Integrated cyber-physical security for health services

THE 3S CLUSTERING EVENT
(SATIE, SAFECARE, SecureGas)

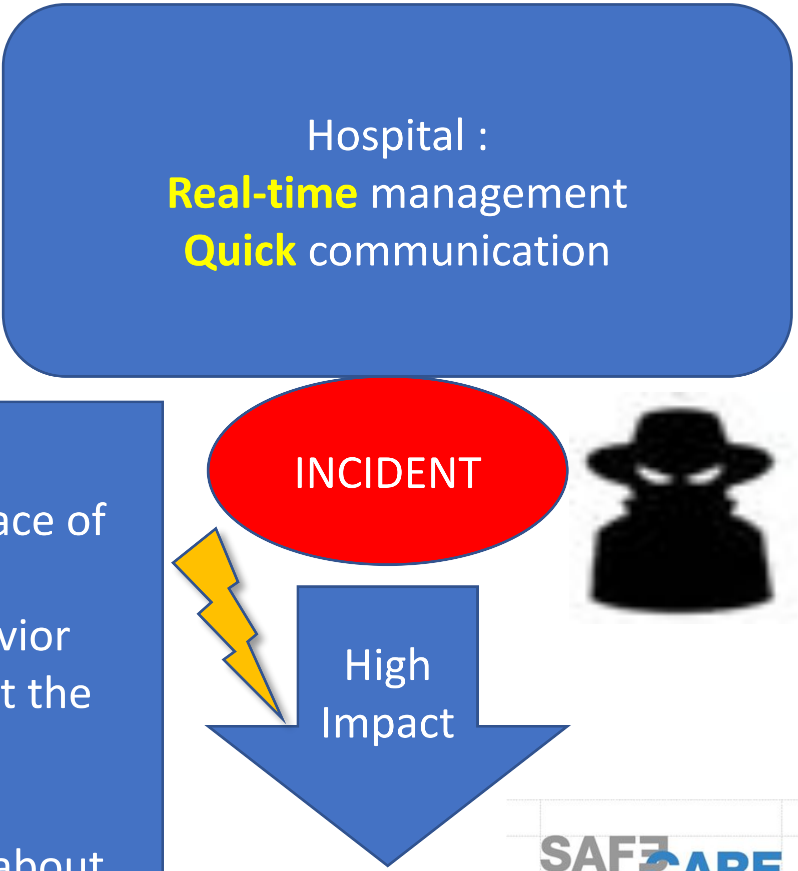
SAFECARE – Risk simulation and process to integrate global protection

2021-10-12/13, 2021

Philippe Tourron - Coordinator

SAFECARE has received funding as part of the “Secure societies – Protecting freedom and security of Europe and its citizens” challenge of the Horizon 2020 Research and Innovation programme of the European Union under grant agreement 787002

Hospital context



Hospital :
Real-time management
Quick communication

INCIDENT

High Impact

SAFECARE
Integrated cyber-physical security for health services

The work is as huge as the surface of health systems

- Detection of malicious behavior
- Emergency measures to limit the threat
- Prepare the repair
- Communicate (information about threat and mitigation) :
  - Between hospitals in a region
  - Between hospitals in a country
  - Between hospitals in Europe …

Paradox of health systems evolution:

- More open (towards patients, towards city medicine, etc.)
- More mobile inside and outside the hospital
- Simpler
- More secure (GDPR)

But…

- Low resources and complex ecosystems

Crisis mode :

- To be as agile as the threat
- To communicate between defensive actors (technical or human) at the speed of attacks to synchronize protection at the scale of a hospital, a territory of a country, a continent?

Needs…

- To understand possible impacts to manage appropriate decisions and…
- To organize preparation and training

Process to be prepared to manage risks

Technical but also managerial and organizational aspects

1 - Critical system(s)

2 - Existing security systems

3 - Organisational structure in place

4 - Crisis management process

RISK ASSESMENT TO UNDERSTAND RISK AND POSSIBLE MITIGATION
What is detected during the kill chain ?

SAFECARE
Integrated cyber-physical security for health services

5 - Map crisis management actors with SAFECARE system's users

6 - New organisational crisis management (assessment of human impacts and ethics point of view)

