

Goal-Oriented Co-engineering of Security and Safety Requirements in Cyber-Physical Systems

Philippe Massonet,
CETIC Research Center, Charleroi, Belgium

Philippe.massonet@cetic.be

www.cetic.be

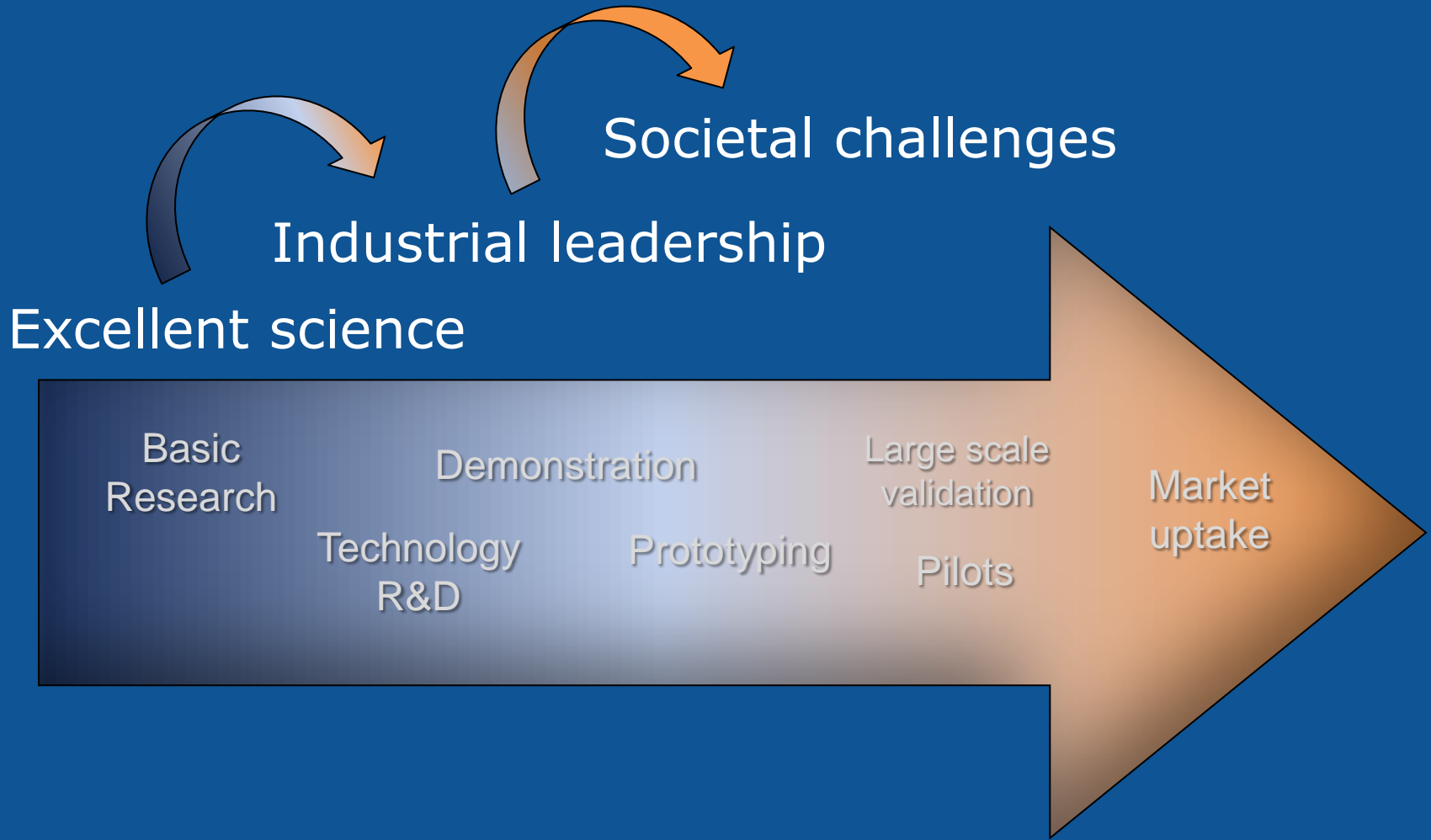


Plan

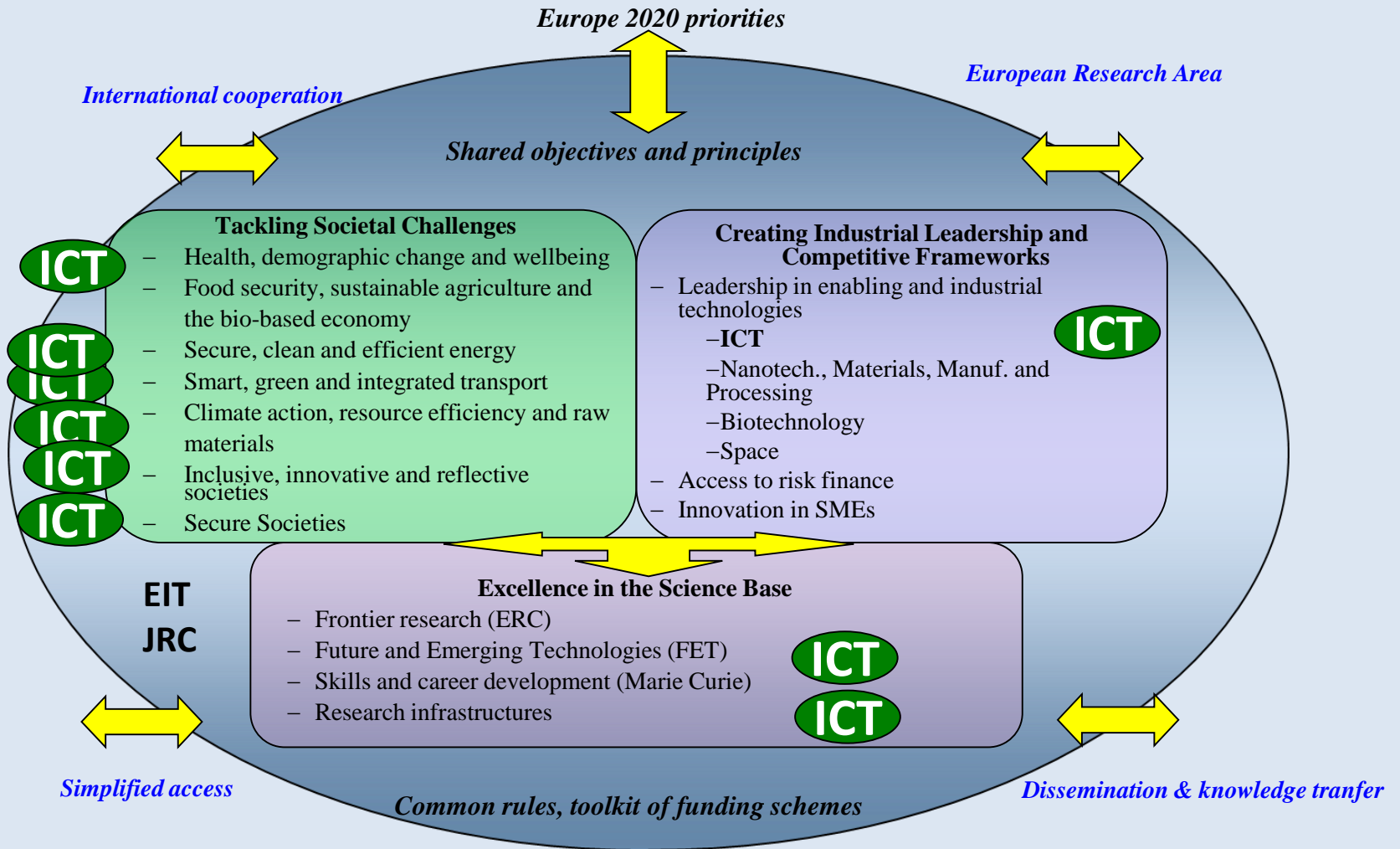
- Introduction to H2020 Framework programme
 - How to find safety related research calls
 - How to find safety related research projects
- Goal-Oriented Co-engineering of Security and Safety Requirements in Cyber-Physical Systems
 - Trend of CPS in multiple domains: **automotive, railway, aerospace, space, energy**
 - Security risks
 - Co-engineering of Security and Safety Requirements



