This presentation was given by Dr. Alejandro Manilla during the Public Webinar of 4 July 2019, on Legal perspectives of using IoT for AD, this in the context of AUTOPILOT H2020 project.
For any request please contact j.allard@mail.ertico.com or the speaker himself.

AUTOPILOT Cybersecurity Evaluation

Index

- **Cybersecurity Objectives for IoT**
- **Methodology**
  - Feature definitions, architectures and AUTOPILOT concept
  - Initation of the cybersecurity plan
- **Study**
  - Threat analysis risk assesement from architecture to device
  - Cybersecurity concept
- **Evaluation of the results**
  - Misbehavior detection and countermeasures
  - Cybersecurity assessment of the AUTOPILOT architectures

Cybersecurity objectives for IoT

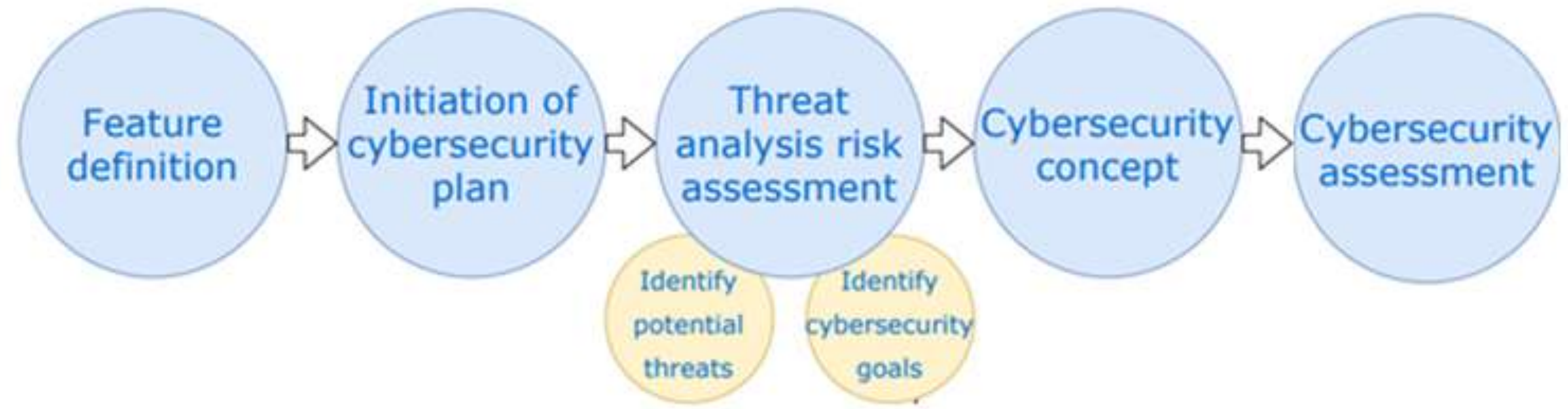
The evaluation will identify the potential cybersecurity issues on IoT devices and architecture and determine if the AUTOPILOT implementations are secure to the required level, accomplishing the next main objectives.

Confidentiality
Integrity
Availability

Reach the objectives also will influence the quality of the service improving the overall system.

Cybersecurity objectives

Evaluation methodology steps


Feature definition
Initiation of cybersecurity plan
Threat analysis risk assessment
Cybersecurity concept
Cybersecurity assessment
Identify potential threats
Identify cybersecurity goals

The methodology is adapted and based from SAEJ3061

Index

- Cybersecurity Objectives for IoT
- Methodology
  - Feature definitions, architectures and AUTOPILOT concept
  - Initation of the cybersecurity plan
- Study
  - Threat analysis risk assesement from architecture to device
  - Cybersecurity concept
- Evaluation of the results
  - Misbehavior detection and countermeasures
  - Cybersecurity assessment of the AUTOPILOT architectures

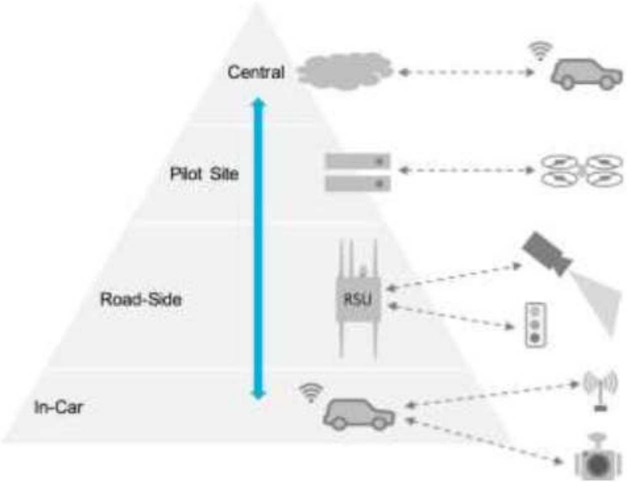
Methodology of the workplan

Feature definition

Gather information about feature definitions and architectures implemented by pilot sites that will be required to start the cybersecurity evaluation methodology. A common architecture for the AUTOPILOT project will be used to start the analysis.

