Car/vehicles
Mobile devices
RFID tags
RFID readers
Radars
Transmission nodes
Interconnection points
Support systems
Wearable
Indoor positioning systems
CE devices
Data
Critical apps
E-health
Cloud-based apps
Financial
Private
Confidential
Billing & mediation
Mobile messaging center
Portals
Web-services
Private Healthcare Information (PHI) database
Cloud based Clinical information system (CIS)
Communication protocols
Cooling systems
Power supplies
Servers
Mobile user and location registers
Radio
Software
Hardware
PKI
Appliance control with smart-grid
Addressing servers
Mobile switches
PSTN switches
Physical security & control systems
Routers & Switches (GSLAM, SRC, etc.)
Mobile base stations and controllers
WBSNs/WBANs
Lighting control system
Household security systems
Physical perimeter
Buildings

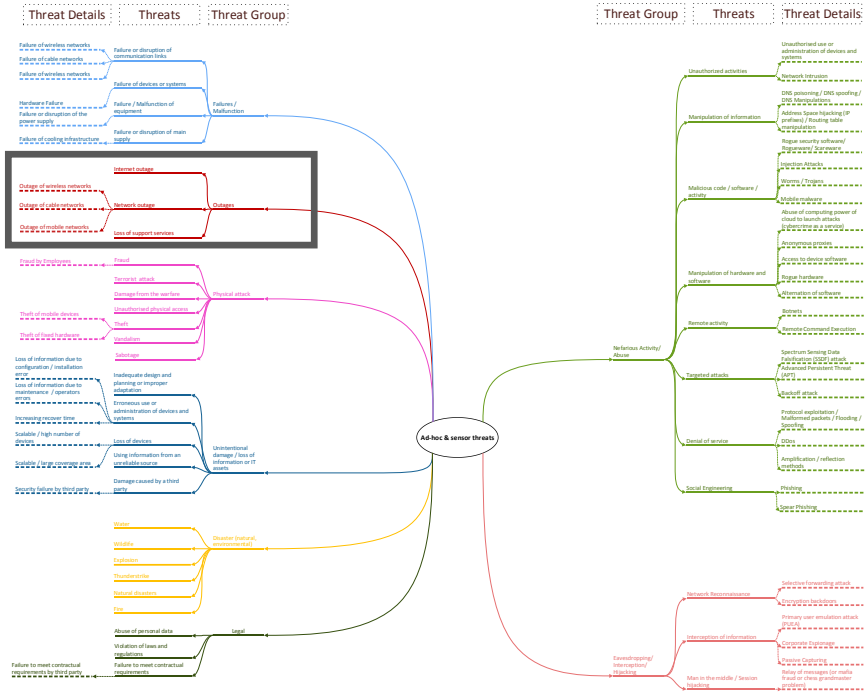
Threats


Threat Details
Threats
Threat Group
Threat Group
Threats
Threat Details
Failure of wireless networks
Failure of cable networks
Failure of wireless networks
Hardware Failure
Failure or disruption of the power supply
Failure of cooling infrastructure
Failure or disruption of communication links
Failure of devices or systems
Failure / Malfunction of equipment
Failure or disruption of main supply
Failures / Malfunction
Internet outage
Outage of wireless networks
Outage of cable networks
Outage of mobile networks
Network outage
Loss of support services
Outages
Fraud by Employees
Theft of mobile devices
Theft of fixed hardware
Fraud
Terrorist attack
Damage from the warfare
Unauthorised physical access
Theft
Vandalism
Sabotage
Physical attack
Loss of information due to configuration / installation error
Loss of information due to maintenance / operators errors
Increasing recover time
Scalable / high number of devices
Scalable / large coverage area
Security failure by third party
Inadequate design and planning or improper adaptation
Erroneous use or administration of devices and systems
Loss of devices
Using information from an unreliable source
Damage caused by a third party
Unintentional damage / loss of information or IT assets
Water
Wildlife
Explosion
Thunderstrike
Natural disasters
Fire
Disaster (natural, environmental)
Abuse of personal data
Violation of laws and regulations
Failure to meet contractual requirements by third party
Failure to meet contractual requirements
Legal
Ad-hoc & sensor threats
Nefarious Activity/ Abuse
Unauthorized activities
Unauthorised use or administration of devices and systems
Network Intrusion
Manipulation of information
DNS poisoning / DNS spoofing / DNS Manipulations
Address Space hijacking (IP prefixes) / Routing table manipulation
Malicious code / software / activity
Rogue security software/ Rogueware/ Scareware
Injection Attacks
Worms / Trojans
Mobile malware
Manipulation of hardware and software
Abuse of computing power of cloud to launch attacks (cybercrime as a service)
Anonymous proxies
Access to device software
Rogue hardware
Alternation of software
Remote activity
Botnets
Remote Command Execution
Targeted attacks
Spectrum Sensing Data Falsification (SSDF) attack
Advanced Persistent Threat (APT)
Backoff attack
Denial of service
Protocol exploitation / Malformed packets / Flooding / Spoofing
DDos
Amplification / reflection methods
Social Engineering
Phishing
Spear Phishing
Eavesdropping/ Interception/ Hijacking
Network Reconnaissance
Selective forwarding attack
Encryption backdoors
Interception of information
Primary user emulation attack (PUEA)
Corporate Espionage
Passive Capturing
Man in the middle / Session hijacking
Relay of messages (or mafia fraud or chess grandmaster problem)