H2020: Coverage of the full innovation chain



H2020: Structure



But no Safety specific topic, it is part of other research areas



South
Korean
Companies,
Research
centers,
Universities
can
participate
in H2020

ec.europa.eu/research/participants/data/ref/h2020/other/hi/h2020_localsupp_korea_en.pc x shift2rail

Les plus visités Débuter avec Firef...

Page : 1 sur 2 Zoom automatique

Republic of Korea – Country Page

1. Available local programs or funds that could provide support to Korean Horizon 2020 participants

Horizon 2020 is fully open to participation of entities from across the world in all parts of the programme, and many topics are flagged as being specifically relevant for cooperation with partners outside Europe.

Korean researchers, universities, research organisations and enterprises are able to team up with their European partners to participate in projects under Horizon 2020 and make the best use of Europe's excellent opportunities in research and innovation. Through participation in Horizon 2020, beneficiaries can gain great benefits from access to excellent talent, knowledge, data and infrastructures and connection to world-leading teams, networks and value chains.

EU-Korea Co-funding Mechanism for Research and Innovation Projects

Korean participants are not automatically eligible for funding through Horizon 2020. Korean participants have themselves to determine the sources of funding and find the resources for their part of the project. These may be own funds, as well as funds received from Korean ministries, foundations and other organisations that fund research and innovation activities in Korea. Contributions can also be made in kind.

To support Korean participants, the Korean government (Ministry of Science, ICT and Future Planning, MSIP, <http://www.msip.go.kr>, and Ministry of Trade, Industry and Energy, MOTIE, <http://www.motie.go.kr>) regularly launches public calls for proposals to co-fund Koreans in Horizon 2020 projects selected for European Union funding, covering all thematic areas. Korean partners should consult these websites in view of submitting applications:

http://www.nrf.re.kr/nrf_tot_cms/board/biz_notice/list.jsp?show_no=170&check_no=169&c_relation=biz&c_relation2=0&c_no=294&c_now_tab=1

Transfert des données depuis ec.europa.eu...

How to find Safety Related Calls

https://ec.europa.eu/research/participants/portal/desktop/en/opportunities/index.html

Rechercher

visités ▾ Débuter avec Firef...

(A-Z) Sitemap About this site Contact Legal Notice Search English ▾

European Commission

RESEARCH & INNOVATION

Participant Portal

European Commission > Research & Innovation > Participant Portal > Funding Opportunities

HOME **FUNDING OPPORTUNITIES** HOW TO PARTICIPATE EXPERTS SUPPORT 🔍 LOGIN REGISTER

EU Programmes 2014-2020

Search Topics

Updates

Calls

- H2020
- 3rd Health Programme
- Asylum, Migration and Integration Fund
- Consumer Programme
- COSME
- Internal Security Fund - Borders
- Internal Security Fund - Police
- Justice Programme
- Promotion of Agricultural Products
- Research Fund for Coal & Steel
- Rights, Equality and Citizenship Programme

Funding Opportunities

H2020 ONLINE MANUAL

Find the European Union funding opportunities and search for new or closed calls of the programmes described on this page.

Horizon 2020

Horizon 2020 is the new EU funding programme for research and innovation running from 2014 to 2020 with a €80 billion budget. H2020 supports **SMEs** with a new **instrument** that runs throughout various funded research and innovation fields, enhances EU **international research** and Third Country participation, attaches high importance to integrate **social sciences and humanities** encourages to develop a **gender dimension** in project.

Cosme

Programme for the Competitiveness of Enterprises and SMEs (COSME) will run from 2014 to 2020, with a planned budget of €2.3bn. It will facilitate SME access to finance, create supportive environment for business creation, help small businesses operate outside their home countries and improve their access to markets.

Consumer Programme

The **Multiannual Consumer Programme** 2014-2020 has a planned budget of 188 million EUR. It will support actions that ensure a high level of consumer protection, that empower consumers and that place the consumer at the heart of the internal market.

Other Funding Opportunities


Search Calls on Safety

ec.europa.eu/geninfo/query/action?query_source=RESEARCHPPP&swlang=en&QueryText=safety

Rechercher

visités Débuter avec Firef...

Archives | A-Z Index | Sitemap | About this site | Contact | Legal notice English (en)



RESEARCH & INNOVATION Participant Portal

European Commission > Research & Innovation > Participant Portal > Search

Search

safety

Search options

Source
Participant Portal

Date
All

Language
English

File formats
All

Filter by

- All Pages (21)
- FP7 Reference Documentation (257)
- H2020 Calls (7)
- H2020 Online Manual (2)
- H2020 Reference Documentation (187)
- Participant Portal FAQs (2)

WEB Opportunities - Research Participant Portal
ec.europa.eu/research/participants/portal/desktop/en/.../index.html
10 Nov 2016 - Fund for Coal and Steel (RFCS) provides funding for high quality research projects which support the competitiveness of the European Coal and Steel industries. The programme

WEB CONS-GPSD-2014
ec.europa.eu/research/participants/portal/.../cons-gpsd-2014.html
10 Nov 2016 - computer. Close EU Programmes 2014-2020 Calls FP7 & CIP Programmes 2007-2013 CALL: JOINT ACTION - GENERAL PRODUCT **SAFETY** DIRECTIVE Call identifier: CONS-GPSD-2014 Publication

WEB H2020-ART-2016-2017
ec.europa.eu/research/participants/.../h2020-art-2016-2017.html
10 Nov 2016 - passenger cars, trucks and urban transport. Demonstrations will be complemented by further research on digital infrastructure to ensure the necessary level of **safety**, reliability

WEB Calls - Research Participant Portal
ec.europa.eu/research/participants/portal/desktop/en/.../index.html
10 Nov 2016 - research projects which support the competitiveness of the European Coal and Steel industries. The programme covers core production processes; new products and applications

WEB FAQ - Research Participant Portal
ec.europa.eu/research/participants/portal/desktop/.../faq-1059.html
17 Nov 2016 - Research & Innovation - Participant Portal > > support Search Loading. Login Online services unavailable You are about to log off. Please close all browser windows, if you

WEB RFCS-2015
ec.europa.eu/research/participants/portal/desktop/.../rfcs-2015.html
10 Nov 2016 - programme is fully in line with the scientific, technological and political objectives of the European Union. This includes the general aim of contributing to sustainable

WEB CONS-GPSD-2015

Example: Automated Road Transport

europa.eu/research/participants/portal/desktop/en/opportunities/h2020/calls/h2020-art-2016-2017

Rechercher

visités ▾ Débuter avec Firef...

