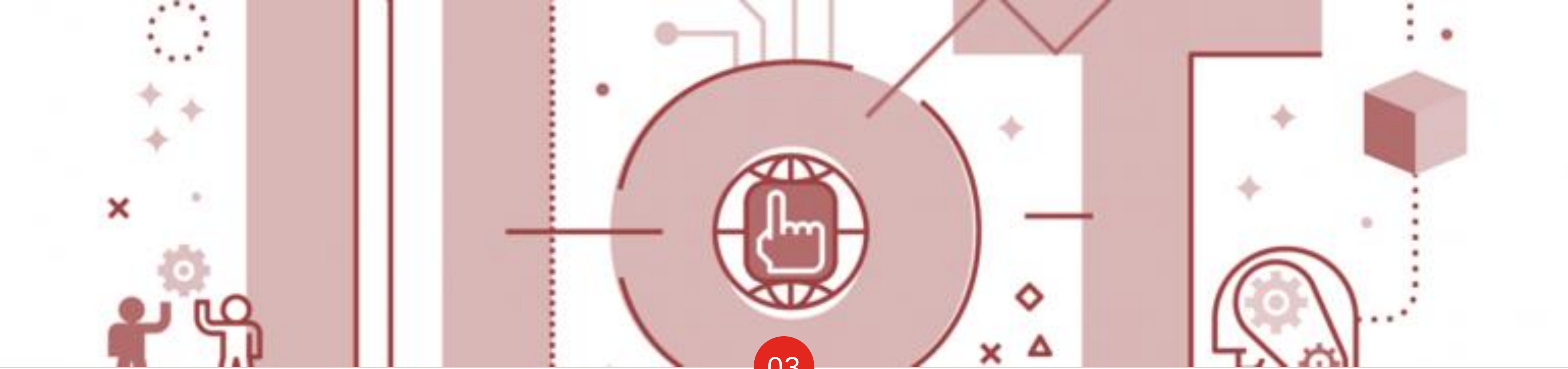
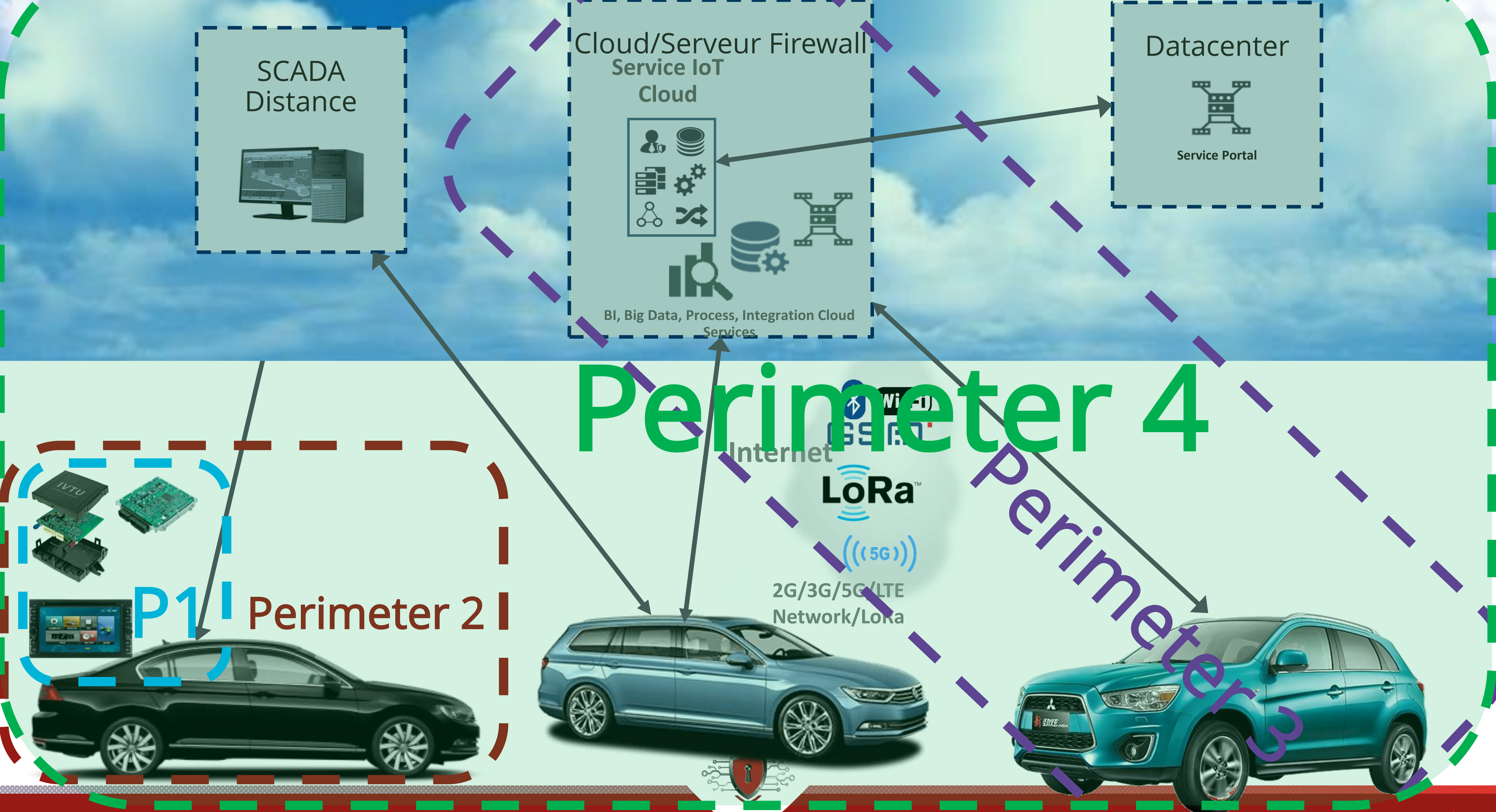
RED ALERT LABS
IoT Security

INTERNET OF THINGS (IOT)
BRINGING TRUST TO THE INTERNET OF THINGS



03

INDUSTRIAL USE CASE: AUTOMOTIVE



SCADA Distance

Cloud/Serveur Firewall

Service IoT Cloud

BI, Big Data, Process, Integration Cloud Services

Datacenter

Service Portal

Perimeter 4

Internet

LoRa

2G/3G/5G/LTE Network/LoRa

P1

Perimeter 2

Perimeter 3

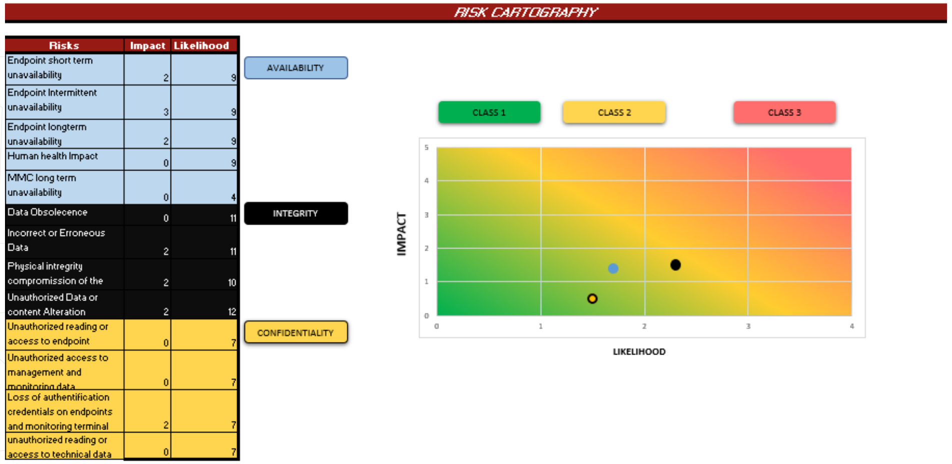
WHICH SOLUTIONS / TOOLS FOR WHAT KIND OF ACTOR?