Failure of wireless networks
Failure of cable networks
Failure of wireless networks
Hardware Failure
Failure or disruption of the power supply
Failure of cooling infrastructure
Failure or disruption of communication links
Failure of devices or systems
Failure / Malfunction of equipment
Failure or disruption of main supply
Failures / Malfunction


Threat Details
Threats
Threat Group
Ad-hoc & sensor threats
Threat Group
Threats
Threat Details


Internet outage
Outage of wireless networks
Outage of cable networks
Network outage
Outages
Outage of mobile networks
Loss of support services


Threat Details
Threats
Threat Group
Ad-hoc & sensor threats
Threat Group
Threats
Threat Details

Fraud by Employees

Fraud

Terrorist attack

Damage from the warfare

Physical attack

Unauthorised physical access

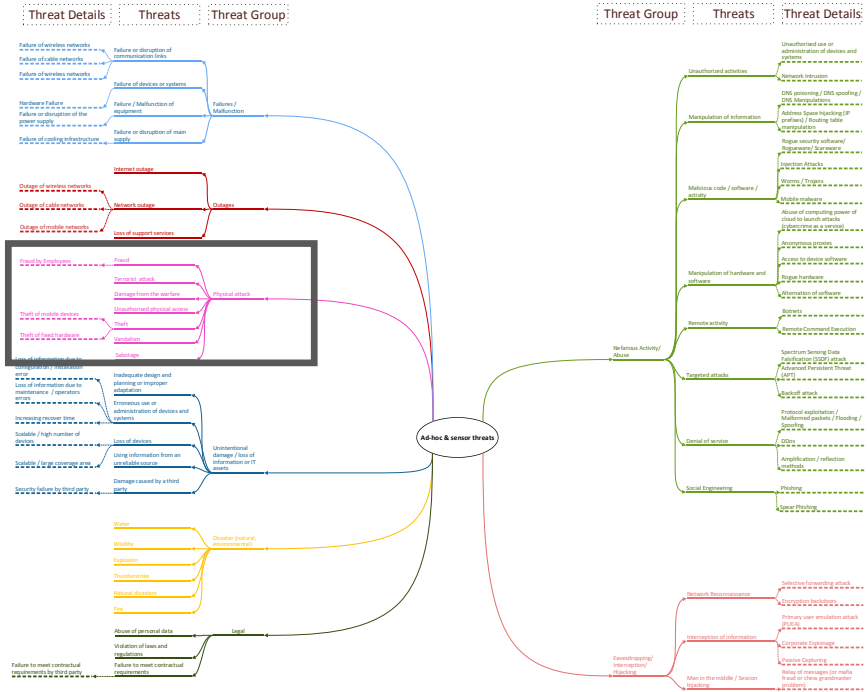
Theft of mobile devices

Theft

Theft of fixed hardware

Vandalism

Sabotage



Loss of information due to configuration / installation error

Loss of information due to maintenance / operators errors

Increasing recover time

Scalable / high number of devices

Scalable / large coverage area

Security failure by third party

Inadequate design and planning or improper adaptation

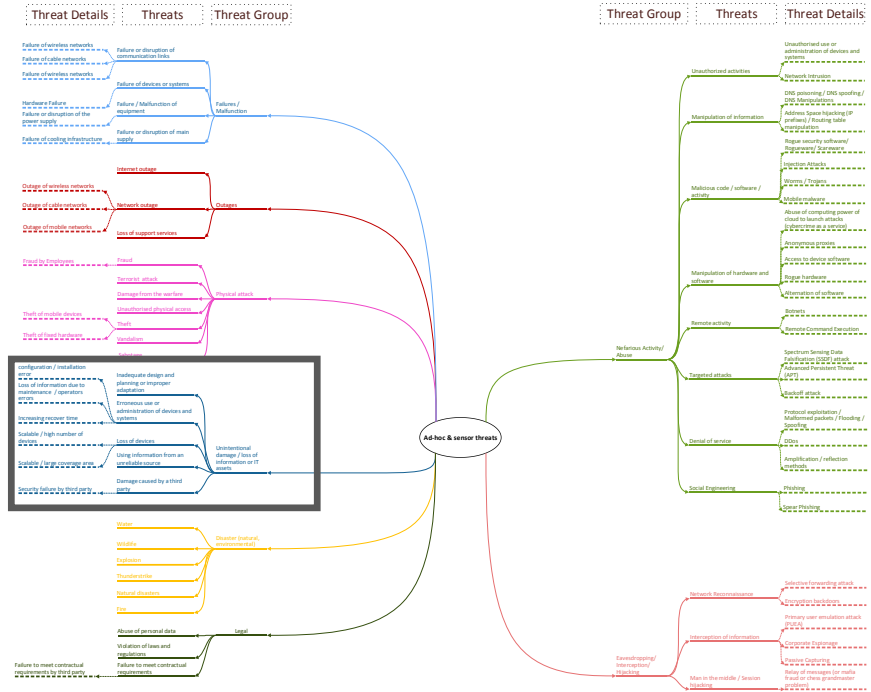
Erroneous use or administration of devices and systems