(A-Z) Sitemap About this site Contact Legal Notice Search English ▾

RESEARCH & INNOVATION
Participant Portal

European Commission

European Commission > Research & Innovation > Participant Portal > Opportunities

HOME FUNDING OPPORTUNITIES HOW TO PARTICIPATE EXPERTS SUPPORT ▾ Search 🔍 LOGIN REGISTER

EU Programmes 2014-2020

Search Topics

Updates 📅 📧

Calls 📅 📧


- H2020
- 3rd Health Programme
- Asylum, Migration and Integration Fund
- Consumer Programme
- COSME
- Internal Security Fund - Borders
- Internal Security Fund - Police
- Justice Programme
- Promotion of Agricultural Products
- Research Fund for Coal & Steel
- Rights, Equality and Citizenship Programme

FP7 & CIP Programmes 2007-2013

Calls

CALL: 2016-2017 AUTOMATED ROAD TRANSPORT [Call budget overview](#)

Call identifier: H2020-ART-2016-2017
Publication date: 14 October 2015

 Horizon 2020 [H2020 website](#)

Pillar: [Societal Challenges](#)
Work Programme Year: H2020-2016-2017
Work Programme Part: [Smart, green and integrated transport](#)

Call summary [- Less](#)

Scene Setter:

Road vehicle automation is one of the major trends that will shape the future of road transport and of our mobility. It holds the promise to help address many of the major challenges of today's transport system, such as user safety, energy efficiency, CO2 emissions, air quality and congestion, and to enhance the drivers' individual comfort and convenience. At the same time, it represents a critical testing ground for the ability of the European automotive industry to preserve and consolidate its global leadership. Automakers around the world are unanimous in predicting the emergence of systems for automated driving sometime in the near future.

Current technology will evolve further towards semi-automation and eventually towards full automation in real moving traffic. This evolution is very promising and may help to drastically reduce road fatalities to near zero, as more than 90% of road accidents are partly or fully due to human errors. Nevertheless, there are still many challenges related to technology, digital infrastructure, user and societal acceptance, driver behaviour, regulation and legislation, and business models, which need to be tackled to enable the deployment of automated driving on European roads.

The main contribution of this call will be to support the short term introduction of passenger cars automated driving level 3 (Conditional Automation - Full driving performed by an automated driving system with the expectation that the human driver will respond appropriately to a request to intervene in real traffic conditions)[[The SAE International's standard J3016 identifies six levels of driving automation from "no automation" to "full automation"]] including safe stops, and of truck platooning in real traffic conditions from 2020 onwards. The main focus of this call is on demonstrations of automated driving systems for passenger cars, trucks and urban transport. Demonstrations will be complemented by further research on digital infrastructure to ensure the necessary level of safety, reliability and efficiency

Tout surligner Respecter la casse Mots entiers Occurrence 1 sur 4

Example: Work Program me




Sample
Topic: Safety
and end-user
acceptance
of road
automation
in the
transition
period

...europea.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/art-04-2016.html

Rechercher

visités ▾ Débuter avec Firef...

(A-Z) Sitemap About this site Contact Legal Notice Search English ▾

 RESEARCH & INNOVATION
Participant Portal

European Commission > Research & Innovation > Participant Portal > Opportunities

HOME FUNDING OPPORTUNITIES HOW TO PARTICIPATE EXPERTS SUPPORT ▾ Search [] LOGIN REGISTER

EU Programmes 2014-2020

Search Topics

Updates [] []

Calls [] []

H2020

3rd Health Programme

Asylum, Migration and Integration Fund

Consumer Programme

COSME

Internal Security Fund - Borders

Internal Security Fund - Police

Justice Programme

Promotion of Agricultural Products

Research Fund for Coal & Steel

Rights, Equality and Citizenship Programme

FP7 & CIP Programmes 2007-2013

Calls


TOPIC : Safety and end-user acceptance aspects of road automation in the transition period

Topic identifier: ART-04-2016
Publication date: 14 October 2015

Types of action: RIA Research and Innovation action
DeadlineModel: two-stage
Opening date: 15 October 2015

Deadline: 20 January 2016 17:00:00
2nd stage Deadline: 29 September 2016 17:00:00

Time Zone : (Brussels time)

 Horizon 2020
Pillar: Societal Challenges
Work Programme Year: H2020-2016-2017
Work Programme Part: Smart, green and integrated transport
Call : H2020-ART-2016-2017

H2020 website
Call budget overview

Topic Description - Less

Specific Challenge:

Automated vehicles will be accepted by customers and society only when they will be deemed easy-to-use and fully reliable and safe regarding the planned manoeuvres and their execution. A key challenge is to ensure safe vehicles handling with reduced driver attention. Especially for level 3 automated driving systems an effective interaction between the driver and the automated vehicle plays an important role. To act in harmony with driver expectations, these systems should be engineered following a user-centric approach. User acceptance is particularly important for the design of, driver interfaces that will facilitate the transitions between human and automated driving. Moreover, the automated driving systems should be resilient to both system and driver failures and guarantee sufficient reliability and robustness in each and every situation in real world traffic. The introduction of automated vehicles into the existing traffic poses specific issues regarding safety, in particular during the transition period where there will be interactions with other vehicles (of any degree of automation or none) and other traffic participants such as pedestrians or cyclists.

Scope:

Proposals for research and innovation activities should address one or several of the following domains:

Tout surligner Respecter la casse Mots entiers Occurrence 2 sur 5

How to find Safety Related Projects

Sample search: « Assurance and Certification of Cyber-Physical Systems »


The screenshot shows the CORDIS website interface. At the top, there is a navigation bar with links for 'About CORDIS', 'Contact', 'Advanced Search', and 'Legal Notice', along with a language dropdown set to 'English (en)'. Below this is the CORDIS logo and the text 'Community Research and Development Information Service'. A breadcrumb trail reads 'European Commission > CORDIS > Projects & Results Service > Home'. A search bar is present with a 'Search' button and a 'Sign in' link. A 'Feedback' button is on the right edge. The main content area has a 'NEWS & EVENTS' section with a 'Browse by:' dropdown menu containing 'Subject', 'Programme', 'Content type', and 'Country', with an 'Advanced search' link below. The 'PROJECTS & RESULTS' section features a heading 'The primary information source for EU-funded projects since 1990' and a paragraph describing the service. Below this, it mentions 'Horizon 2020 project information' and 'report summaries'. A search box titled 'Search projects and results' is highlighted with a red circle, containing the text 'tification of Cyber-Physical Systems' and a search icon. The 'Latest Results in Brief' section lists two items: 'Fact-finding and generalisations' (dated 2016-11-22) with a thumbnail of a stone plaque for Immanuel Kant, and 'Euro-Mediterranean efforts foster innovation in the energy sector' (dated 2016-11-22) with a thumbnail of solar panels.

Sample Search Result

cordis.europa.eu/projects/result_en?q='Architecture-driven,' AND 'Multi-concern' AND 'Seamless' AMASS project

Les plus visités Débuter avec Firef...

About CORDIS | Contact | Advanced Search | Legal Notice English (en)



CORDIS

Community Research and Development Information Service

European Commission > CORDIS > Projects & Results Service > Results page

Search Sign in

NEWS & EVENTS **PROJECTS & RESULTS** RESEARCH*EU MAGAZINES PARTNERS

Horizon 2020 project information and now also report summaries are available on CORDIS. All H2020 projects can be downloaded from the EU Open Data Portal .