03 **SOLUTION 1:** BUSINESS RISK TOOL IN IoT

Output tool

Dashboard including:

- ❑ The level of **the projects sensitivity**,
- ❑ **Risk mapping**,
- ❑ The **impact categories** (example: financial, brand image …)
- ❑ The **measures** and **strategic actions** to be put in place to ensure adequate coverage of identified residual risks



RISK CARTOGRAPHY

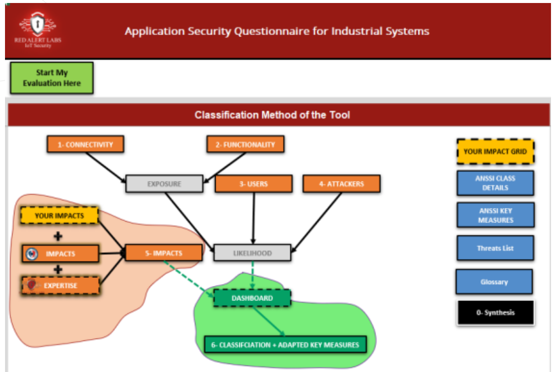
Risks	Impact	Likelihood
Endpoint short term unavailability	2	9
Endpoint Intermittent unavailability	3	9
Endpoint longterm unavailability	2	9
Human health Impact	0	9
MMC long term unavailability	0	4
Data Obsolecence	0	11
Incorrect or Erroneous Data	2	11
Physical intregrity compromission of the	2	10
Unauthorized Data or content Alteration	2	12
Unauthorized reading or access to endpoint	0	7
Unauthorized access to management and monitoring data	0	7
Loss of authentification credentials on endpoints and monitoring terminal	2	7
unauthorized reading or access to technical data	0	7

Audience

- ❑ Business-line / risk-owners, project manager, security managers (example: CISO), architects.

Properties of the offered tool

- ❑ Format: Excel file,
- ❑ **Interactive** and **customizable** tool (customer brand and dashboard content)
- ❑ Possible extension: tool for **extracting** and **consolidating** results for **project management.**



Application Security Questionnaire for Industrial Systems

Classification Method of the Tool

WHICH SOLUTIONS / TOOLS FOR WHAT KIND OF ACTOR?

03

SOLUTION 1: BUSINESS RISK TOOL IN IoT

Target

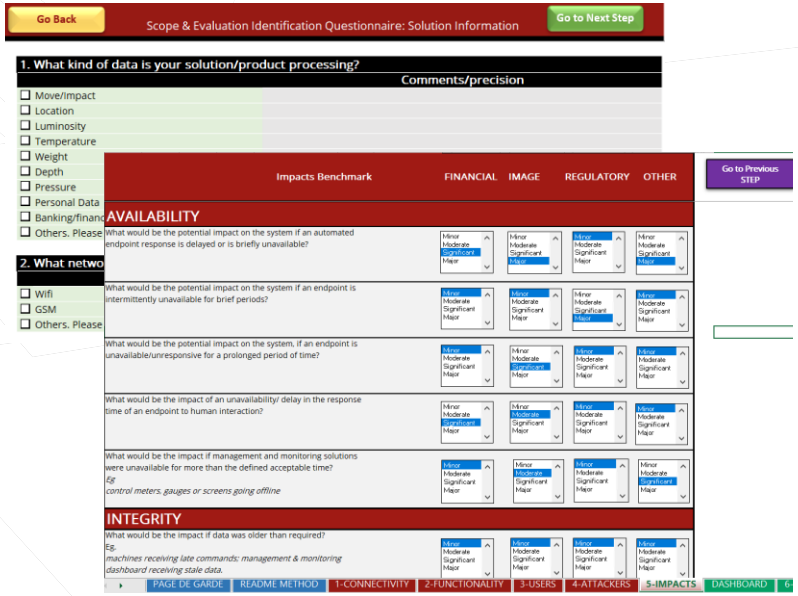
- ❑ **Companies benefiting** from IoT solutions (example: Bolloré Group, EDF …)
- ❑ **Manufacturers** and **developers** of IoT solutions (Example: Peugeot, VEOLIA, …)
- ❑ **Consultants** and **integrators** of IoT solutions (Example: ATOS, EY, Wipro …)

Time required for delivery

T0 + 2 weeks or **T0=** the day of reception of the inputs of the benefit/Services)

Input benefit

- ❑ Answers to a **questionnaire of a technical framework** of the solution /IoT product
- ❑ **Customer's** business **impact** scale



Scope & Evaluation Identification Questionnaire: Solution Information

1. What kind of data is your solution/product processing?

Comments/precision

- ☐ Move/Impact
- ☐ Location
- ☐ Luminosity
- ☐ Temperature
- ☐ Weight
- ☐ Depth
- ☐ Pressure
- ☐ Personal Data
- ☐ Banking/financ
- ☐ Others. Please

2. What netwo

- ☐ Wifi
- ☐ GSM
- ☐ Others. Please

Impacts Benchmark	FINANCIAL	IMAGE	REGULATORY	OTHER
AVAILABILITY				
What would be the potential impact on the system if an automated endpoint response is delayed or is briefly unavailable?	Significant	Major	Minor	Major
What would be the potential impact on the system if an endpoint is intermittently unavailable for brief periods?	Minor	Minor	Major	Minor
What would be the potential impact on the system, if an endpoint is unavailable/unresponsive for a prolonged period of time?	Minor	Significant	Minor	Minor
What would be the impact of an unavailability/ delay in the response time of an endpoint to human interaction?	Significant	Moderate	Minor	Minor
What would be the impact if management and monitoring solutions were unavailable for more than the defined acceptable time? *Eg* *control meters, gauges or screens going offline*	Minor	Moderate	Minor	Significant
INTEGRITY				
What would be the impact if data was older than required? Eg. *machines receiving late commands; management & monitoring dashboard receiving stale data.*	Minor	Minor	Minor	Minor

WHICH SOLUTIONS / TOOLS FOR WHAT KIND OF ACTOR?