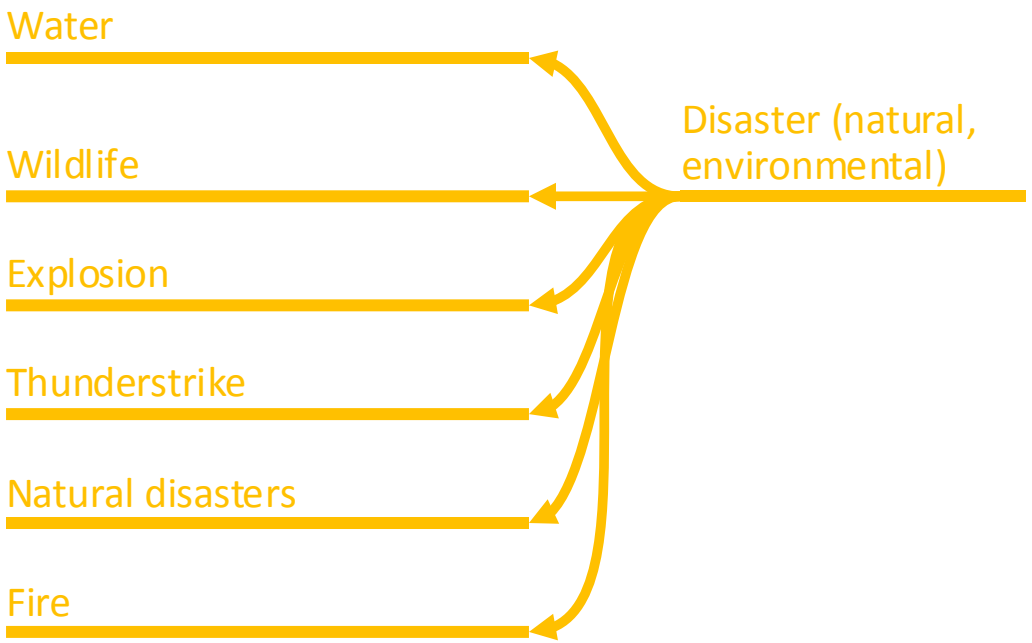
Loss of devices

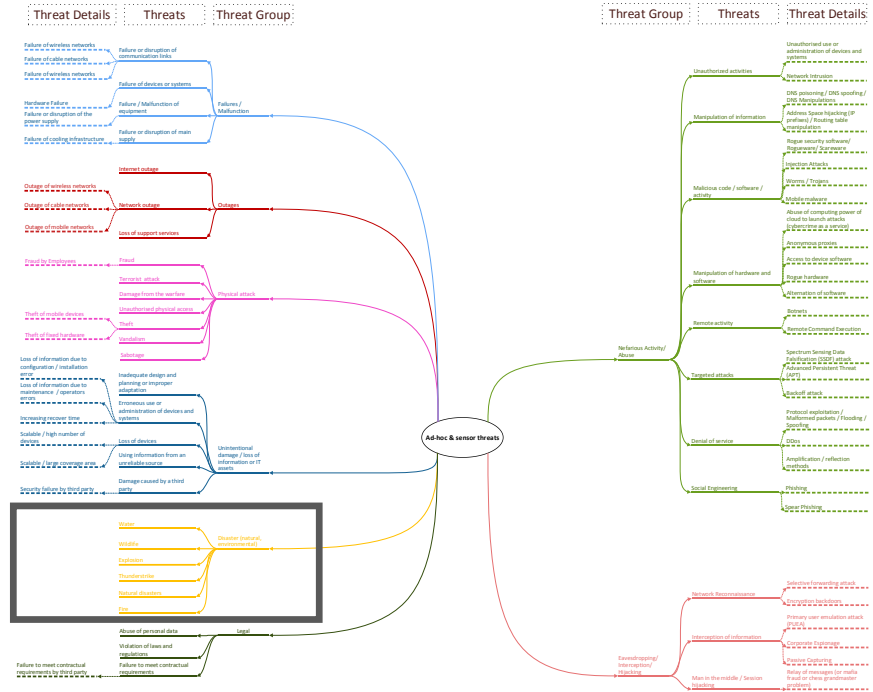
Using information from an unreliable source