7 - Specific knowledge to adapt the impact propagation calculation

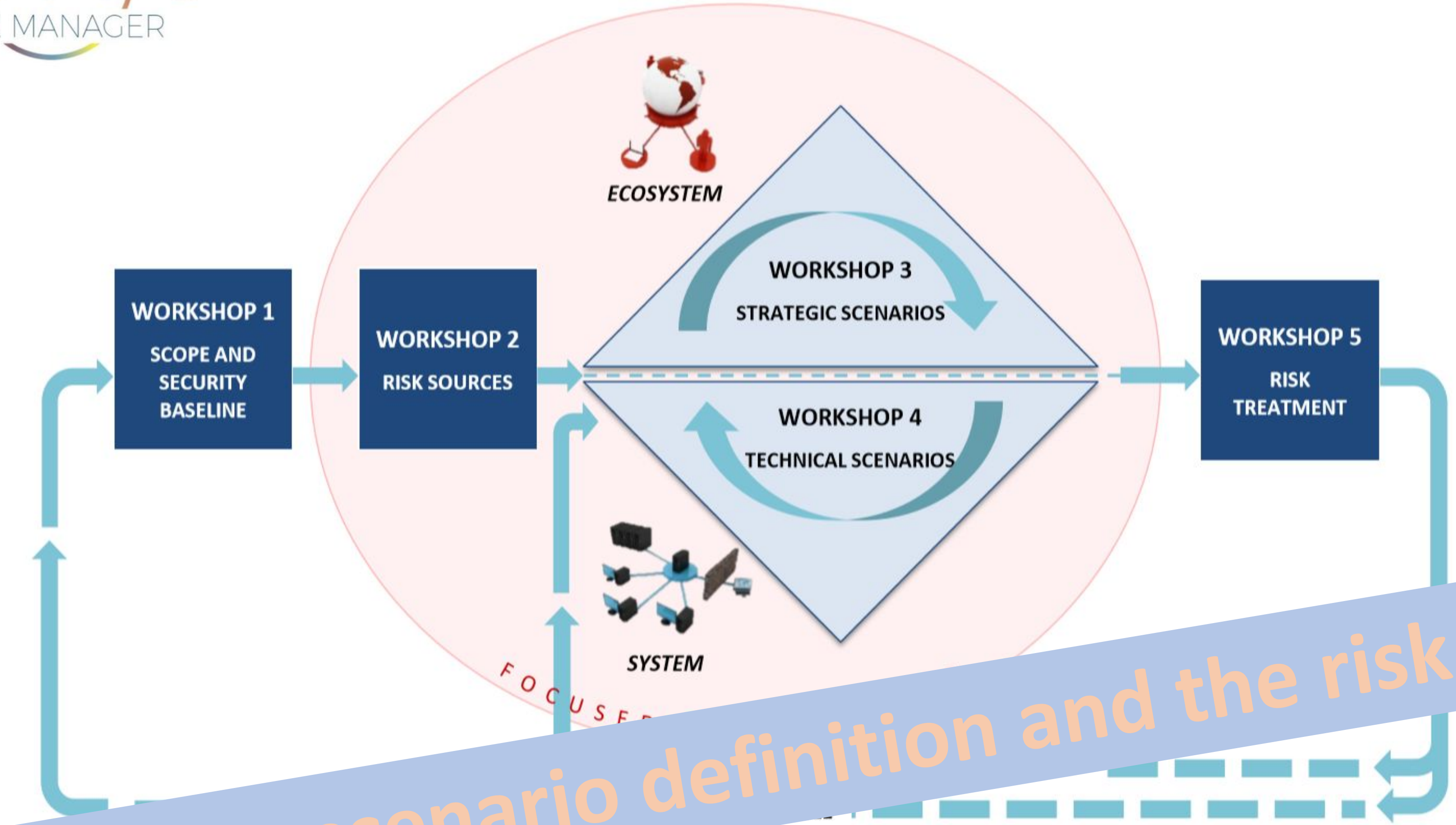
8 – Understanding complete safecare tools and global process
Training future system users -

Training guide, training HAMS, role play (with EBIOS RM/Bowtie methodology and Safecare tools) …