03

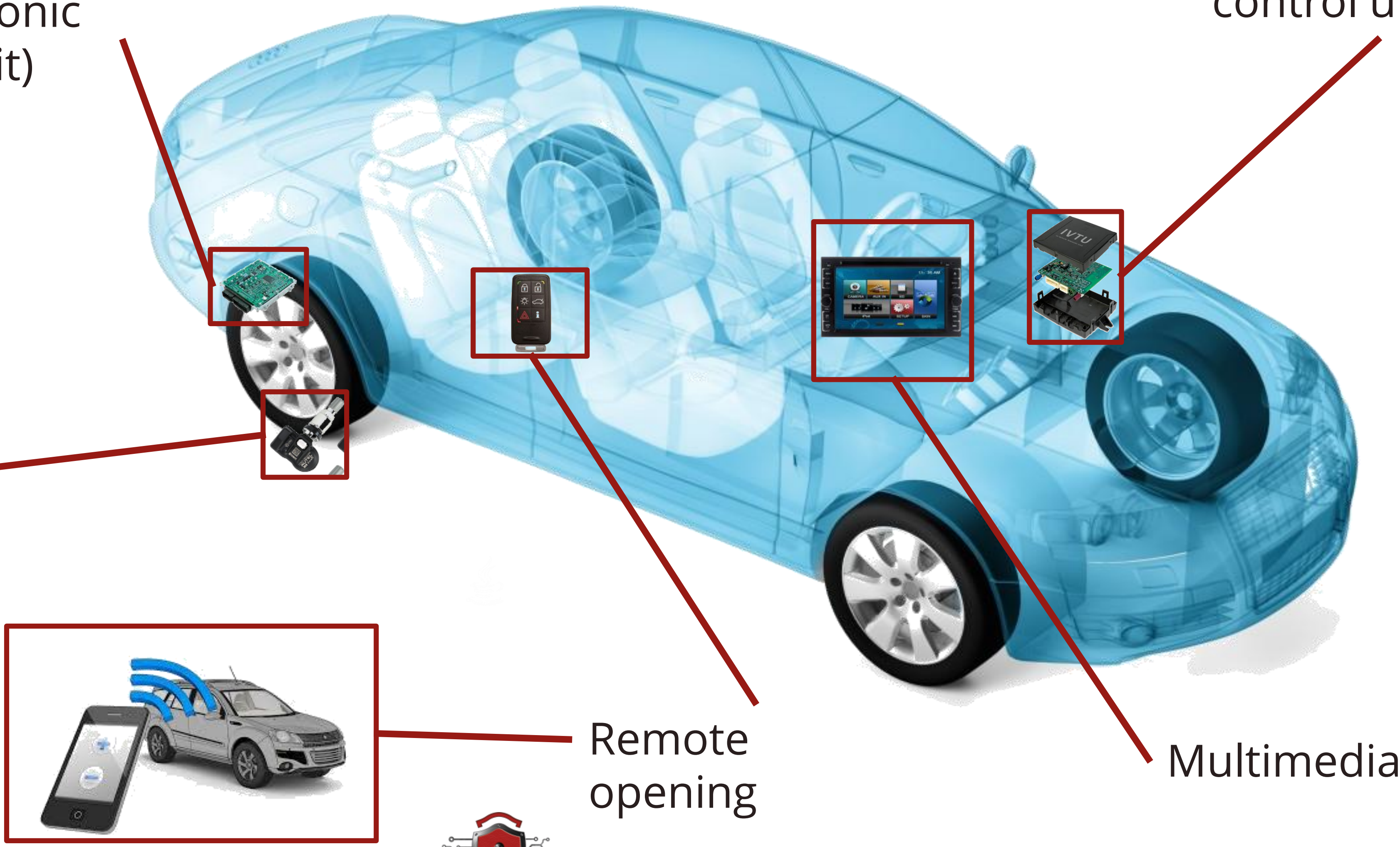
SOLUTION 1: BUSINESS RISK TOOL IN IoT

	BASIC SOLUTION		OUR SOLUTION	
SPECIALIZED EXPERTISE	• **No homogeneous** methodology, • **No IoT specialization**	🪫	• **Homogeneous** methodology • **IoT-oriented** methodology	🔋
RISKS	• **No participation of the business lines in identifying the impacts** • **No business-line support or awareness**	🪫	• **Involvement of decision-makers /businesses since the identification phase of the impact(s)** • **Direct support** and **awareness** for businesses	🔋
ACCESS / TIME TO MARKET	• **No simple and effective** way to have inputs **for a business plan**	🪫	• The results of the tool allow to establish **a bus plan** based on a **risk approach in less than two h**	🔋
COSTS	• **Risk analysis** in an **automatic way (expensive costs)**	🪫	• **Prioritization of actions depending on the projects sensitivity** • **Cost cut related to risk analysis or lost opportunities more than 30%**	🔋

03

WHICH SOLUTIONS / TOOLS FOR WHAT KIND OF ACTOR?

SOLUTION 2 : SECURITY PROFILE/ PERIMETER



ECU (Electronic Control Unit)

Telematics control unit

Tire sensor

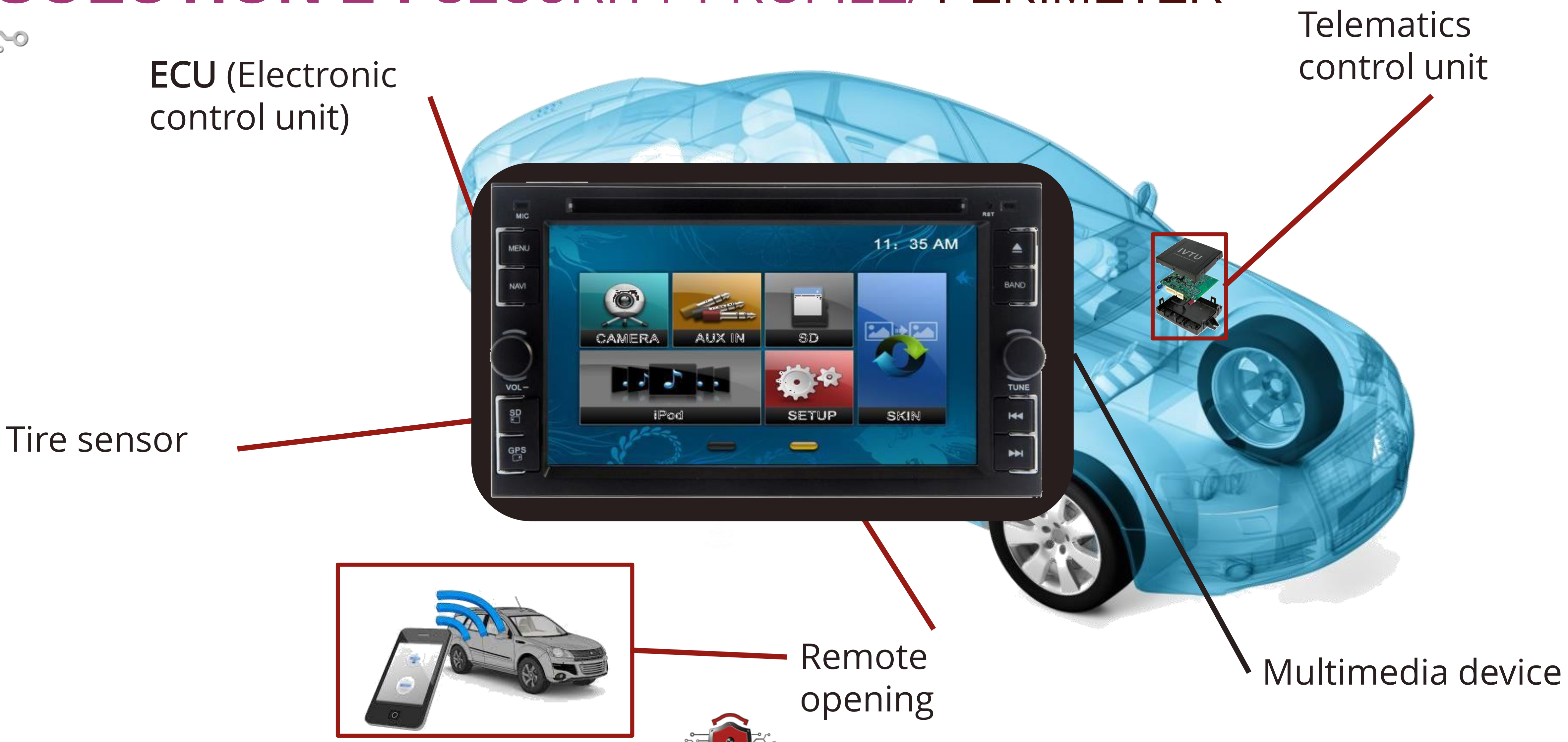
Remote opening

Multimedia device

03

WHICH SOLUTIONS / TOOLS FOR WHAT KIND OF ACTOR?