Search projects and results

Free text 'Architecture-driven,' AND 'Multi-cor

Results 1 - 10 of 26976 Results/page: 10

1 2 3 4 5 6 7 8 9 10 > >|

[PROJECT] **AMASS - Architecture-driven, Multi-concern and Seamless Assurance and Certification of Cyber-Physical Systems**
ID: 692474
Start date: 2016-04-01, End date: 2019-03-31
Embedded systems have significantly increased in technical complexity towards open, interconnected systems. This has exacerbated the problem of ensuring dependability in the presence of human, environmental and technological risks. The rise of complex Cyber-Physical Systems...
Programme: H2020-EU.2.1.1.7.
Record Number: 202642
Last updated on: 2016-10-14

[REPORT SUMMARY] **Final Report Summary - COOPEUS (Strengthening the cooperation between the US and the EU in the field of environmental research infrastructures)**
Much more than any other organizational form, research infrastructures appear to be the natural choice for establishing sustainable links across geoscience disciplines. They are meant to serve the needs of their users and typically offer standard services...
Programme: FP7-INFRASTRUCTURES
Record Number: 182586

My refinements
Search term:
Architecture-driven, Multi-concern Seamless Assurance Certification of Cyber-Physical Systems
Save search
My saved searches

Download results of this page
XML CSV
My booklet (0)

Refine by:
Subject
Programme
Content type
Country

Feedback

Sample Project Data



AMASS

Project ID: 692474
Funded under: [H2020-EU.2.1.1.7. - ECSEL](#)

Architecture-driven, Multi-concern and Seamless Assurance and Certification of Cyber-Physical Systems

From 2016-04-01 to 2019-03-31, ongoing project

Project details

Total cost:

EUR 20 534 411,25

EU contribution:

EUR 6 178 242,90

Coordinated in:

Spain

Topic(s):

[ECSEL-07-2015 - Design Technology](#)

Call for proposal:

H2020-ECSEL-2015-1-RIA-two-stage [See other projects for this call](#)

Funding scheme:

ECSEL-RIA - ECSEL Research and Innovation Action

Objective

Embedded systems have significantly increased in technical complexity towards open, interconnected systems. This has exacerbated the problem of ensuring dependability in the presence of human, environmental and technological risks. The rise of complex Cyber-Physical Systems (CPS) has led to many initiatives to promote reuse and automation of labor-intensive activities. Two large-scale projects are OPENCROSS and SafeCer, which dealt with assurance and certification of software...



Coordinator

FUNDACION TECNALIA RESEARCH & INNOVATION
PARQUE CIENTIFICO Y TECNOLOGICO DE BIZKAIA C GELDO EDIFICIO 700
48160 DERIO BIZKAIA
Spain

Spain



EU contribution: EUR 524 742,50

Activity type: Research Organisations

Participants

[Expand all](#)



TELVENT ENERGIA SA

Spain



HONEYWELL INTERNATIONAL SRO

Czech Republic



SCHNEIDER ELECTRIC ESPANA SA

Spain

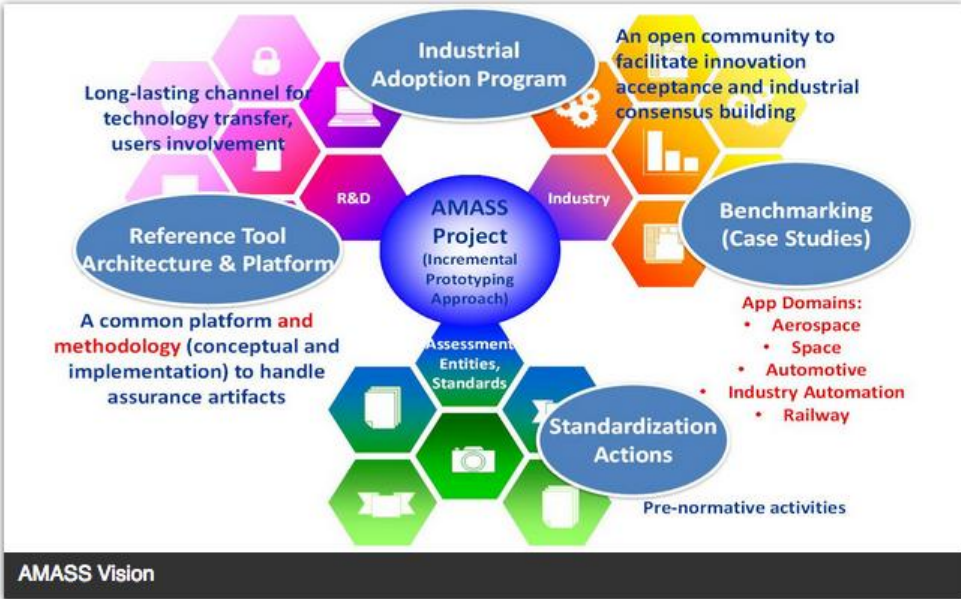


AMASS Project Web page



- Home
- Objectives
- Organization
- Partners
- Library**
- Blo
- Events
- Contact Us

Home » About



AMASS at a Glance

Funded under: [H2020 – ECSEL](#)

Area : Design Technologies

Project No. : 692474

Total budget : 20,5 Million Euro

Duration : Apr 2016–Mar 2019

Coordinator : TECNALIA R&I

Agenda

- Today
- Wednesday, 23 November**
- PROFES 2016
 - FISMA SPIN 3_2016/ Safety Panel
- Thursday, 24 November**
- PROFES 2016
- Displaying events until 31/1.
[Look for more](#)

About

AMASS (Architecture-driven, Multi-concern and Seamless Assurance and Certification of Cyber-Physical Systems) will create and consolidate the de-facto European-wide open tool platform, ecosystem, and self-sustainable community for assurance and certification of **Cyber-Physical Systems (CPS)** in the largest industrial vertical markets including **automotive, railway, aerospace, space, energy.**

Deliverable

ECSEL Research and Innovation actions (RIA)

AMASS

Architecture-driven, Multi-concern and Seamless Assurance and Certification of Cyber-Physical Systems

Baseline and requirements for architecture-driven assurance D3.1

Work Package:	WP3 Architecture-Driven Assurance
Dissemination level:	PU = Public
Status:	Final
Date:	30 September 2016
Responsible partner:	Tecnalia, Inria and Airbus (RIA)
Contact information:	amass@amass41.fr
Document reference:	D3.1 Baseline and Requirements for Architecture-Driven Assurance AMASS

PROFES R&I RIGHTS STATEMENT
The document contains information, which is proprietary to the AMASS Consortium. Neither this document nor the information contained herein shall be used, disclosed or communicated by any means to any third party, in whole or in parts, except with prior written consent of the AMASS Consortium.

Example of ECSEL PPP (Electronics)

www.ecsel-ju.eu/web/index.php

ECSEL Joint Undertaking
Electronic Components and Systems for European Leadership

HOME ABOUT ECSEL JU CALLS FOR PROPOSALS PROJECTS & PARTNERS DOCUMENTS PUBLICATIONS EVENTS CONTACT

THE PUBLIC-PRIVATE PARTNERSHIP KEEPING EUROPE AT THE FOREFRONT OF TECHNOLOGY DEVELOPMENT

Electronic Components and Systems are a pervasive Key Enabling Technology, impacting all industrial branches and almost all aspects of life.

ECSEL JU offers funding for Research, Development and Innovation projects with unparalleled systemic and strategic impact for smart, sustainable and inclusive economic growth.