Risk Assessment

EBIOS RISK MANAGER

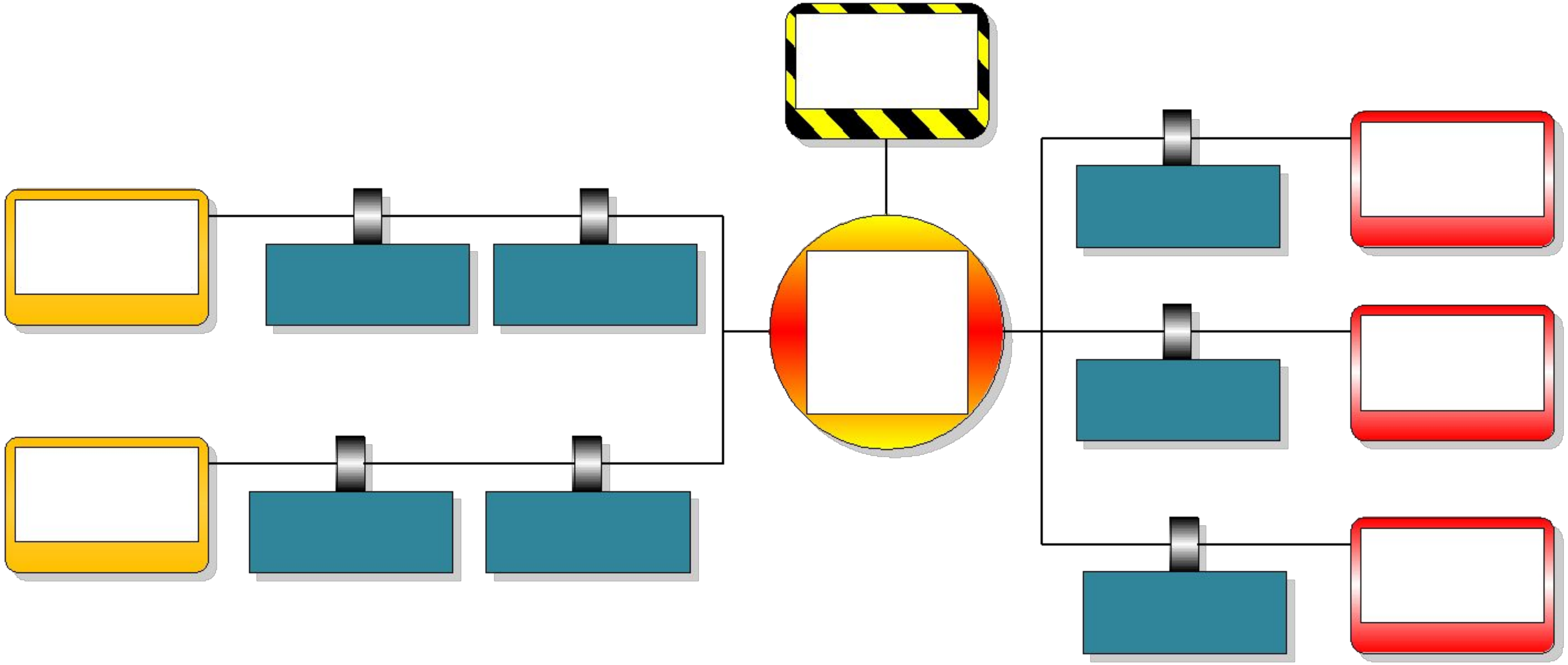
Expression of Needs and Identification of Security Objectives



SAFECARE
Integrated cyber-physical security for health services

Both for the scenario definition and the risk assessment

BowTie to map measures (existing and new ones)