SOLUTION 2 : SECURITY PROFILE/ PERIMETER



03

WHICH SOLUTIONS / TOOLS FOR WHAT KIND OF ACTOR?

SOLUTION 2 : SECURITY PROFILE/

Output solution

For a **product category** in a **specific environment** (example: connected camera, telematics product)

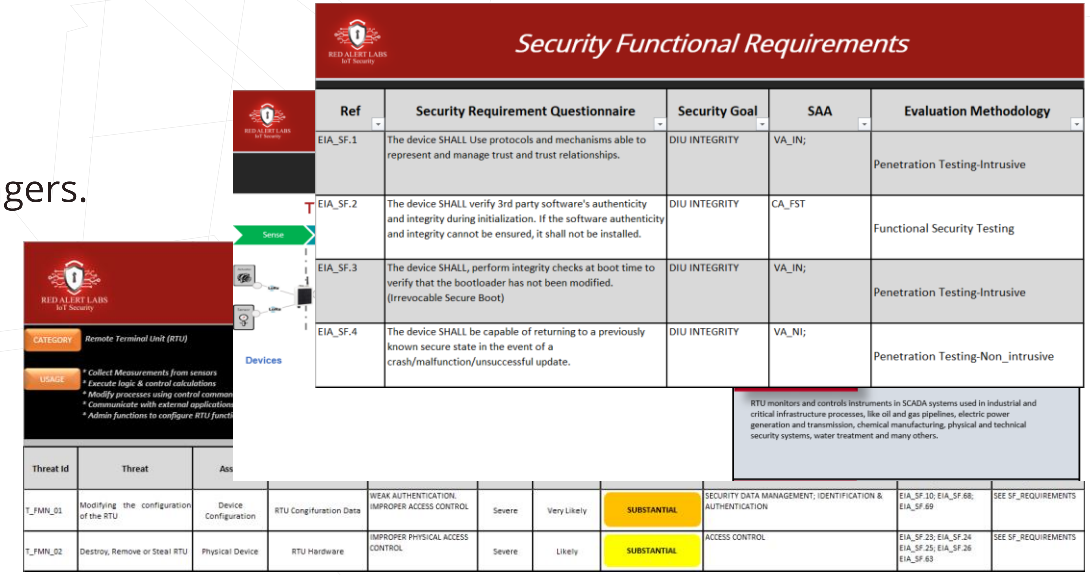
- ❑ Catalog of Security **Functional** Requirements
- ❑ Catalog of **organizational security** requirements (policies, processes ...)
- ❑ Catalog of security **assurance** requirements (verification rules, audits, documentation, ...)

Audience

- ❑ Developers, Procurement, architects, project managers, security managers.

Properties of the proposed solution:

- ❑ Format: Excel file
- ❑ Possible extension: dashboard including mapping for existing security standards



Security Functional Requirements

Ref	Security Requirement Questionnaire	Security Goal	SAA	Evaluation Methodology
EIA_SF.1	The device SHALL Use protocols and mechanisms able to represent and manage trust and trust relationships.	DIU INTEGRITY	VA_IN;	Penetration Testing-Intrusive
EIA_SF.2	The device SHALL verify 3rd party software's authenticity and integrity during initialization. If the software authenticity and integrity cannot be ensured, it shall not be installed.	DIU INTEGRITY	CA_FST	Functional Security Testing
EIA_SF.3	The device SHALL, perform integrity checks at boot time to verify that the bootloader has not been modified. (Irrevocable Secure Boot)	DIU INTEGRITY	VA_IN;	Penetration Testing-Intrusive
EIA_SF.4	The device SHALL be capable of returning to a previously known secure state in the event of a crash/malfunction/unsuccessful update.	DIU INTEGRITY	VA_NI;	Penetration Testing-Non_intrusive

CATEGORY *Remote Terminal Unit (RTU)*

USAGE
** Collect Measurements from sensors*
** Execute logic & control calculations*
** Modify processes using control comman*
** Communicate with external applications*
** Admin functions to configure RTU functi*

RTU monitors and controls instruments in SCADA systems used in industrial and critical infrastructure processes, like oil and gas pipelines, electric power generation and transmission, chemical manufacturing, physical and technical security systems, water treatment and many others.

Threat Id	Threat	Ass								
T_FMN_01	Modifying the configuration of the RTU	Device Configuration	RTU Congifuration Data	WEAK AUTHENTICATION. IMPROPER ACCESS CONTROL	Severe	Very Likely	SUBSTANTIAL	SECURITY DATA MANAGEMENT; IDENTIFICATION & AUTHENTICATION	EIA_SF.10; EIA_SF.68; EIA_SF.69	SEE SF_REQUIREMENTS
T_FMN_02	Destroy, Remove or Steal RTU	Physical Device	RTU Hardware	IMPROPER PHYSICAL ACCESS CONTROL	Severe	Likely	SUBSTANTIAL	ACCESS CONTROL	EIA_SF.23; EIA_SF.24 EIA_SF.25; EIA_SF.26 EIA_SF.63	SEE SF_REQUIREMENTS

03

WHICH SOLUTIONS / TOOLS FOR WHAT KIND OF ACTOR?

SOLUTION 2 : SECURITY PROFILE/

Target

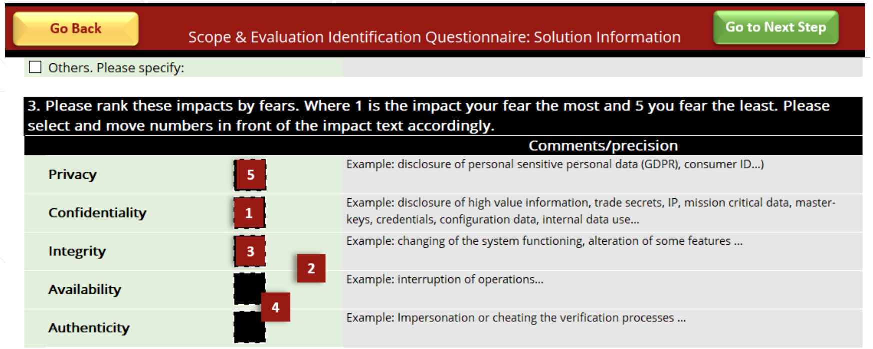
- ❑ **Companies benefiting** from IoT solutions (example: Bolloré Group, EDF ...)
- ❑ **Manufacturers and developers** of IoT solutions (Example: Peugeot, VEOLIA, ...)
- ❑ **Consultants and integrators** of IoT solutions (Example: ATOS, EY, Wipro ...)