> NEXT

SMART MOBILITY	KEY APPLICATION
SMART SOCIETY	
SMART ENERGY	
SMART HEALTH	
SMART PRODUCTION	
SEMICONDUCTOR PROCESS EQUIPMENT MATERIALS	ESSENTIAL CAPABILITIES
CYBER PHYSICAL SYSTEMS	
SAFETY AND SECURITY	
DESIGN TECHNOLOGY	
SMART SYSTEMS INTEGRATION	

NEWSLETTER SEARCH

NEWS

AENEAS is looking for a Director General to lead their organization.
More information [here](#).

17/11/2016 - **Call 2016: ECSEL JU Public Authorities Board publishes decision on funding.**
The relevant decisions can be found under [DOCUMENTS](#) (click here).
Update: See the Press-release [HERE](#).

ECSEL JU is procuring for a web-site host and design (18/11/2016) a corporate video-clip production (25/11/2016) and a technical writer (25/11/2016)
See [Procurement](#) for details

New ECSEL JU publications already available to download!
Go to [Publications](#) and take a look at our new flyer & ECSEL Book of Projects!

Example of Shift2Rail PPP (Railroad)

The screenshot shows the Shift2Rail website interface. At the top, there is a navigation bar with the Shift2Rail logo, menu items (Home, About us, Participate, R&D Programme), and the Horizon 2020 European Union Funding for Research & Innovation logo. A search bar is located on the right side of the navigation bar. Below the navigation bar, a large blue banner features the text "2017 call for proposals published" in white. Underneath the banner is a stylized illustration of a cityscape with buildings, wind turbines, and a train. Below the illustration, there are four dots indicating a carousel. The main content area is divided into three columns. The left column is titled "About the Initiative" and contains text about the project's goals and funding. The middle column is titled "S2R in the News" and features a small image of a train and a circular graphic with the text "Call for Proposals". The right column is titled "News" and lists several recent updates with dates and brief descriptions. A "read more" button is located below the "About the Initiative" section, and a "view all" button is located below the "News" section.

Member Area

Shift2Rail

Home About us · Participate · R&D Programme ·

Horizon 2020
European Union Funding
for Research & Innovation

Search

2017 call for proposals published

About the Initiative

Shift2Rail will be the first European rail joint technology initiative to seek focused research and innovation (R&I) and market-driven solutions by accelerating the integration of new and advanced technologies into innovative rail product solutions. Shift2Rail will promote the competitiveness of the European Rail Industry and will meet the changing EU transport needs. Through the R&I carried out within this Horizon2020 Initiative, the necessary technology will be created to complete the Single European Railway Area (SERA).

read more

S2R in the News

November 23, 2016
Shift2Rail Information Day – Open Calls for Proposals 2017

Call for Proposals

News

November 23, 2016
Shift2Rail Information Day – Open Calls for Proposals 2017
The Shift2Rail Joint Undertaking is pleased to announce the Information Day – Open Calls for [...]

November 11, 2016
Call for proposals 2017 now published
The Shift2Rail joint undertaking (S2R JU) has published the 2017 call for proposals and its Annual [...]

November 8, 2016
Shift2Rail 2015/16 projects now fully operational
Press release: Shift2Rail 2015/16 projects now fully operational [PDF] More info: Call for Proposals [...]

October 20, 2016
Shift2Rail Executive Director to speak at International Railway Summit
Press release: Shift2Rail Executive Director to speak at International Railway Summit [PDF] [...]

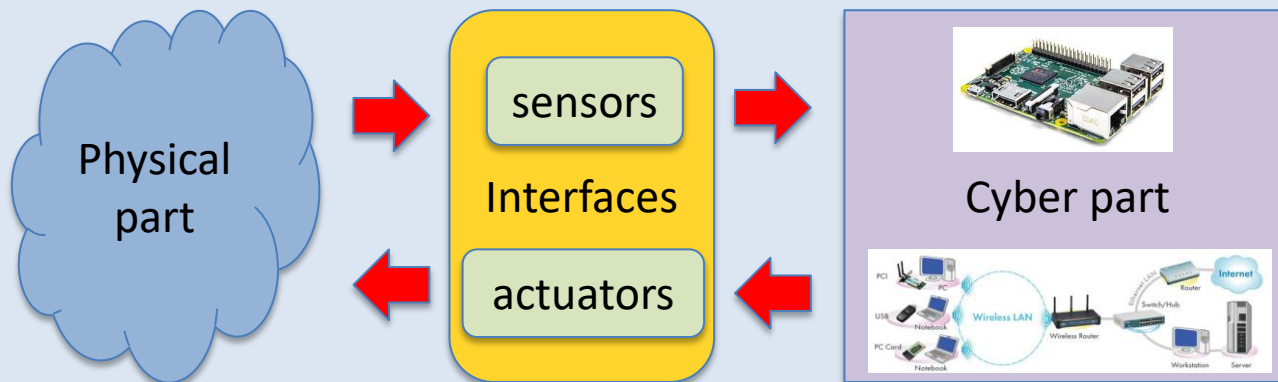
view all

Challenges in CPS Safety and Security

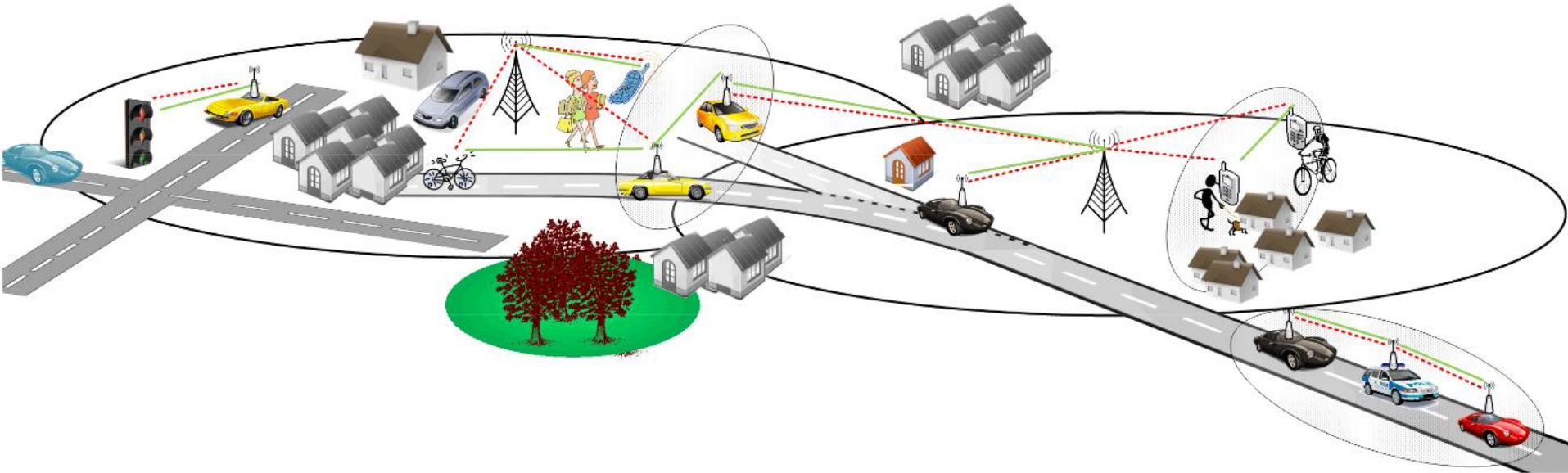
- Growing trend to connect the related cyber-physical systems to the Internet
 - Transport domain (automotive or railway)
 - Smart cities
 - Smart manufacturing
 - ...
- Possibly exposes safety critical cyber-physical systems to a new range of threats which are constantly evolving

Growing Adoption of CPS

- Automotive
- Railway
- Aerospace
- Space
- Energy
- Manufacturing
- ...