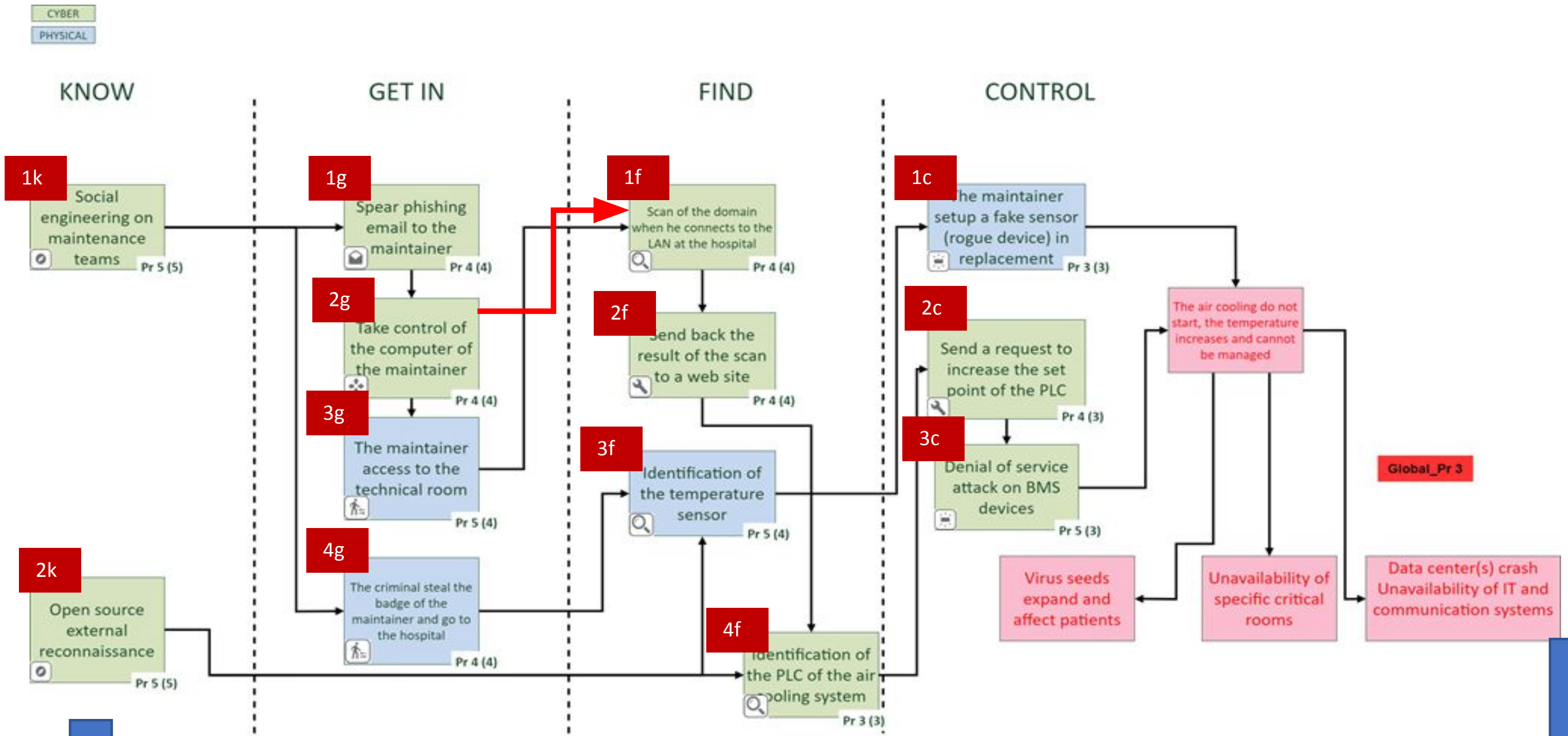


SAFECARE

Integrated cyber-physical security for health services

Risk assessment methodology

The risk assessment (Example with non representative data)



CYBER

PHYSICAL

KNOW

GET IN

FIND

CONTROL

1k Social engineering on maintenance teams Pr 5 (5)

2k Open source external reconnaissance Pr 5 (5)

1g Spear phishing email to the maintainer Pr 4 (4)

2g Take control of the computer of the maintainer Pr 4 (4)

3g The maintainer access to the technical room Pr 5 (4)

4g The criminal steal the badge of the maintainer and go to the hospital Pr 4 (4)

1f Scan of the domain when he connects to the LAN at the hospital Pr 4 (4)

2f end back the result of the scan to a web site Pr 4 (4)

3f ldentification of the temperature sensor Pr 5 (4)

4f ientification of the PLC of the air oling system Pr 3 (3)

1c he maintainer setup a fake sensor (rogue device) in replacement Pr 3 (3)

2c Send a request to increase the set point of the PLC Pr 4 (3)

3c Denial of service attack on BMS devices Pr 5 (3)

The air cooling do not start, the temperature increases and cannot be managed

Virus seeds expand and affect patients

Unavailability of specific critical rooms

Data center(s) crash Unavailability of IT and communication systems

Global_Pr 3

Which supporting assets ?

Which vulnérabilities ?

Which incidents ?

On which supporting assets ?

Which Impacts on which primary assets (critical/business values)

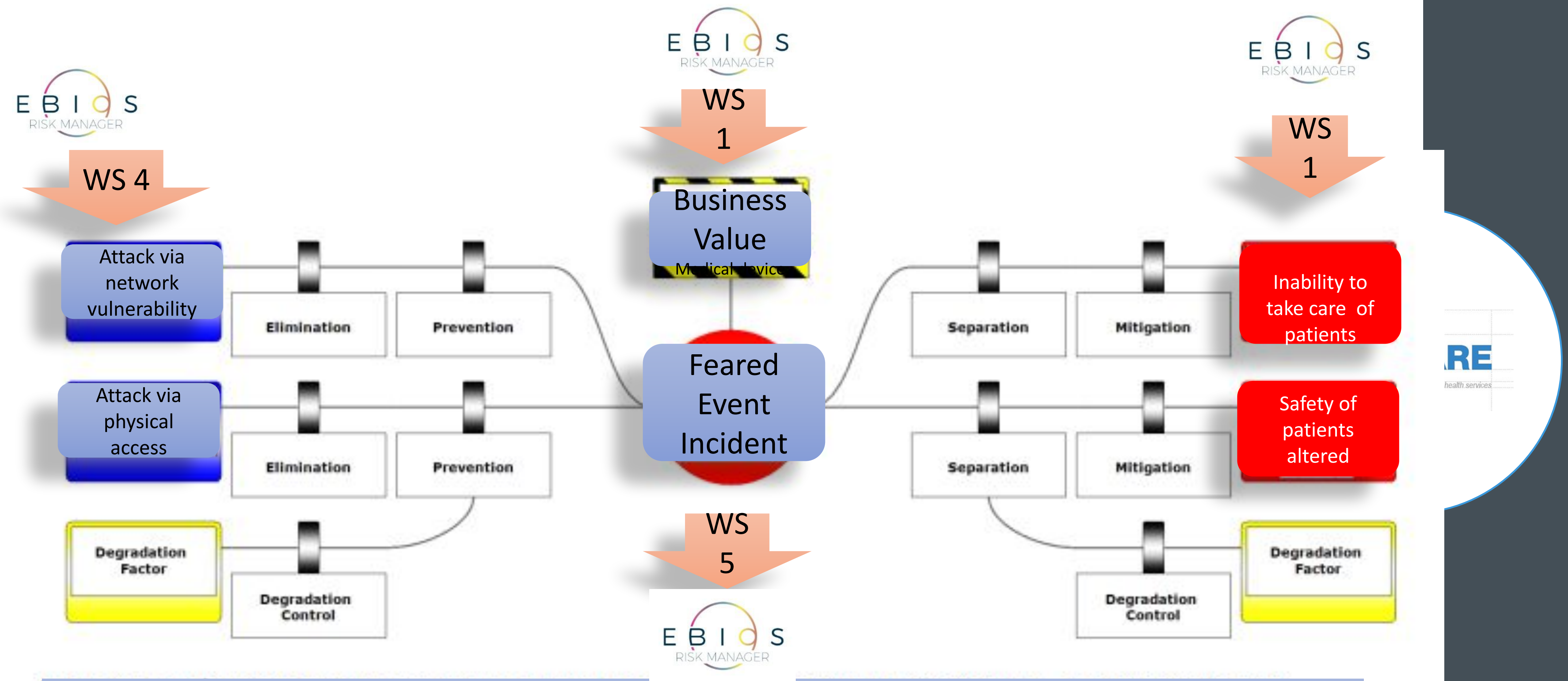
Scenarios : a representative sample of the complexity