Time required for delivery

T0 + 2 weeks or **T0=** the day of receipt of input service

Input service

Answers to a **generic questionnaire** about IoT solution / the product



Scope & Evaluation Identification Questionnaire: Solution Information

☐ Others. Please specify:

3. Please rank these impacts by fears. Where 1 is the impact your fear the most and 5 you fear the least. Please select and move numbers in front of the impact text accordingly.

			Comments/precision
Privacy	5		Example: disclosure of personal sensitive personal data (GDPR), consumer ID...)
Confidentiality	1		Example: disclosure of high value information, trade secrets, IP, mission critical data, master-keys, credentials, configuration data, internal data use...
Integrity	3		Example: changing of the system functioning, alteration of some features ...
Availability		2	Example: interruption of operations...
Authenticity		4	Example: Impersonation or cheating the verification processes ...

03

WHICH SOLUTIONS/TOOLS FOR WHICH ACTORS?

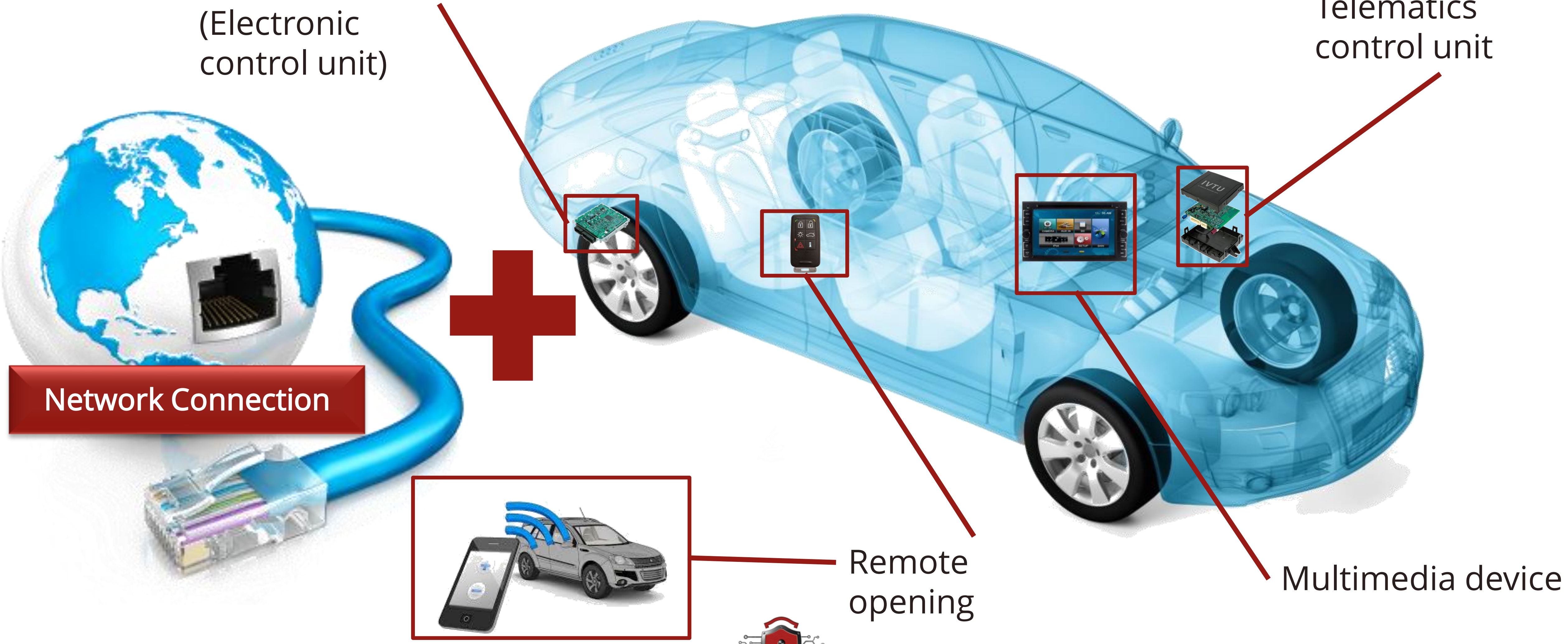
SOLUTION 2: SECURITY PROFILE

	BASIC SOLUTION	OUR SOLUTION
SPECIALIZED EXPERTISE	Limited to security requirements	Contains **assurance requirements**
RISKS	• Non existing security specifications/Framework? or merged with functional specifications • Unclear communication with stakeholders	• Complete **security specifications/Framework?** to be aimed for several actors in particular **buyers/procurement team.** • **Facilitates communication with stakeholders**
ACCÈS / TIME TO MARKET	• Time-consuming risk analysis • Complex content for reading • Content not easy to maintain especially towards standards and certifications	• **Quick solution (5 to 12 days)** • **Simple content to read** • **Easy to map to existing standards** • **Gives access to certifications**
COSTS	Risk analysis in an automatic way (costly)	**Reduce costs** by **more than 60%**

03

WHICH SOLUTIONS/TOOLS FOR WHICH ACTORS?

SOLUTION 3: INDEPENDENT EVALUATION LABORATORY/ PERIMETER



ECU (Electronic control unit)