Intelligent Transport Systems - Automotive



Digital Railways?

From paper, physical indications...



Physical World



...to data, digital (mobile) communication, "Internet of Things"



Digital World

"Data enabled railway"



... applied to processes across the entire value chain (passengers and freight)

Digital Railways & e-transport

Digital Railways as a component of e-transport

(e-transport = one of the digital services required by the Digital Single Market Strategy of the EU)

Digital railways are aimed at increasing:

Competitiveness

Reliability

Efficiency

Effectiveness

Capacity

Availability

Accessibility

Attractiveness

Safety

(Cyber)security

Railways

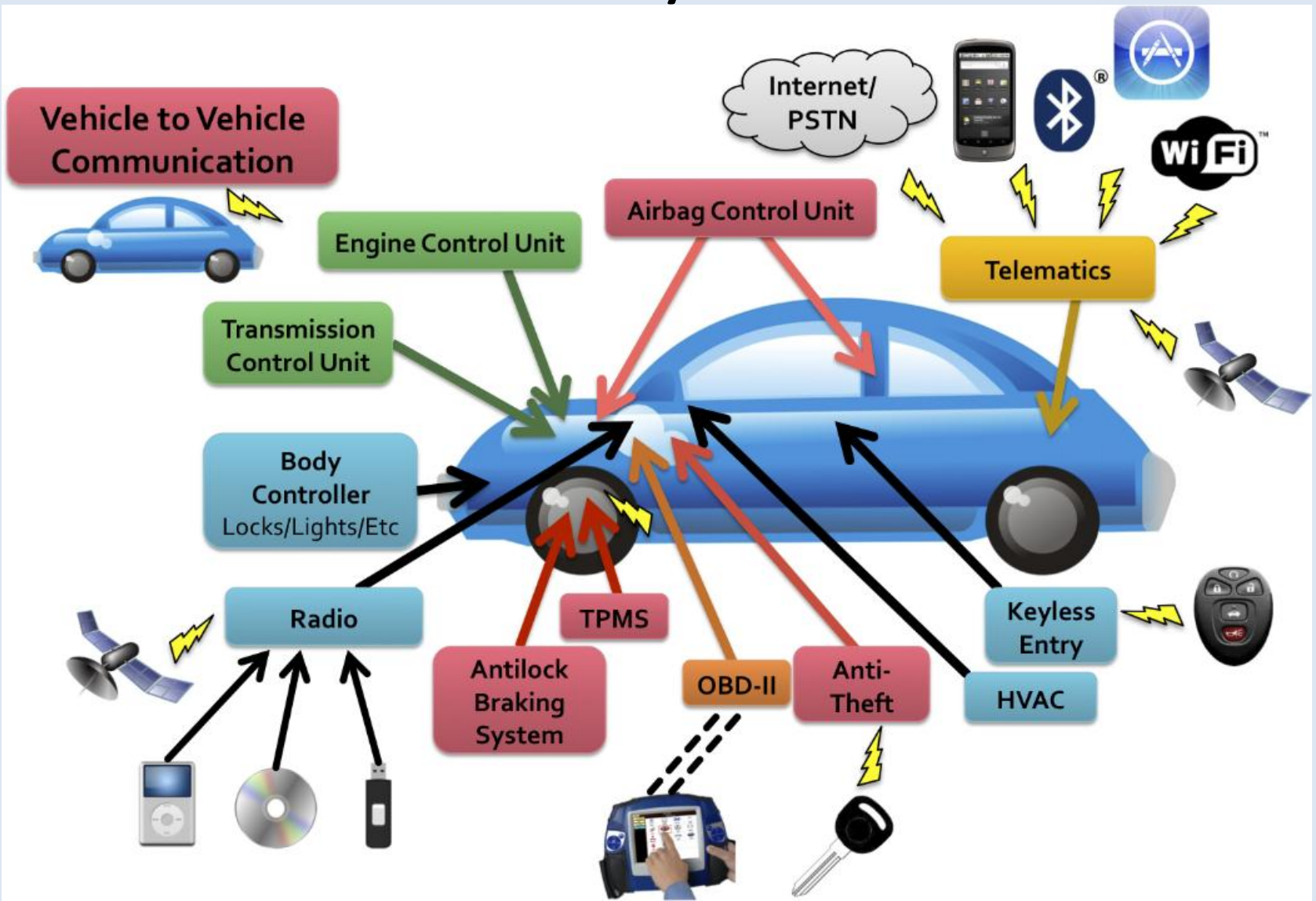


OVERVIEW OF SHIFT²RAIL

INCREASED CAPACITY, CONSOLIDATED RELIABILITY
FOR EFFICIENT AND SUSTAINABLE RAIL TRANSPORT
AND A COMPETITIVE EUROPEAN RAIL INDUSTRY



Automotive Case Study: connected car sub-system



Example Threats

Researchers take control of car (not life threatening)

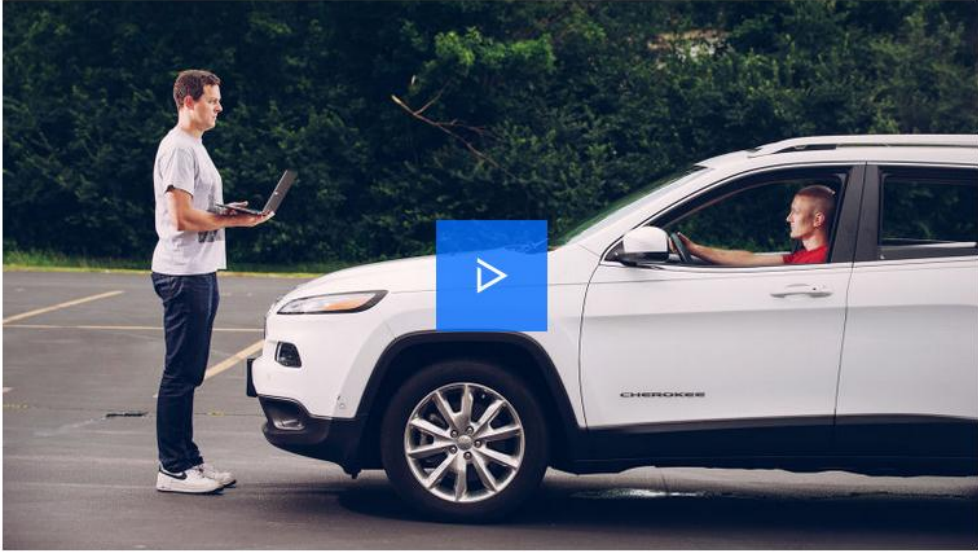
- Cold air blowing at max
- In-seat climate control
- Radio station switched at full volume; control knobs no longer working
- Windshield wipers turned on, wiper fluid blurs glass
- Photo of hackers displayed on digital display

Zero-day exploit from laptop:

- Wireless control via internet
- Access to entertainment system, dashboard functions, steering, brakes, and transmission