- Sc1: Cyber-physical attack targeting **power supply** of the hospital
- Sc2: Cyber-physical attack to steal **patient data** in the hospital
- Sc3: Cyber-physical attack targeting **IT systems**
- Sc4: Cyber-physical attack to cause a **hardware fault**
- Sc5: Cyber-physical attack targeting the **air-cooling system** of the hospital
- Sc6: Cyber-physical attack on **medical devices**
- Sc7: Cyber-physical attack to **steal credentials** to access IT systems
- Sc8: Cyber-Physical attack in access control provider to **steal medical devices**
- Sc9: Physical attack against hospital staff using a **gun**
- Sc10: Physical attack **to steal drugs**
- Sc11: Cyber-physical attack due to a **personal laptop**
- Sc12: Cyber-physical attack to **block national crisis management**

SAFECARE

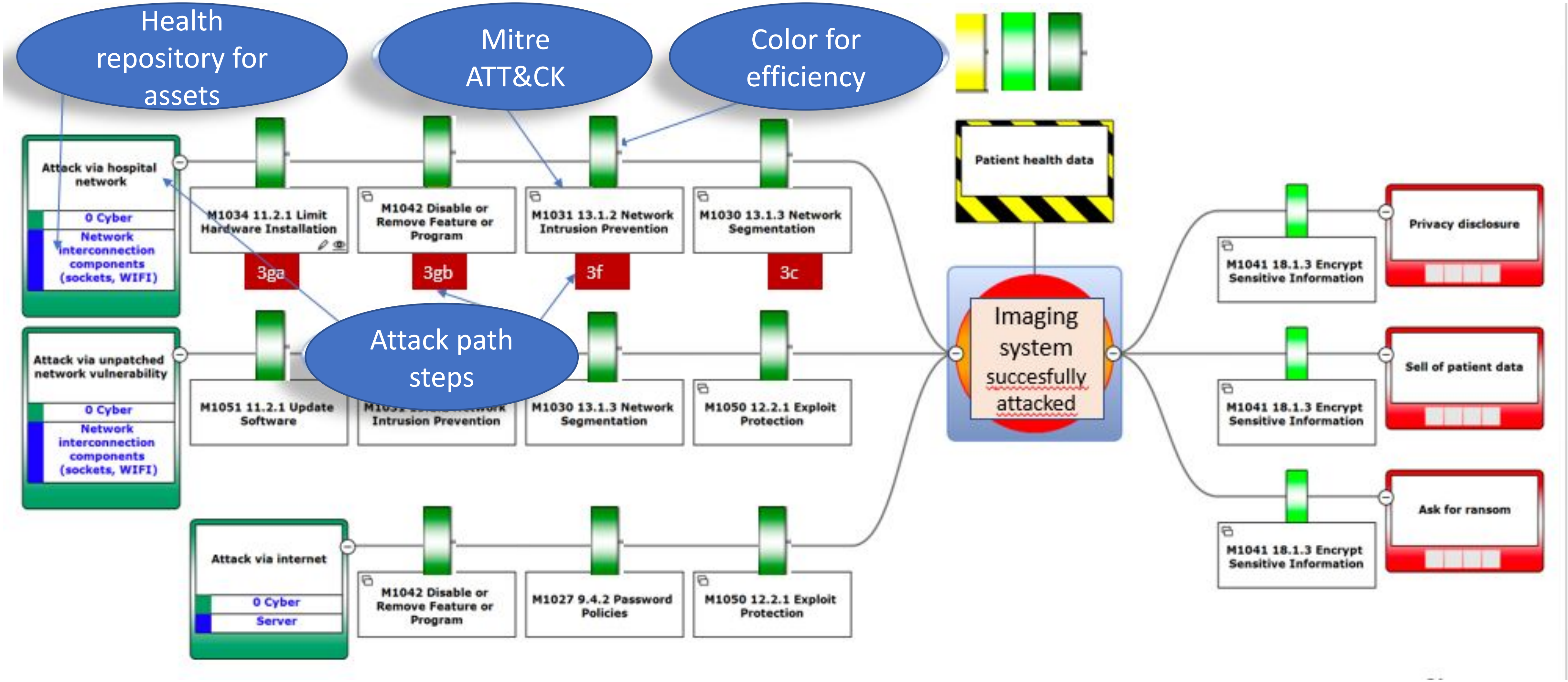
Integrated cyber-physical security for health services