Telematics control unit

Network Connection

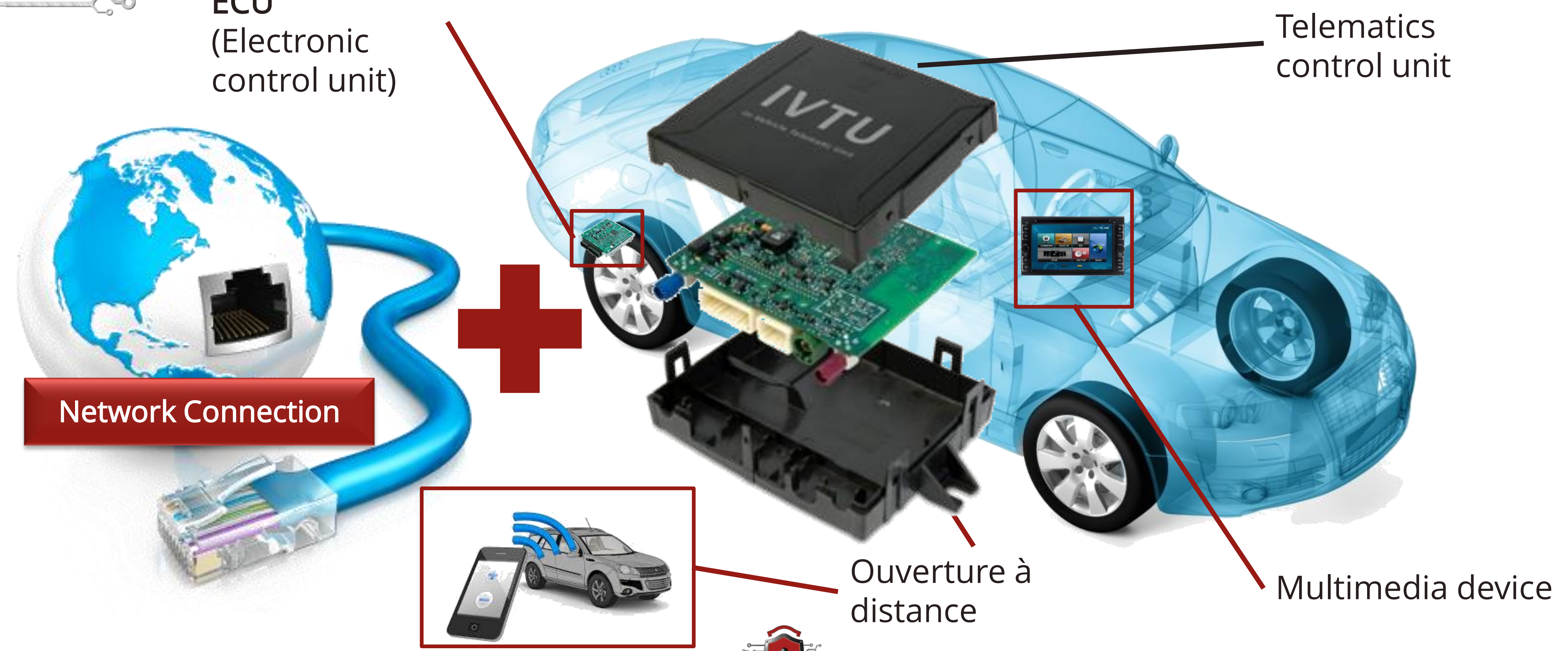
Remote opening

Multimedia device

03

WHICH SOLUTIONS/TOOLS FOR WHICH ACTORS?

SOLUTION 3: INDEPENDENT EVALUATION LABORATORY/ PERIMETER



ECU (Electronic control unit)

Telematics control unit

Network Connection

Ouverture à distance

Multimedia device

WHICH SOLUTIONS/TOOLS FOR WHICH ACTORS?

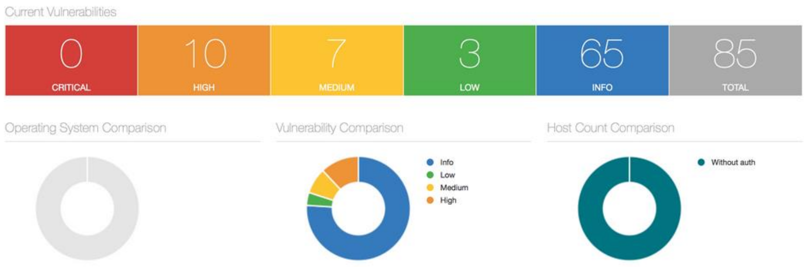
03

SOLUTION 3: INDEPENDENT EVALUATION LABORATORY

Output

Technical **report** of **security** evaluation, containing:

- ❑ The list of **identified vulnerabilities** (compliance + robustness)
- ❑ **Classification of vulnerabilities** by level (example: critical and major)
- ❑ The list of **recommendations** following the evaluation
- ❑ **Managerial summary** and **dashboard** for **decision makers** and **trades**



Current Vulnerabilities

0	10	7	3	65	85
CRITICAL	HIGH	MEDIUM	LOW	INFO	TOTAL

Operating System Comparison

Vulnerability Comparison

Host Count Comparison

Audience

- ❑ Businesses / risk bearers, developers, architects, project managers, security managers.

Properties of the solution

- ❑ Format: benefits of **evaluation** service in our **laboratory**

- ❑ <u>Type of solutions / products:</u>
- ✓ **IoT products** (example: telematics, multimedia ...)
- ✓ **Mobile Apps**

03

WHICH SOLUTIONS/TOOLS FOR WHICH ACTORS?

SOLUTION 3: INDEPENDENT EVALUATION LABORATORY

Target

- ❑ **Companies benefiting from IoT solutions** (example: Groupe Bolloré, EDF…)
- ❑ **Manufacturers** and **Developers** of IoT Solutions (example: Peugeot, VEOLIA,…|)

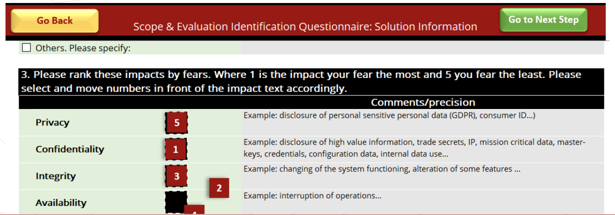
Time required for delivery

T0 + 4 weeks* or **T0=** the day of the receipt of input service

*In case the evaluated products require an implication
of several highly advanced hardware tests, the deadline could be revised upward.

Service Input

- ❑ Answers to a **generic questionnaire** related to IoT solution / the product and technical framewo
- ❑ **OR** Security Profile
- ❑ **Product + functional environment**

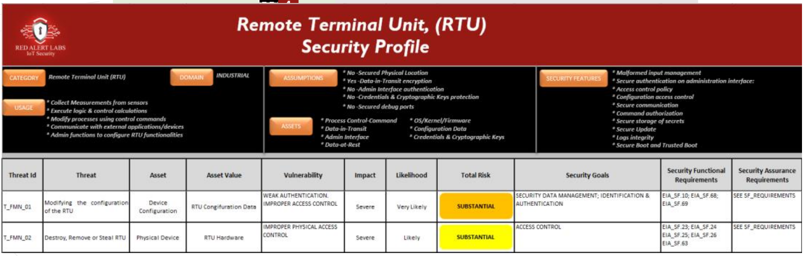


Scope & Evaluation Identification Questionnaire: Solution Information

☐ Others. Please specify:

3. Please rank these impacts by fears. Where 1 is the impact your fear the most and 5 you fear the least. Please select and move numbers in front of the impact text accordingly.

		Comments/precision
Privacy	5	Example: disclosure of personal sensitive personal data (GDPR), consumer ID…)
Confidentiality	1	Example: disclosure of high value information, trade secrets, IP, mission critical data, master-keys, credentials, configuration data, internal data use…
Integrity	3	Example: changing of the system functioning, alteration of some features …
Availability	2	Example: interruption of operations…



Remote Terminal Unit, (RTU)
Security Profile

CATEGORY: Remote Terminal Unit (RTU)
DOMAIN: INDUSTRIAL

USAGE:
* Collect Measurements from sensors
* Execute logic & control calculations
* Modify processes using control commands
* Communicate with external applications/devices
* Admin functions to configure RTU functionalities

ASSUMPTIONS:
* No -Secured Physical Location
* Yes -Data-in-Transit encryption
* No -Admin Interface authentication
* No -Credentials & Cryptographic Keys protection
* No -Secured debug ports

ASSETS:
* Process Control-Command
* Data-in-Transit
* Admin Interface
* Data-at-Rest
* OS/Kernel/Firmware
* Configuration Data
* Credentials & Cryptographic Keys

SECURITY FEATURES:
* Malformed input management
* Secure authentication on administration interface:
* Access control policy
* Configuration access control
* Secure communication
* Command authorization
* Secure storage of secrets
* Secure Update
* Logs integrity
* Secure Boot and Trusted Boot

Threat Id	Threat	Asset	Asset Value	Vulnerability	Impact	Likelihood	Total Risk	Security Goals	Security Functional Requirements	Security Assurance Requirements
T_FMN_01	Modifying the configuration of the RTU	Device Configuration	RTU Congifuration Data	WEAK AUTHENTICATION. IMPROPER ACCESS CONTROL	Severe	Very Likely	SUBSTANTIAL	SECURITY DATA MANAGEMENT; IDENTIFICATION & AUTHENTICATION	EIA_SF.10; EIA_SF.68; EIA_SF.69	SEE SF_REQUIREMENTS
T_FMN_02	Destroy, Remove or Steal RTU	Physical Device	RTU Hardware	IMPROPER PHYSICAL ACCESS CONTROL	Severe	Likely	SUBSTANTIAL	ACCESS CONTROL	EIA_SF.23; EIA_SF.24 EIA_SF.25; EIA_SF.26 EIA_SF.63	SEE SF_REQUIREMENTS

03

WHICH SOLUTIONS/TOOLS FOR WHICH ACTORS?