ANDY GREENBERG SECURITY 07.21.15 8:00 AM

HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT



SHARE

f SHARE 2594

t TWEET

p PIN 3

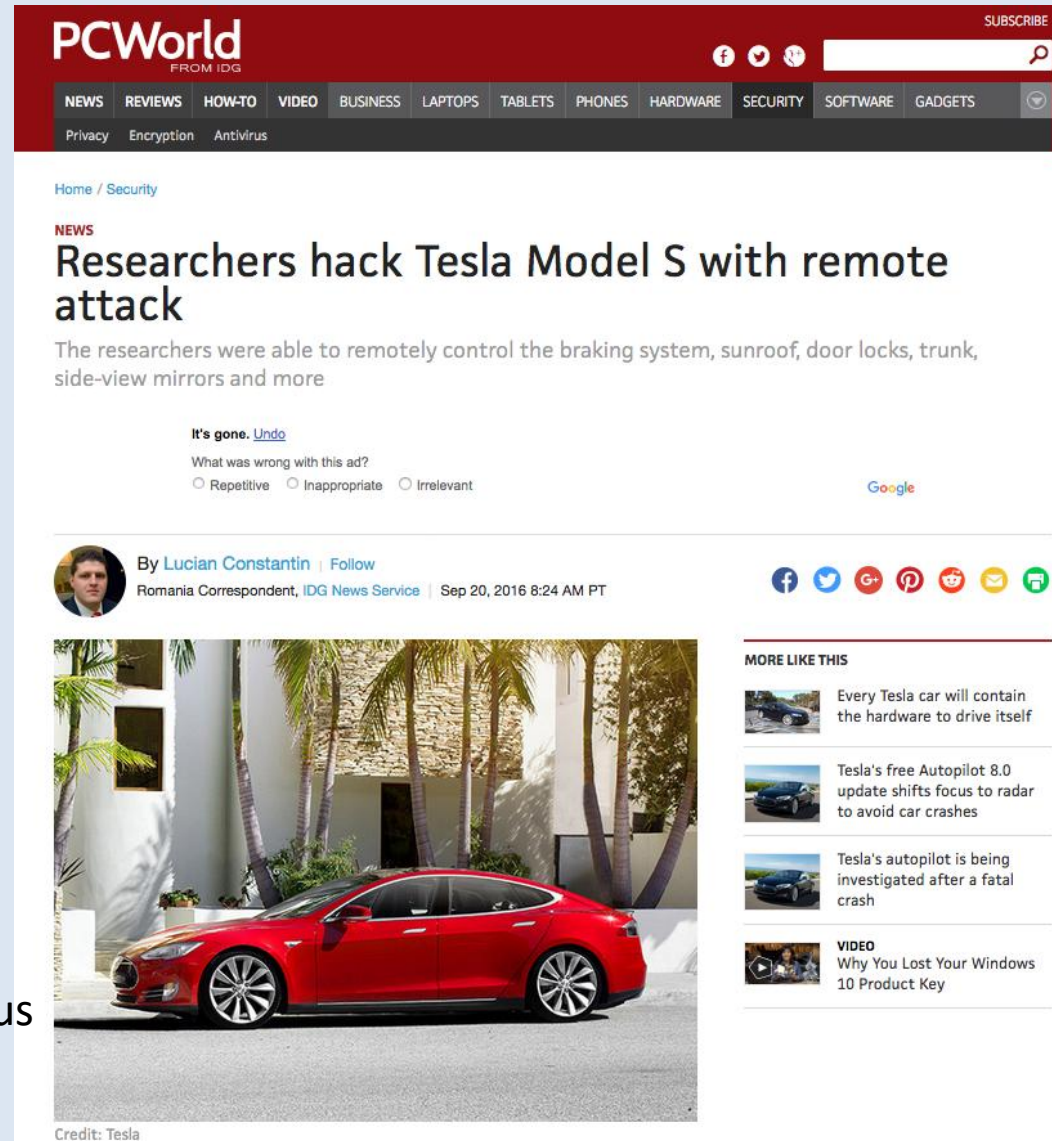
I WAS DRIVING 70 mph on the edge of downtown St. Louis when the exploit began to take hold.

Though I hadn't touched the dashboard, the vents in the Jeep Cherokee started blasting cold air at the maximum setting, chilling the sweat on my back through the in-seat climate control system. Next the radio switched to the local hip hop station and began blaring Skee-lo at full volume. I spun the control knob left and hit the power button, to no avail. Then the windshield wipers turned on, and wiper fluid blurred the glass.

Another Example

- Researchers from Chinese technology company Tencent found a series of vulnerabilities
- When combined, allowed them to remotely take over a Tesla Model S car
- Control
 - Sunroof,
 - central display,
 - door locks and even the
 - braking system

Even though it is a cybersecurity-conscious with car manufacturer bug bounty program



The image shows a screenshot of a PCWorld article. The page has a red header with the PCWorld logo and navigation tabs for NEWS, REVIEWS, HOW-TO, VIDEO, BUSINESS, LAPTOPS, TABLETS, PHONES, HARDWARE, SECURITY, SOFTWARE, and GADGETS. The article title is "Researchers hack Tesla Model S with remote attack" and the sub-headline is "The researchers were able to remotely control the braking system, sunroof, door locks, trunk, side-view mirrors and more". The author is Lucian Constantin, a Romania Correspondent for IDG News Service, and the article was published on Sep 20, 2016 at 8:24 AM PT. The article includes a photo of a red Tesla Model S car parked in front of a building with palm trees. The credit for the photo is Tesla.

PCWorld
FROM IDG

NEWS REVIEWS HOW-TO VIDEO BUSINESS LAPTOPS TABLETS PHONES HARDWARE SECURITY SOFTWARE GADGETS

Privacy Encryption Antivirus

Home / Security

NEWS

Researchers hack Tesla Model S with remote attack

The researchers were able to remotely control the braking system, sunroof, door locks, trunk, side-view mirrors and more


It's gone. [Undo](#)

What was wrong with this ad?

Repetitive Inappropriate Irrelevant




Google

By [Lucian Constantin](#) | Follow
Romania Correspondent, IDG News Service | Sep 20, 2016 8:24 AM PT




Credit: Tesla

MORE LIKE THIS

-  Every Tesla car will contain the hardware to drive itself
-  Tesla's free Autopilot 8.0 update shifts focus to radar to avoid car crashes
-  Tesla's autopilot is being investigated after a fatal crash

VIDEO

 Why You Lost Your Windows 10 Product Key

Current Approaches to link Safety and Security Engineering

- 4 potential approaches to link safety and security (cfr ITEA Merge project):

[HOME](#)[OVERVIEW](#)[CONSORTIUM](#)[DISSEMINATION](#)[PROJECT WIKI](#)[EVENTS](#) ▼[DOWNLOAD](#) ▼[CONTACT US](#)

Multi-Concerns Interactions System Engineering

The ITEA 2 project MERgE, aims to develop and demonstrate innovative concepts and design tools to address multi-concerns interactions in systems, targeting the elaboration of effective architectural solutions with a focus on safety and security.