Damage caused by a third party

Unintentional damage / loss of information or IT assets




Water
Wildlife
Explosion
Thunderstrike
Natural disasters
Fire
Disaster (natural, environmental)


Threat Details
Threats
Threat Group
Threat Group
Threats
Threat Details
Ad-hoc & sensor threats
Failure of wireless networks
Failure of cable networks
Failure of wireless networks
Hardware Failure
Failure or disruption of the power supply
Failure of cooling infrastructure
Failure or disruption of communication links
Failure of devices or systems
Failure / Malfunction of equipment
Failure or disruption of main supply
Failures / Malfunction
Outage of wireless networks
Outage of cable networks
Outage of mobile networks
Internet outage
Network outage
Loss of support services
Outages
Fraud by Employees
Fraud
Terrorist attack
Damage from the warfare
Unauthorised physical access
Theft
Vandalism
Sabotage
Physical attack
Theft of mobile devices
Theft of fixed hardware
Loss of information due to configuration / installation error
Loss of information due to maintenance / operators errors
Increasing recover time
Scalable / high number of devices
Scalable / large coverage area
Security failure by third party
Inadequate design and planning or improper adaptation
Erroneous use or administration of devices and systems
Loss of devices
Using information from an unreliable source
Damage caused by a third party
Unintentional damage / loss of information or IT assets
Water
Wildfire
Explosion
Thunderstrike
Natural disasters
Fire
Disaster (natural, environmental)
Abuse of personal data
Violation of laws and regulations
Failure to meet contractual requirements
Failure to meet contractual requirements by third party
Legal
Nefarious Activity/ Abuse
Eavesdropping/ Interception/ Hijacking
Unauthorised activities
Manipulation of information
Malicious code / software / activity
Manipulation of hardware and software
Remote activity
Targeted attacks
Denial of service
Social Engineering
Unauthorised use or administration of devices and systems
Network Intrusion
DNS poisoning / DNS spoofing / Domain hijacking
Address Space hijacking (IP prefixes) / Routing table poisoning
Rogue security software/ Rogueware/ Scareware
Injection Attacks
Worms / Trojans
Mobile malware
Abuse of computing power of cloud to launch attacks
Anonymous proxies
Access to device software
Rogue hardware
Alternation of software
Botnets
Remote Command Execution
Spectrum Sensing Data Falsification (SSDF) attack
Low-and-Slow / Stealthy / Advanced Persistent Threat (APT)
Blackoff attack
Protocol exploitation / Malformed packets / Flooding / Spoofing
DDos
Amplification / reflection methods
Phishing
Spear Phishing
Network Reconnaissance
Interception of information
Man in the middle / Session hijacking
Selective Forwarding attack
Sinkhole/ blackhole
Primary user emulation attack (PUEA)
Corporate Espionage
Passive Capturing
Relay of messages (or mafia fraud) or chess grandmaster problem)