Risk Assessment - Ebios RM Combined with BowTie



To facilitate mesures and controls identification (existing and new ones) and links with degradation (or improvement) factors

Example with links to standards and repositories

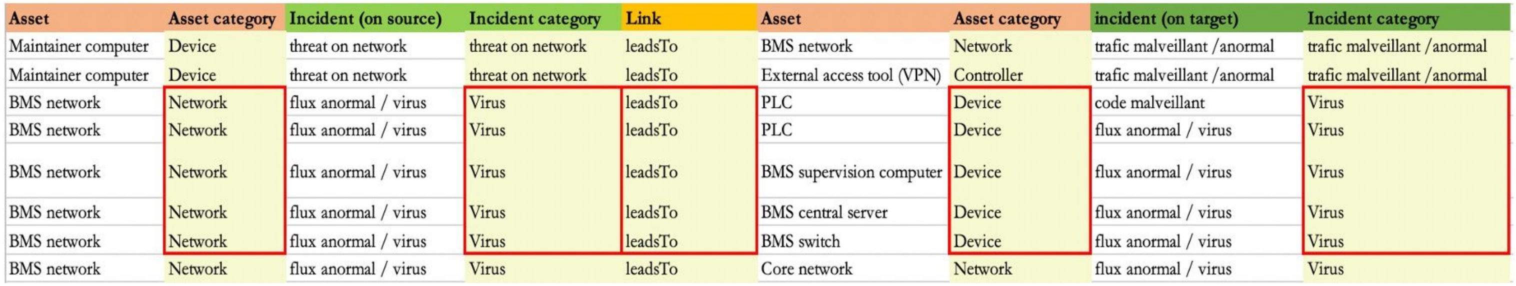

Health repository for assets
Mitre ATT&CK
Color for efficiency
Attack path steps
Attack via hospital network
0 Cyber
Network interconnection components (sockets, WIFI)
M1034 11.2.1 Limit Hardware Installation
M1042 Disable or Remove Feature or Program
M1031 13.1.2 Network Intrusion Prevention
M1030 13.1.3 Network Segmentation
3ga
3gb
3f
3c
Attack via unpatched network vulnerability
0 Cyber
Network interconnection components (sockets, WIFI)
M1051 11.2.1 Update Software
M1031 13.1.2 Network Intrusion Prevention
M1030 13.1.3 Network Segmentation
M1050 12.2.1 Exploit Protection
Attack via internet
0 Cyber
Server
M1042 Disable or Remove Feature or Program
M1027 9.4.2 Password Policies
M1050 12.2.1 Exploit Protection
Patient health data
Imaging system succesfully attacked
M1041 18.1.3 Encrypt Sensitive Information
Privacy disclosure
M1041 18.1.3 Encrypt Sensitive Information
Sell of patient data
M1041 18.1.3 Encrypt Sensitive Information
Ask for ransom

Ontology based incidents propagation: Propagation rules and impact scores *(source Cnam paris)*

SAFECARE

Integrated cyber-physical security for health services

(1) Knowledge acquisition (tables of knowledge)

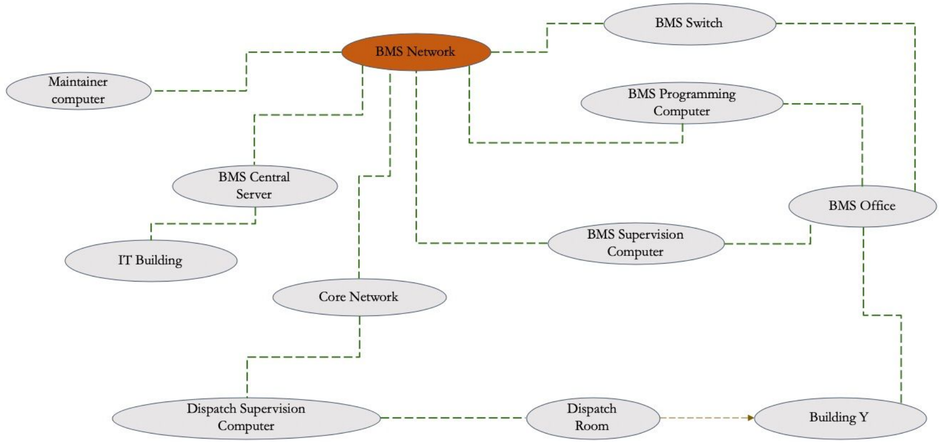


Asset	Asset category	Incident (on source)	Incident category	Link	Asset	Asset category	incident (on target)	Incident category
Maintainer computer	Device	threat on network	threat on network	leadsTo	BMS network	Network	trafic malveillant /anormal	trafic malveillant /anormal
Maintainer computer	Device	threat on network	threat on network	leadsTo	External access tool (VPN)	Controller	trafic malveillant /anormal	trafic malveillant /anormal
BMS network	Network	flux anormal / virus	Virus	leadsTo	PLC	Device	code malveillant	Virus
BMS network	Network	flux anormal / virus	Virus	leadsTo	PLC	Device	flux anormal / virus	Virus
BMS network	Network	flux anormal / virus	Virus	leadsTo	BMS supervision computer	Device	flux anormal / virus	Virus
BMS network	Network	flux anormal / virus	Virus	leadsTo	BMS central server	Device	flux anormal / virus	Virus
BMS network	Network	flux anormal / virus	Virus	leadsTo	BMS switch	Device	flux anormal / virus	Virus
BMS network	Network	flux anormal / virus	Virus	leadsTo	Core network	Network	flux anormal / virus	Virus