SOLUTION 3: INDEPENDENT EVALUATION LABORATORY

	BASIC SOLUTION		OUR SOLUTION	
SPECIALIZED EXPERTISE	**Subjective** and **not adaptable evaluation** to **IoT**	🪫	**Thoughtful** and **structured evaluation** for **IoT**	🔋
RISKS	**Generic Evaluation Methodology** not based on **Risk-based approach**	🪫	**Security Profile specific evaluation methodology** with a **risk approach**	🔋
ACCESS / TIME TO MARKET	**Time-consuming evaluation**	🪫	**Quick assessment** through **risk-based approach and automated IoT tools**	🔋
COSTS	**Costly evaluation**	🪫	**Cost reduction** of more than **40%** thanks to **risk approach** and **automated IoT tools**	🔋

05 CONCLUSION

All
IoT sectors
(Health, Transport, Industrial, Energy)
•••)

3
Solutions

Security & Trust
By Design

100 %
Guarantee in specialized security expertise
and cost-efficient results

CONTACT

Red Alert Labs
3 rue Parmentier, 94140 Alfortville

✉ *contact@redalertlabs.com*

☎ +33 9 53 55 54 11

🌐 www.redalertlabs.com

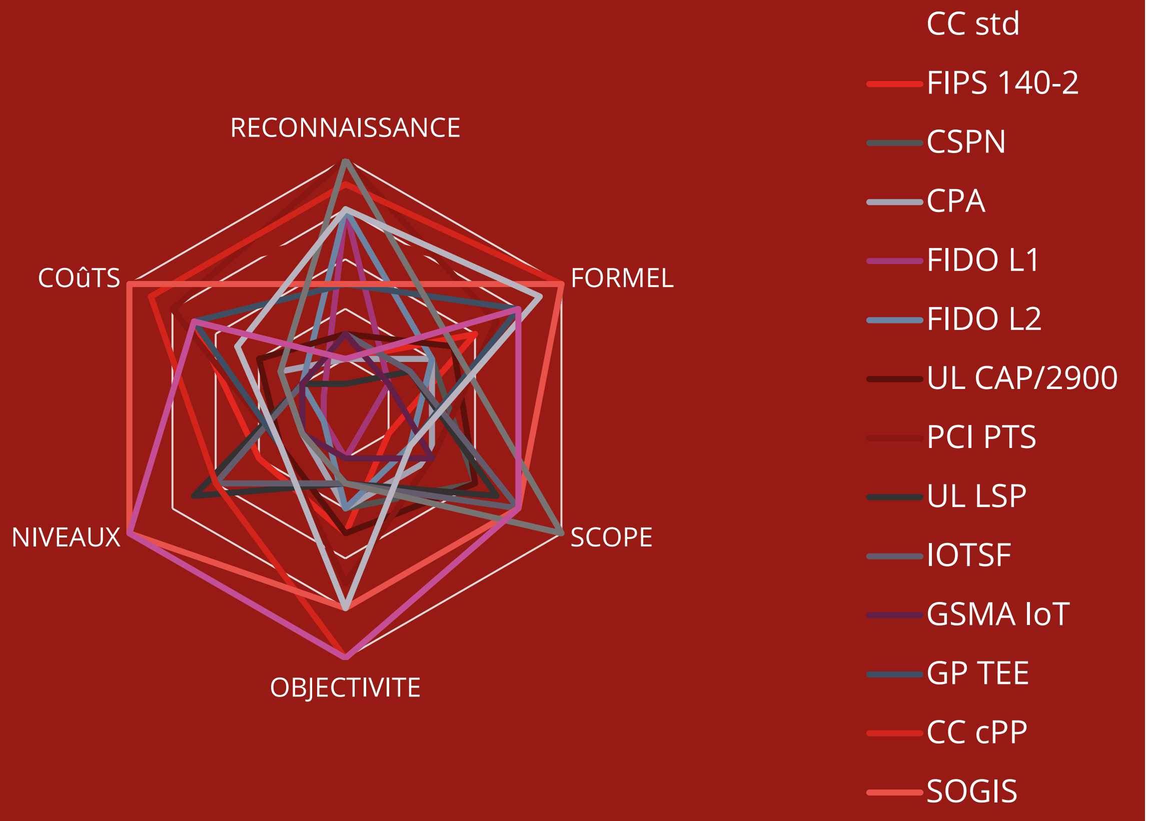
Thank you for your **TRUST**

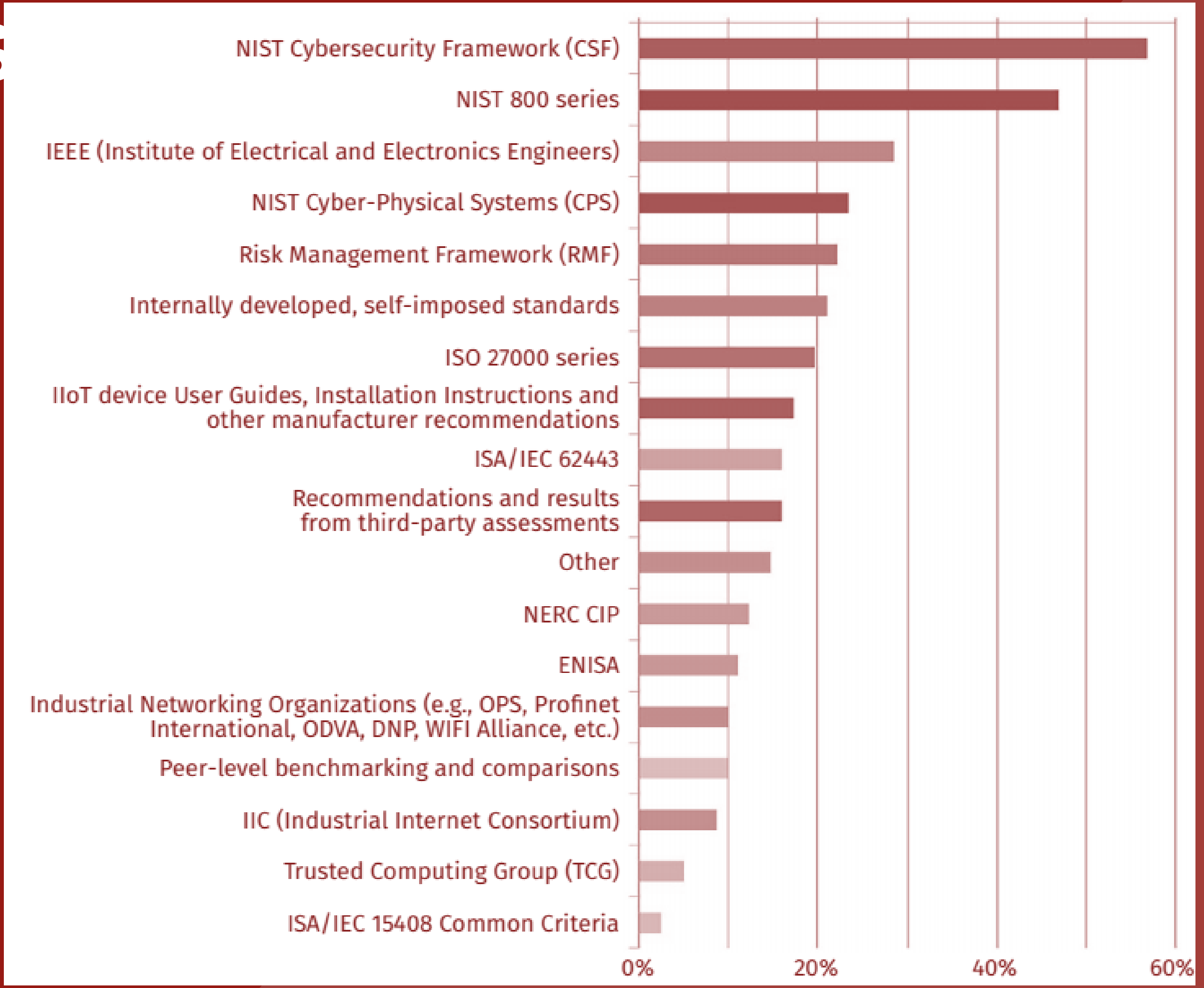
TWITTER @RedAlertLabs

RED ALERT LABS
IoT Security

ANNEX

TOO MANY STANDARDS

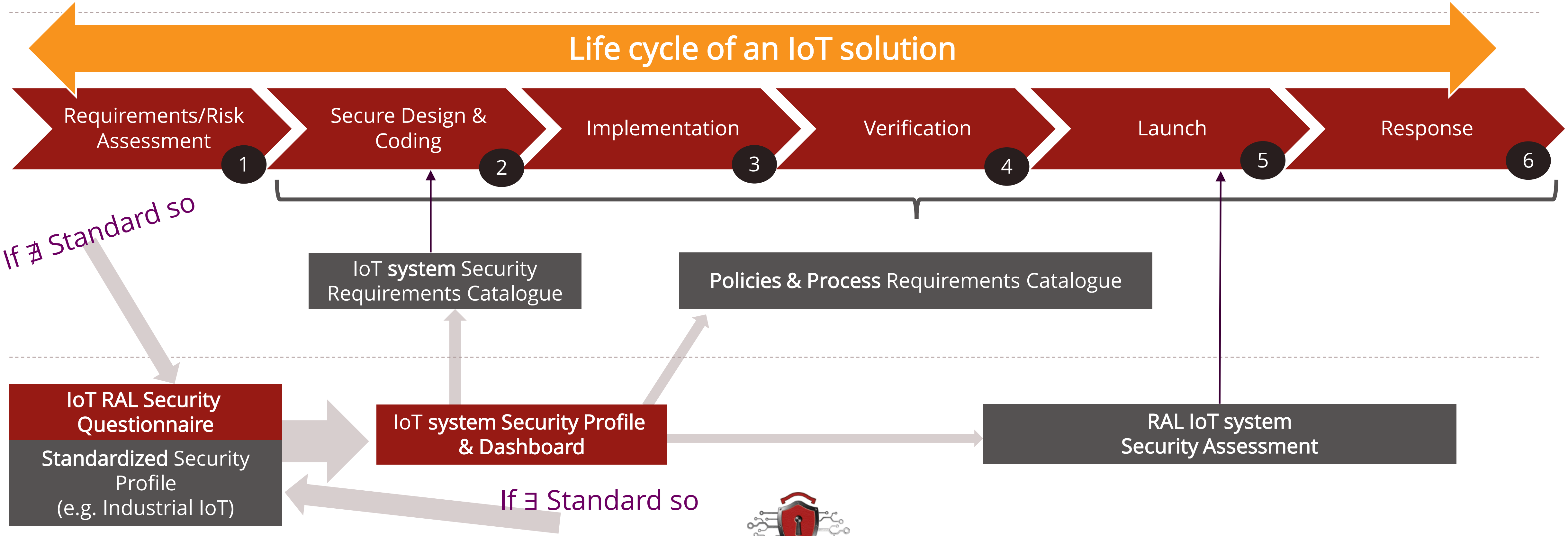




https://www.sans.org/.../2018-industrial-iot-security-survey-shaping-iiot-security-conc...