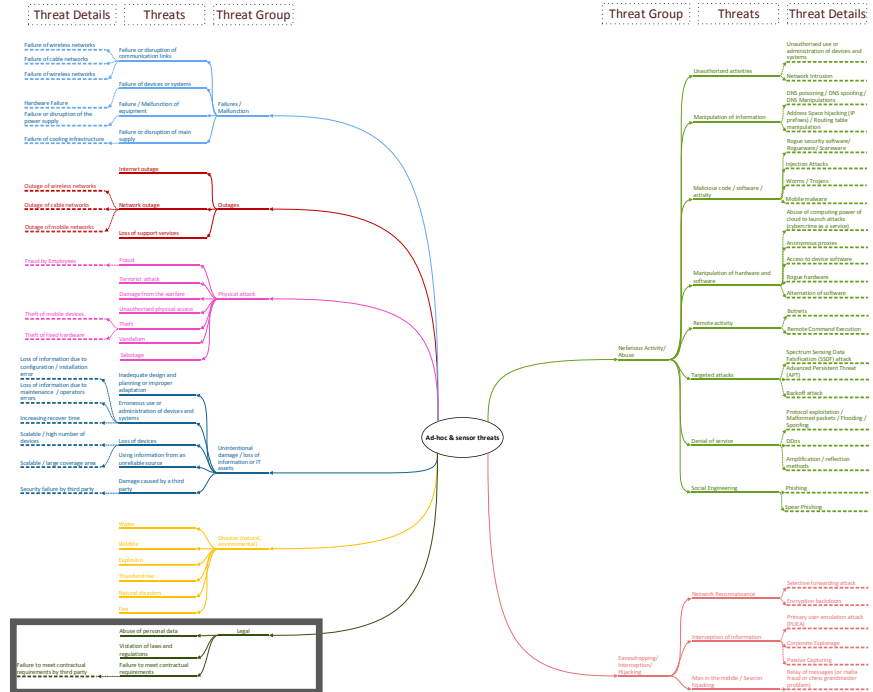
Abuse of personal data

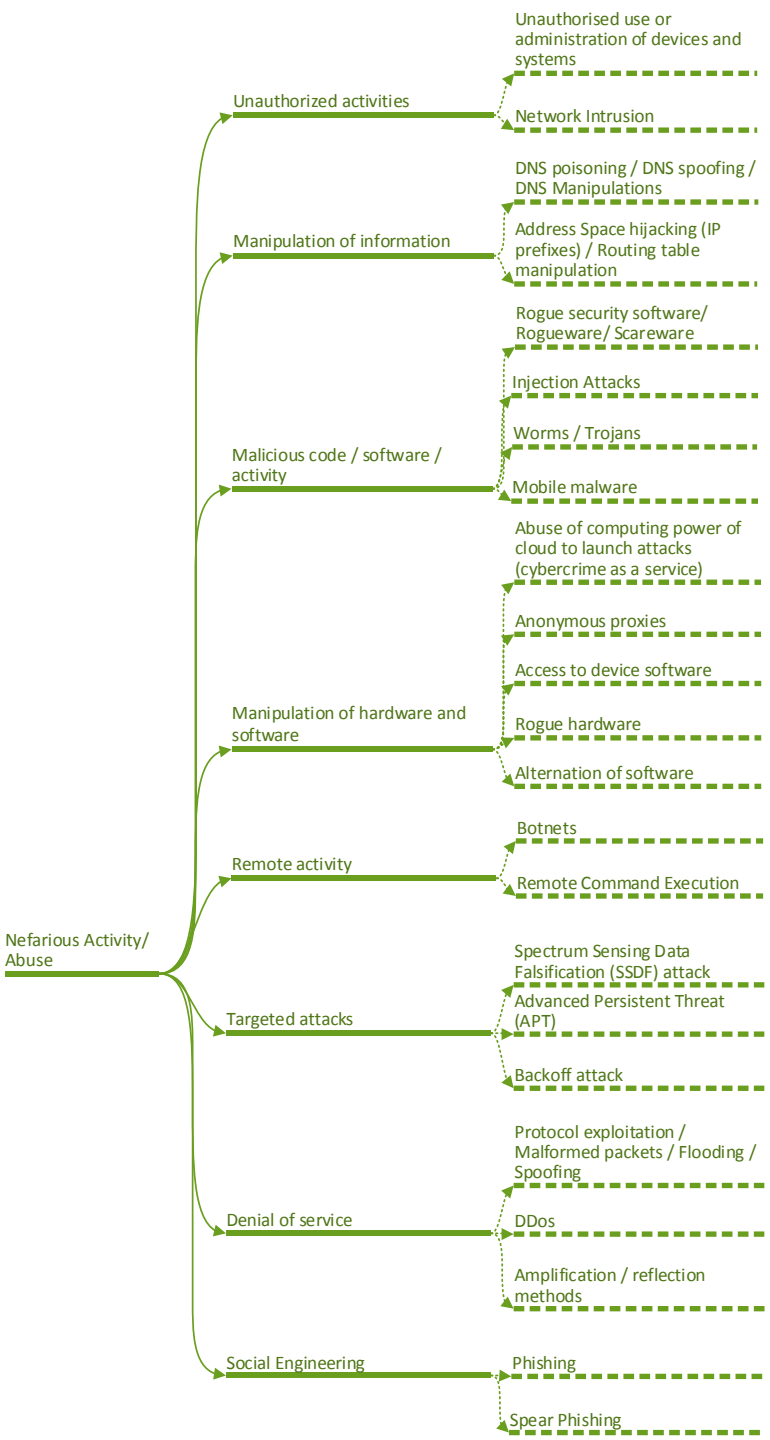
Legal

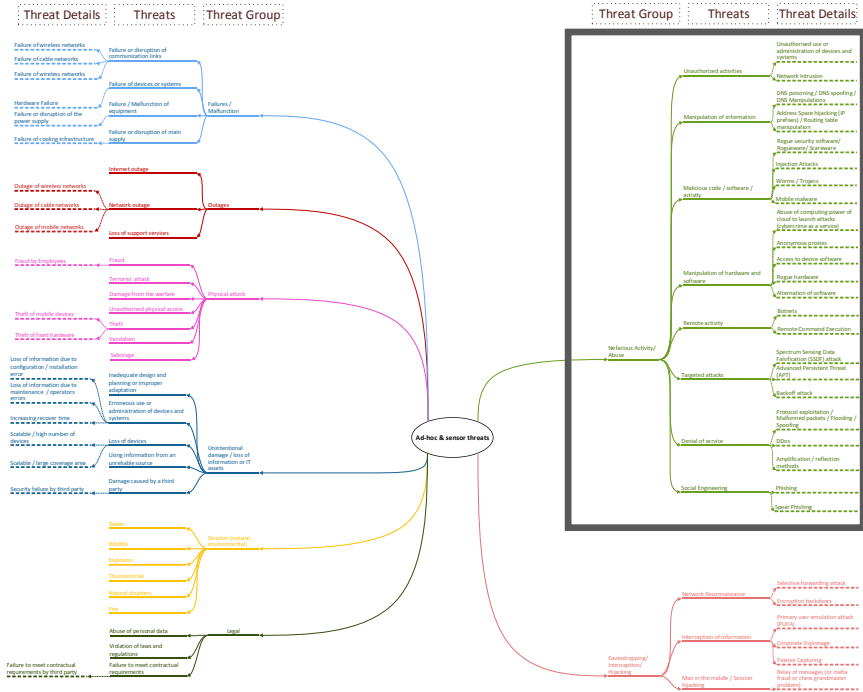
Violation of laws and regulations

Failure to meet contractual requirements by third party

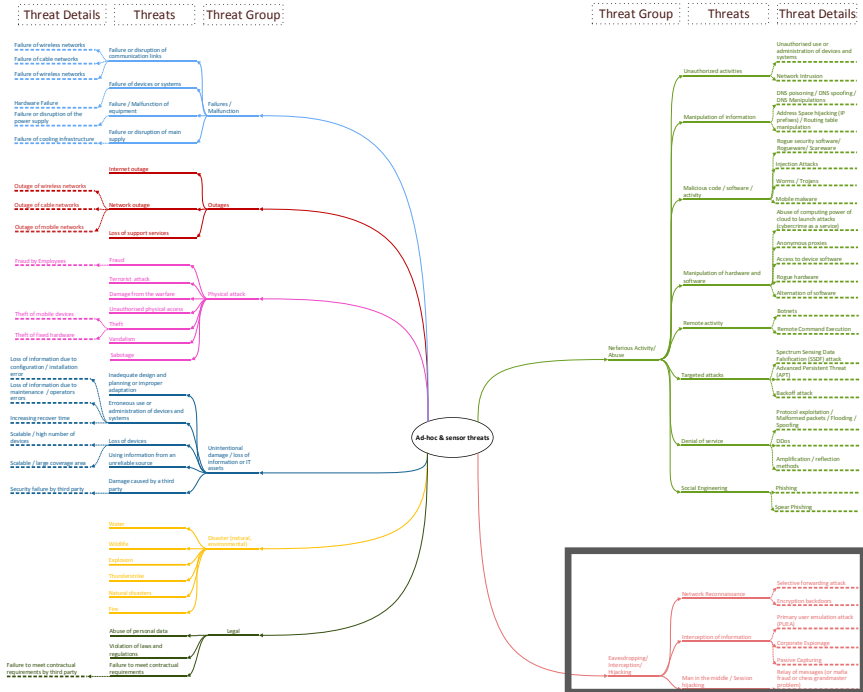
Failure to meet contractual requirements




Nefarious Activity/ Abuse
Unauthorized activities
Unauthorised use or administration of devices and systems
Network Intrusion
Manipulation of information
DNS poisoning / DNS spoofing / DNS Manipulations
Address Space hijacking (IP prefixes) / Routing table manipulation
Malicious code / software / activity
Rogue security software/ Rogueware/ Scareware
Injection Attacks
Worms / Trojans
Mobile malware
Manipulation of hardware and software
Abuse of computing power of cloud to launch attacks (cybercrime as a service)
Anonymous proxies
Access to device software
Rogue hardware
Alternation of software
Remote activity
Botnets
Remote Command Execution
Targeted attacks
Spectrum Sensing Data Falsification (SSDF) attack
Advanced Persistent Threat (APT)
Backoff attack
Denial of service
Protocol exploitation / Malformed packets / Flooding / Spoofing
DDos
Amplification / reflection methods
Social Engineering
Phishing
Spear Phishing


Threat Details
Threats
Threat Group
Ad-hoc & sensor threats
Threat Group
Threats
Threat Details