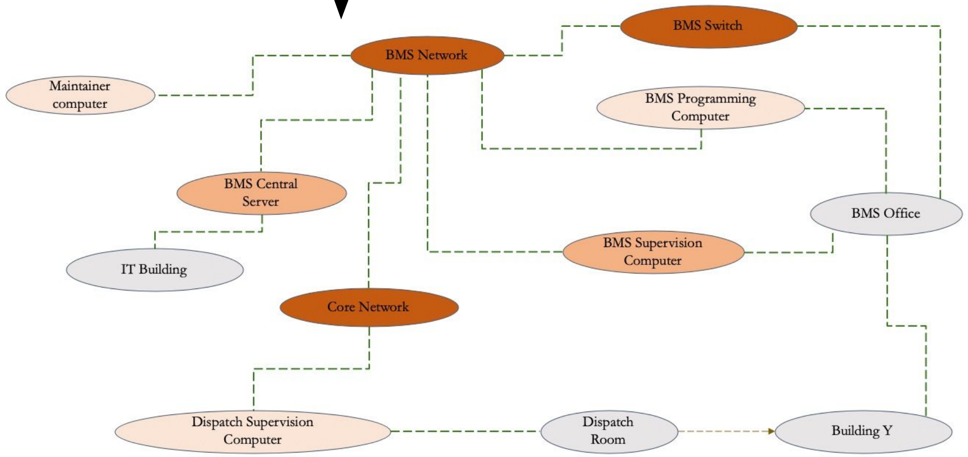
(2) Propagation rules generation

isImpacted(asset2), hasIncident(asset2, incident) :-
    hasIncident(asset1, incident), Network(asset1), Virus(incident),
    leadsToCP(asset1, controlPoint), leadsToAsset(controlPoint, asset2),
Device(asset2)