Methodology of the workplan

Top-down analysis of the AUTOPILOT concept



The cybersecurity analysis in AUTOPILOT will be performed from the high level architecture concept to the IoT devices, without going in deep to the devices requirements.

Methodology of the workplan

Initiation of cybersecurity plan

Describes the activities to be carried out as part of the cybersecurity evaluation methodology in AUTOPILOT

Index

- **Cybersecurity Objectives for IoT**
- **Methodology**
  - Feature definitions, architectures and AUTOPILOT concept
  - Initation of the cybersecurity plan
- **Study**
  - Threat analysis risk assesment from architecture to device
  - Cybersecurity concept
- **Evaluation of the results**
  - Misbehavior detection and countermeasures
  - Cybersecurity assessment of the AUTOPILOT architectures

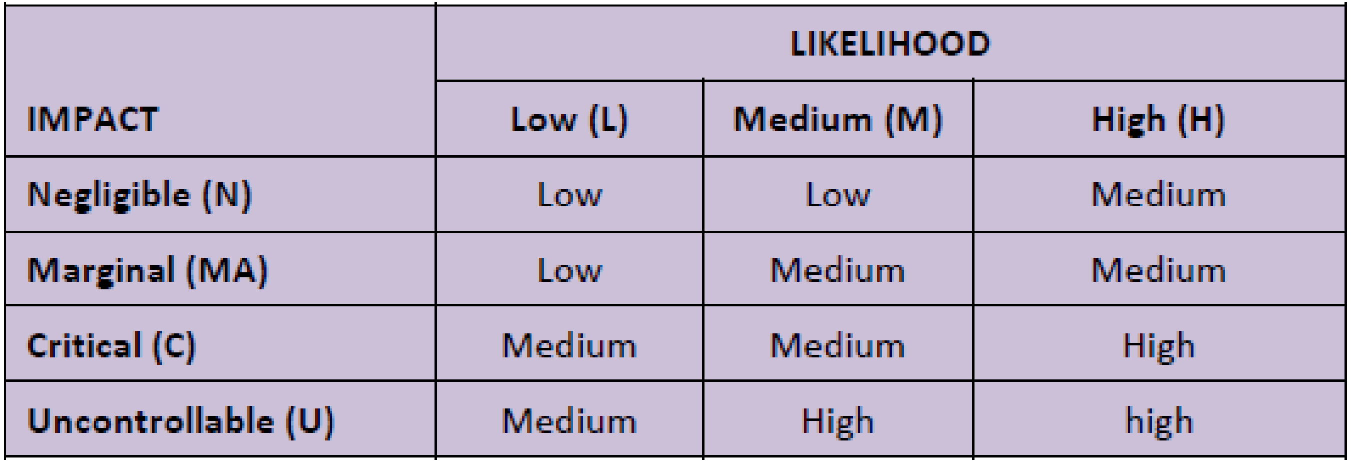
Study of cybersecurity solutions

Threat analysis risk assessment (TARA)

This activity is used to identify the potential threats and determine the risk associated to each threat, it helps to identify potential vulnerabilities. The analysis will be performed from the high level architecture and infrastructure to the IoT devices, without going deep in devices requirements.

Study of cybersecurity solutions

Identify potential threats - Threats will be determined for the studied architectures and system features.



IMPACT	LIKELIHOOD		
	Low (L)	Medium (M)	High (H)
Negligible (N)	Low	Low	Medium
Marginal (MA)	Low	Medium	Medium
Critical (C)	Medium	Medium	High
Uncontrollable (U)	Medium	High	high

Table shows FERMA standard approach

Identify cybersecurity goals - Cybersecurity goals for the evaluation will be identified for the highest risks based on the identified threats.

Study of cybersecurity solutions

Cybersecurity concept

The cybersecurity concept may contain the high-level cybersecurity goals identified during the “Threat analysis risk assessment” stage. The strategy for addressing the cybersecurity goals will be based on the potential risk level of the threats associated for the IOT technology.

Study of cybersecurity solutions

Misbehavior detection and countermeasures

The TARA cannot cover previously unknown threads, therefore functionality misbehavior detection systems will be considered and proposed, along with their countermeasures.

Index

- **Cybersecurity Objectives for IoT**
- **Methodology**
  - Feature definitions, architectures and AUTOPILOT concept
  - Initation of the cybersecurity plan
- **Study**
  - Threat analysis risk assesment from architecture to device
  - Cybersecurity concept
- **Evaluation of the results**
  - Misbehavior detection and countermeasures
  - Cybersecurity assessment of the AUTOPILOT architectures

Evaluation of the results

Misbehavior detection and countermeasures

During the evaluation of results, function misbehaviors will be noted and countermeasures to the detected issues will be proposed.

Evaluation of the results

Cybersecurity assessment

Cybersecurity assessment analysis is performed to evaluate the cybersecurity state of the autopilot system. It provides the justification that the system is “secure” to the required level, this means that cybersecurity goals identified in the TARA and the strategy in the cybersecurity concept is satisfied and pass the evaluation.