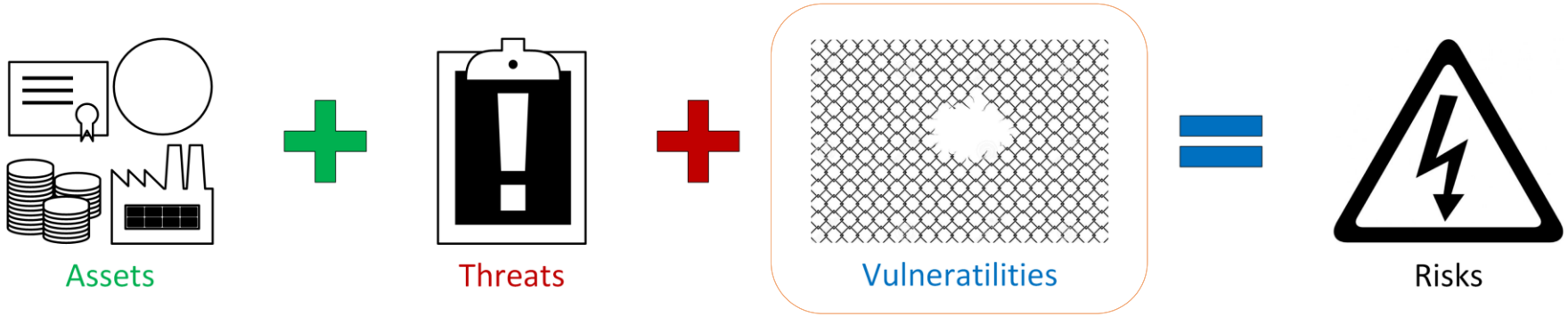
- Eavesdropping/ Interception/ Hijacking
  - Network Reconnaissance
    - Selective forwarding attack
    - Encryption backdoors
  - Interception of information
    - Primary user emulation attack (PUEA)
    - Corporate Espionage
    - Passive Capturing
  - Man in the middle / Session hijacking
    - Relay of messages (or mafia fraud or chess grandmaster problem)



Threat Agents

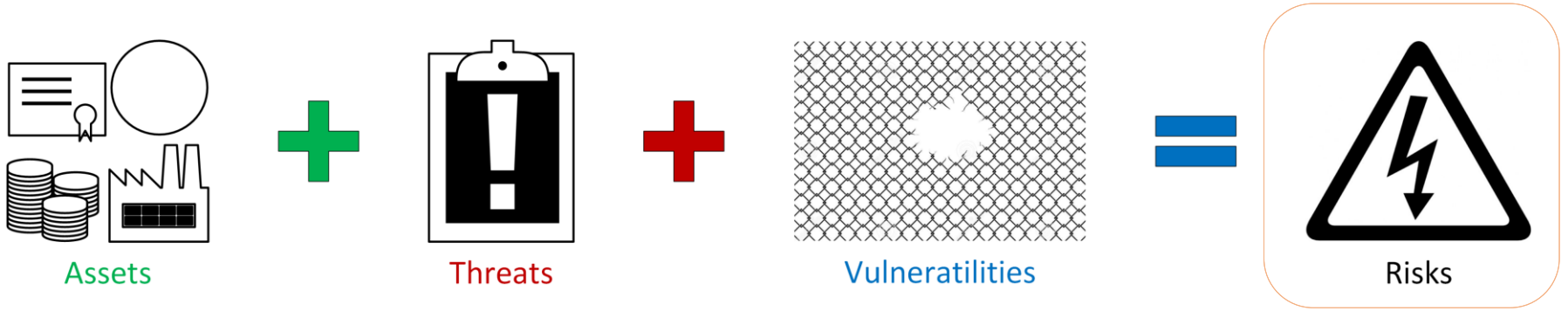
	Motivation	Rationality	Sophistication
CORPORATIONS	Corporate espionage	High	Depends
CYBER CRIMINALS	Financial gain, the hacking itself	Low	High
CYBER TERRORISTS, HACKTIVISTS	Politics, social matters, ideologies	Medium	Medium
SCRIPT KIDDIES	The thrill of danger	Very Low	Low
EMPLOYEES	Unintentional, personal profit	High	High
NATION STATES	Defense, protection of state	High	High
NATURAL DISASTERS	None	None	None

Vulnerabilities and Risks



- Small devices, with low-level of **power independency**
- Devices are scattered in **wide areas**
- **Means** of communication
- Specific **protocol** operations

Vulnerabilities and Risks



Risks

- **Data** loss
- Loss of **devices**
- **Privacy** leakage

Risk Management

- Operational control
- Specialized tools and techniques
- Risk prioritizing, risk data analysis
- Constant monitoring
- Stakeholders feedback and assessment

Good Practices

Categories	Subcategories	Details
Authentication	Specific methods	Authentication methods for **RFID** Point of Sales (**POS**)
Data protection	Cryptography	**Constrained environments** Public key (**Ad-hoc networks**) Symmetric key (**sensor networks**)
	Privacy preservation	**Health data access control**
	Networking	Mechanisms for **horizontal handover** **Dedicated Short-Range Communications (DSRC)** applications
	RFID tags	Secure **disposal** Non-revealing i**dentifier** format
Simulation, visualisation and testing activities	Benchmarking	**Signal** measurement (interference, strength)
	Communication standards	**Overclaiming** and **Misclaiming** Attacks