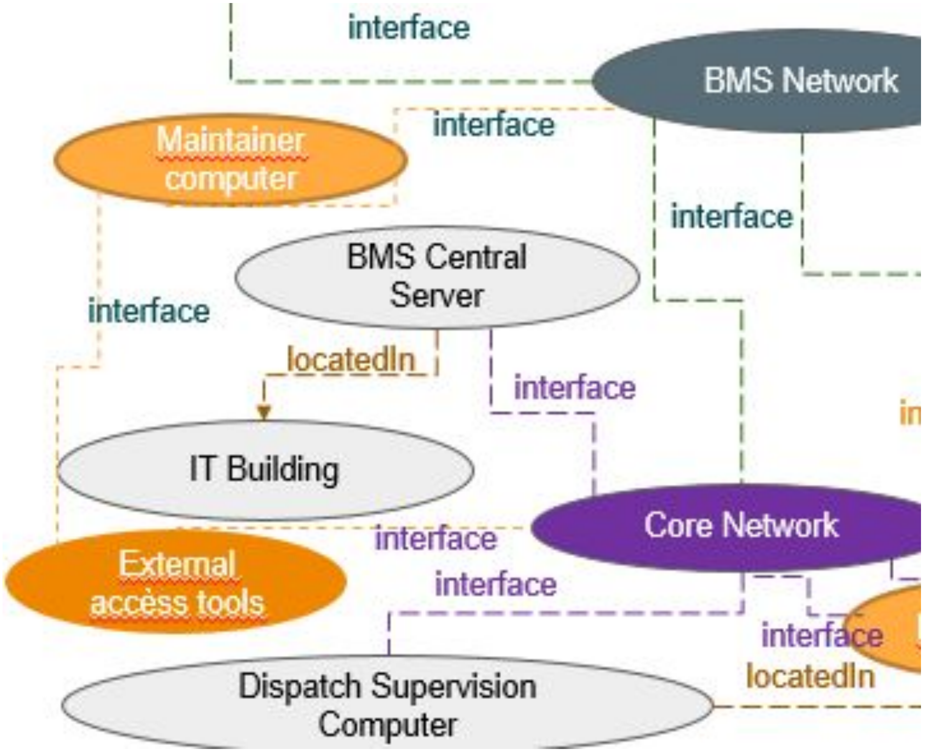
(3) Impact propagation



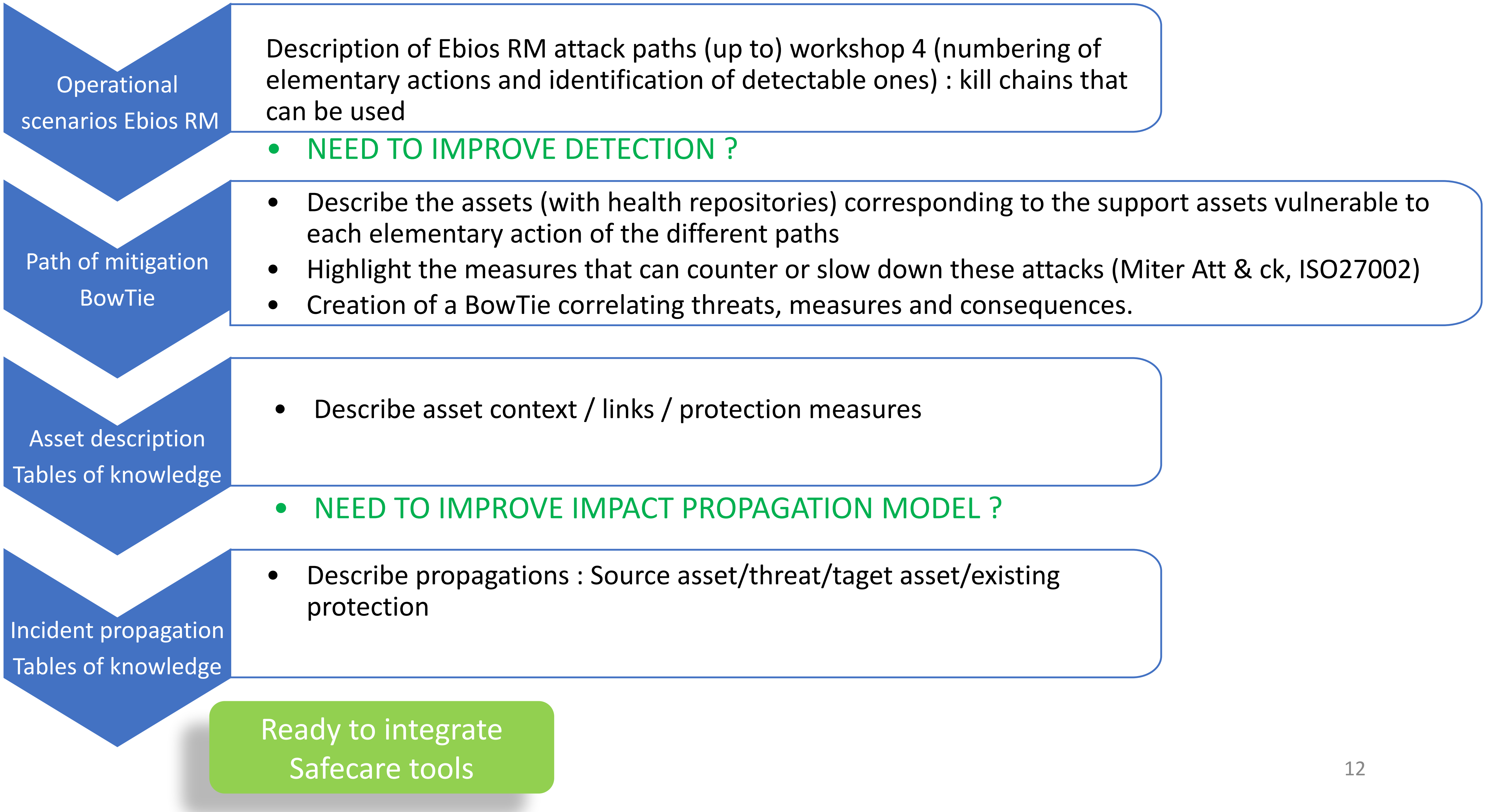
(4) Impact score evaluation



Assets map (from table of knowledge to map)



SAFECARE Step by step



Operational scenarios Ebios RM

Description of Ebios RM attack paths (up to) workshop 4 (numbering of elementary actions and identification of detectable ones) : kill chains that can be used

- NEED TO IMPROVE DETECTION ?

Path of mitigation BowTie

- Describe the assets (with health repositories) corresponding to the support assets vulnerable to each elementary action of the different paths
- Highlight the measures that can counter or slow down these attacks (Miter Att & ck, ISO27002)
- Creation of a BowTie correlating threats, measures and consequences.

Asset description Tables of knowledge

- Describe asset context / links / protection measures

- NEED TO IMPROVE IMPACT PROPAGATION MODEL ?

Incident propagation Tables of knowledge

- Describe propagations : Source asset/threat/taget asset/existing protection

Ready to integrate Safecare tools

Bibliography

SAFECARE: https://www.safecare-project.eu

EBIOS Risk Manager: https://www.ssi.gouv.fr/entreprise/management-du-risque/la-methode-ebios-risk-manager/

Club EBIOS generic approach: https://club-ebios.org/site/ebios-lapproche-generique/

MITRE ATT&CK: https://attack.mitre.org/

ISO 27002: https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-2:v1:fr

BowTieXp: https://www.cgerisk.com/products/bowtiexp/