Security Framework

Which solution related to the development cycle?



Life cycle of an IoT solution

Requirements/Risk Assessment 1

Secure Design & Coding 2

Implementation 3

Verification 4

Launch 5

Response 6

If ∄ Standard so

IoT system Security Requirements Catalogue

Policies & Process Requirements Catalogue

IoT RAL Security Questionnaire

Standardized Security Profile (e.g. Industrial IoT)

IoT **system Security Profile & Dashboard**

RAL IoT system Security Assessment

If ∃ Standard so

3 SECURITY PROFILE

Domains

- Industrial,
- Consumer,
- Critical,
- Enterprise

Categories

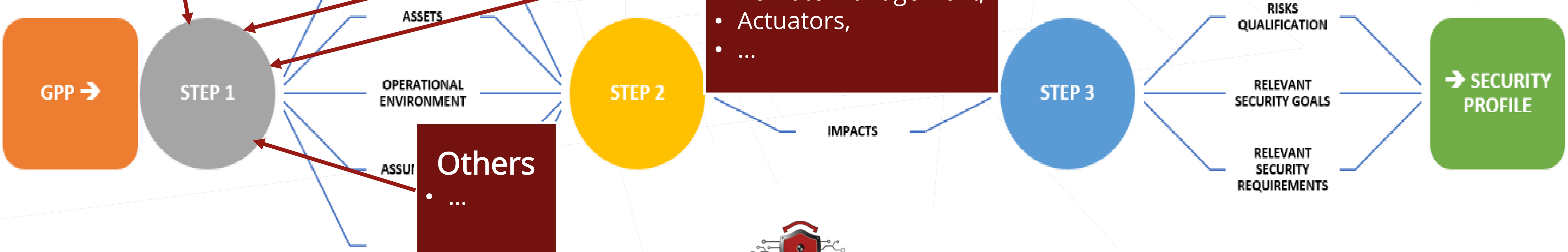
- Mobile Devices,
- Access control Devices – Physical Access (eg: smart doors, Key card)
- Security Monitoring Devices (alarm, doorbell, camera, …),
- Multifunction Device (printer, scanner, fax …),
- Wearables (smart watches, badges …),
- Energy providing devices (Room heaters, smart meters, …)
- Automobiles (cars,…),
- Networking components (routers, swit
- ….

Assets

- Os,
- Firmware,
- Sensors,
- Network Interface,
- Remote Management,
- Actuators,
- …

Others

- …



GPP ➔

STEP 1

ASSETS

OPERATIONAL ENVIRONMENT

ASSU

STEP 2

IMPACTS

STEP 3

RISKS QUALIFICATION

RELEVANT SECURITY GOALS

RELEVANT SECURITY REQUIREMENTS

➔ SECURITY PROFILE