Good Practices

Categories	Subcategories	Details
Monitoring	Audits, alerts and logs	**Low-power wearable** ECG **monitoring system** for multiple-patient remote monitoring **Resource usage patterns** monitoring
	Physical Access	**Wi-Fi** area RFID tag's **range**
	Detection tools	Remote Intrusion Monitoring (**RIM**)
	Resource related	**Redundant** or **loop** packet transmission avoidance Decreased **power reduction** on nodes **Vampire** attacks prevention **Energy Weight Monitoring** system
	Special nodes	Sensor clusters monitoring (**gNodes**) Traffic throughput in clusters (**cNodes**)

Good Practices

Categories	Subcategories	Details
Management and support	RFID	**Back-end** server **passwords** for tags System **security** of readers and middleware **Secure placement** of tags and readers **Electromagnetic shielded** tunnels **Critical data** identification and access control
	Access Points (AP)	**Channel number** and **power output** configuration **A**void default **SSID** name Maximum **beacon time interval**; announcements of position Prevent **unauthorized** management (i.e. unauthorized **resetting**) Control access of **STAs** (device with a wireless interface)
Specialised tools & techniques	Nodes	**Positioning** of nodes in grid Camouflage or **hide** sensor nodes Frequent change of the **base station**
	Generic	Wireless Intrusion Detection Systems (**WIDS**) Reject unknown received calls/SMS/MMS/e-mails

Good Practices

Categories	Subcategories	Details
Specialised tools & techniques	Routing protocols	**Flat-based/Hierarchical-based/Location-based** **Multipath** MAC Protocol (**S-MAC**, **T-MAC**, **B-MAC** or **G-MAC**) Expected Transmission Count (**ETX**) with **MESH-LINK** protocol **Geographic Routing Protocol** Next Generation Access Control Protocols and API definitions (**NGAC-FA, NGAC-GOADS, INCITS 499, SP 800-178**) **Ariadne** Secure Efficient ad-hoc Distance vector (**SEAD**) Authenticated Routing for ad-hoc Network (**ARAN**)
	RFID	**Radio frequency shielded** sheltering mechanism Tags with a "**press-to-activate**" switch Tag polling in **small time intervals**

Good Practices

Categories	Subcategories	Details
Specialised tools & techniques	Threat-focused	**Lightweight Secure Mechanism**||Path Based **DoS** attacks **Packet Leash**||**wormhole** attacks **Limit** node neighbours||**Sybil** attacks **Spread Spectrum** and **Cryptographic puzzle**||external **Jamming** attacks **End-to-end acknowledgements** and **global time synchronisation**||**Sybil** attack, **massive flood** of replies **Gossiping** algorithms||**collisions** and **messaging costs** Secure **wakeup** and secure **bootstrapping**||**DoS** attacks (sleep deprivation attacks) **Repeated Game Theory** and **Bayesian Game Theory**||**DoS** attacks **Signal strength detection** and **Ant Based Framework**||**DoS** attacks **Distributed** algorithms||**sinkhole** attacks **Randomized Multicast** or **Line-Selected Multicast**||node **replication** attacks

Gap Analysis (1)

Device Domain

- *The **sophistication of attacks** is **greater** than the **level of security** that practices offer*

Network Domain

- *WIDS requires **resources***
- *The **time-period** between the **assessment** and the **deployment/withdrawal** of firmware updates*
- *The standalone characteristics of **routing protocols** are not sufficient for **threat protection***

Application Domain

- *Security patches and updates do not mitigate **zero-day exploits***
- ***Cloud-based applications** cannot be safeguarded due to the **complex backend environment***

Gap Analysis (2)

Operational Domain

- *The **human factor** and the **poor video quality** of surveillance systems*
- ***Physical security** is **limited** when defense-in-depth is implemented*
- ***Fraudulent activities** are addressed only with mechanisms without functional procedures*

Product/Business Processes Domain

- *The **regulations** focus mainly on threats against **data***
- *The **regulations** do not necessarily resolve all the **responsibilities of individuals***
- *The use of **external/customized components** derails **security by design***

Recommendations

Authentication/Authorization

- **Multi-factor** authentication methods (MFA)
- **Certificate-based** authentication
- **Attribute-based** access controls

Proactive Defense

- Orchestration of **WIDS** in every bottleneck
- Continuous **update** of the IDS sensors' **ruleset** in strict time **intervals** and by following **trustful sources** of signatures
- Focus on the **routing protocols** vulnerabilities

Reactive Defense

- A **defense zone** consisting of a ***honeynet***

Thank you!

Questions?

Read more at: DOI 10.2824/58281

contact details

Z. Garofalaki z.garofalaki@unipi.gr
D. Kallergis: d.kallergis@unipi.gr