Applus IDIADA

YOUR DEVELOPMENT PARTNER

Applus IDIADA
Headquarters and Main Technical Centre
L’Albornar – PO Box 20
E-43710 Santa Oliva (Tarragona) Spain
T +34 977 166 000 F +34 977 166 007
e-mail: idiada@idiada.com

www.idiada.com

Applus IDIADA Belgium
T +32 2 757 27 07 (Brussels)
e-mail: idiada_belgium@idiada.com

Applus IDIADA Brazil
T +55 11 4330 9880 (São Paulo)
T +55 31 3591 6832 (Betim)
T +55 11 4330 9880 (Curitiba)
T +55 24 3355 3133 (Resende)
e-mail: idiada_brasil@idiada.com

Applus IDIADA China
T
T +86 10 8446 3317 (Beijing)
T +86 431 8190 9680 (Changchun)
T +86 23 6756 8060 (Chongqing)
T +86 20 2282 9202 (Guangzhou)
T +86 (772) 3166 619 (Liuzhou)
T +86 (772) 0532 66019017 (Qingdao)
T +86 (755) 29184532 (Shenzhen)
T +86 0535 8933658 (Zhaoyuan)
e-mail: idiada_china@idiada.com

Applus IDIADA Czech Republic
T +420 493 654 811 (Hradec Králové)
T +420 778 430 095 (Brno)
T +420 482 424 243 (Liberec)
T +420 326 736 860 (Mladá Boleslav)
e-mail: info@idiada.cz

Applus IDIADA France
T +33 (0) 141 146 085 (Paris)
e-mail: idiada_france@idiada.com

Applus IDIADA Germany
T +49 (0) 841 88538-0 (Ingolstadt)
T +49 (0) 69 97503116 (Frankfurt)
T +49 (0) 89 309056-0 (Munich)
T +49 (0) 711 67400109 (Stuttgart)
T +49 (0) 5374 920606-0 (Wolfsburg)
e-mail: idiada_germany@idiada.com

Applus IDIADA India
T +91 994 0679 933 (Chennai)
T +91 124 4028 888 (New Delhi)
T +91 20 6605 6800 (Pune)
e-mail: idiada_india@idiada.com

Applus IDIADA Indonesia
T +6221 2939 1143 (Jakarta)
e-mail: idiada_indonesia@idiada.com

Applus IDIADA Italy
T +390 11 2644000 (Leini)
T +390 51 0923530 (Bologna)
T +390 05 10923500 (Erbusco)
e-mail: idiada_italia@idiada.com

Applus IDIADA Japan
T +81 (0) 42 512 8982 (Tokyo)
T +81 (0) 56 464 3463 (Aichi)
e-mail: idiada_japan@idiada.com

Applus IDIADA Malaysia
T +603 9207 7018 (Kuala Lumpur)
T +601 2410 7686 (Penang)
e-mail: idiada_malaysia@idiada.com

Applus IDIADA Mexico
T +52 (222) 644 1374 (Puebla)
e-mail: idiada_mexico@idiada.com

Applus IDIADA Poland
T +48 61 6226 905 (Poznan)
e-mail: idiada_polska@idiada.com

Applus IDIADA Russia
T +7 (831) 297 94 32 (Nizhny Novgorod)
T +7 (831) 261 37 06 (Togliatti)
e-mail: idiada_russia@idiada.com

Applus IDIADA Scandinavia
T +46 (0) 31 320 1844 (Gothenburg)
e-mail: idiada_scandinavia@idiada.com

Applus IDIADA Slovakia
T +420 778 430 098 (Košice)
e-mail: idiada_slovakia@idiada.com

Applus IDIADA South Africa
T +27 83 450 8925 (Pretoria)
e-mail: idiada_southafrica@idiada.com

Applus IDIADA South Korea
T +82 31 478 1821 (Seoul)
e-mail: idiada@idiada.co.kr

Applus IDIADA Spain
T +34 977 166 000 (Santa Oliva)
T +34 928 587 447 (Las Palmas)
T +34 915 095 795 (Madrid)
T +34 950 473 256 (Mojácar)
T +34 868 912 179 (Murcia)
T +34 948 292 921 (Pamplona)
T +34 986 900 300 (Vigo)
e-mail: idiada@idiada.com

Applus IDIADA Taiwan
T +886 47 810 702 (Lukang)
e-mail: idiada_taiwan@idiada.com

Applus IDIADA Thailand
T +66 86 7917 071 (Bangkok)
e-mail: idiada_thailand@idiada.com

Applus IDIADA Turkey
T +90 216 250 6050 (Istanbul)
e-mail: idiada_turkey@idiada.com

Applus IDIADA UK
T +44 1223 441 434 (Cambridge)
T +44 2476 328 083 (Nuneaton)
T +44 1926 623 132 (Warwick)
e-mail: idiada_uk@idiada.com

Applus IDIADA USA
T +1 248 978 0111 (Detroit)
T +1 760 246 1672 (Los Angeles)
e-mail: idiada_USA@idiada.com