Comparison of Safety and Security Engineering

	Safety Engineering	Security Engineering
Goal Category	Safety Goal	Security goal
Obstacle variant	Hazard	Anti-goal (or Threat)
Finest refinement	Root cause	Vulnerability
Agent	Environment (unexpected)	Attacker (malicious)
Impact	Damage to people and things, priority over all other requirements (e.g. availability)	Measured in business terms, e.g. system availability, reputation
Refinement Methods	Fault Tree Analysis, HAZOP, FMECA	Attack trees, Threat trees
Risk management techniques	Obstacle elimination Obstacle reduction Obstacle tolerance (goal restoration)	Vulnerability removal/isolation Attack recovery Attack impact reduction
Analysis Type	Design-time analysis. Update not frequent. But learning from past accident important activity.	Run-time monitoring for discovery of vulnerabilities, suspect behaviours. Frequent updates to patch.
Standards	IEC61508 (generic), ISO26262 (automotive), IEC50128 (railways), DO178B/C, etc	Common criteria

Requirements Engineering

- Definition: The process of eliciting, analyzing, documenting and validating the **services** required of a system and the **constraints** under which it will operate and be developed
- Requirements Specification
 - Natural language Requirements:
 - Ambiguity: several interpretations of requirements
 - Confusion: functions, constraints, goals and design may be mixed
 - Amalgamation; several requirements expressed together
 - Model based approach

Requirements Specification Qualities

- **Completeness:** descriptions of all required services and constraints should be included.

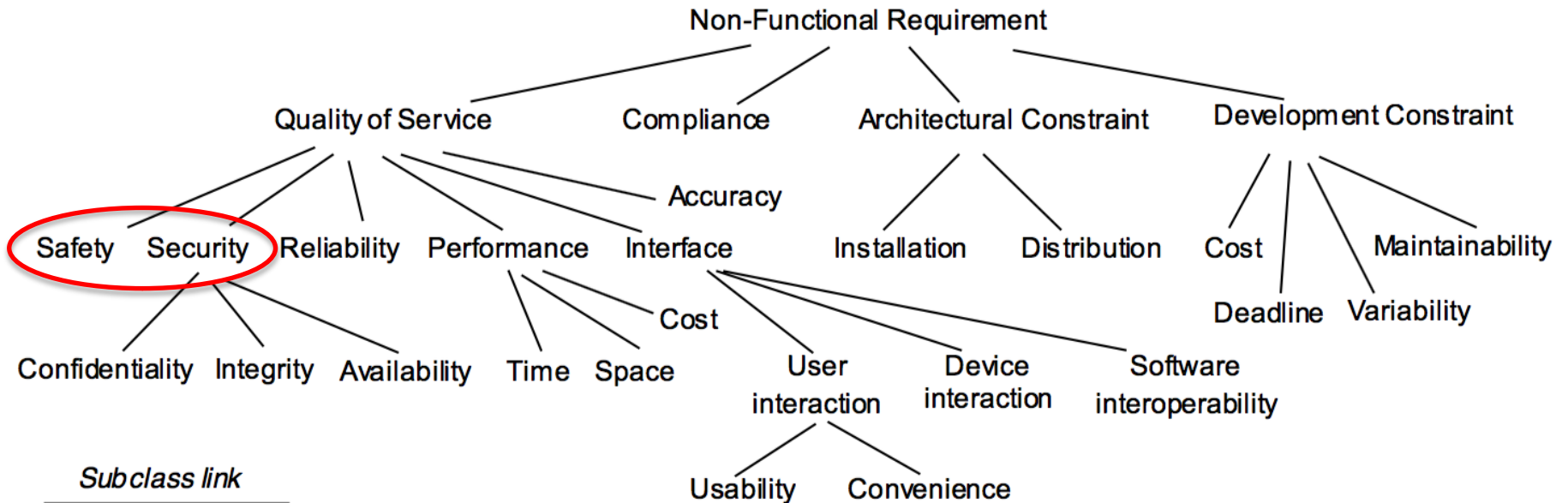
« Requirements \wedge Assumptions \wedge Domain properties \Rightarrow Objectives »

- **Consistency:** there should be no conflicts or contradictions in the descriptions.

« Requirements \wedge Assumptions \wedge Domain properties \neq false »

- ...

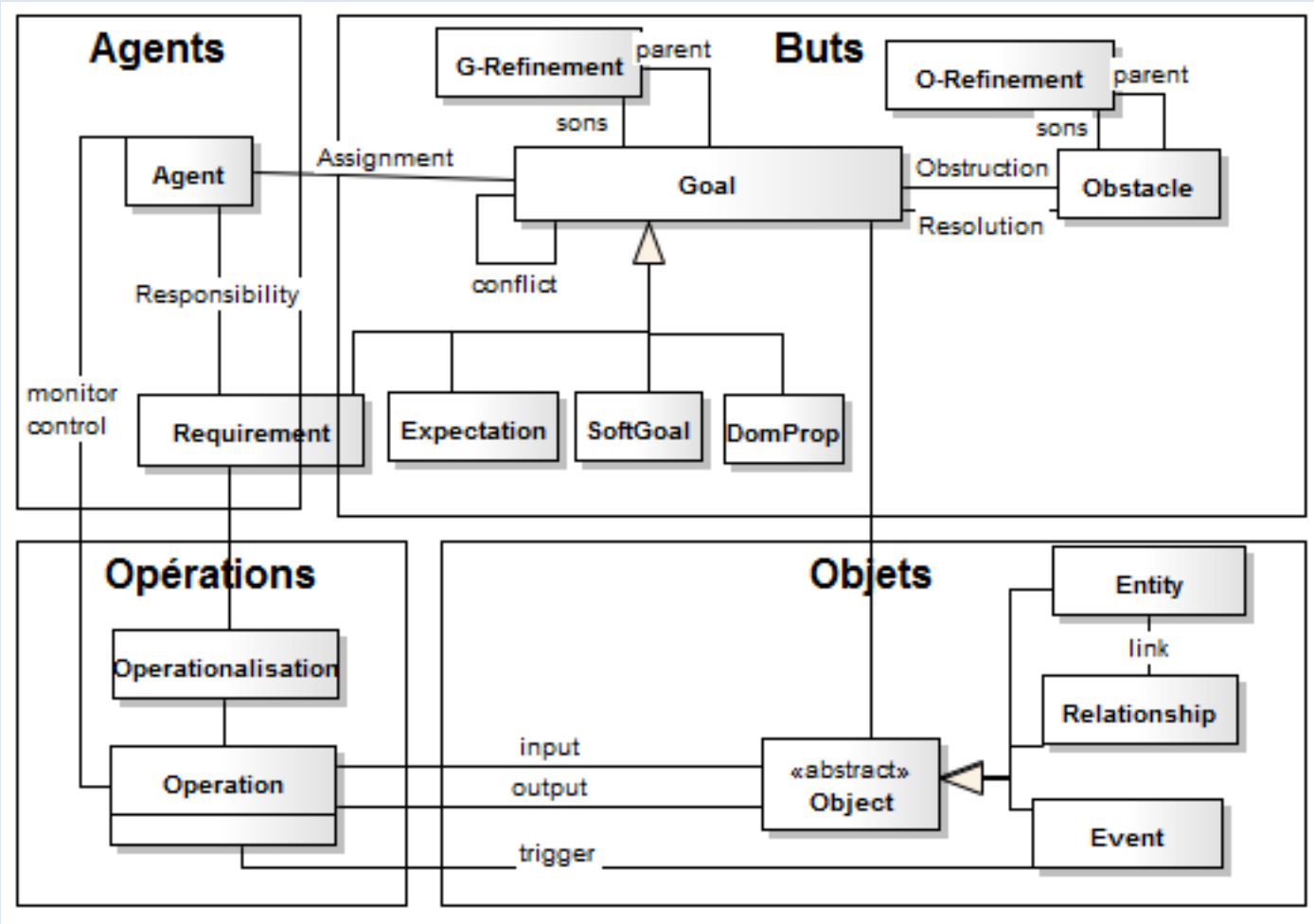
Functional and non-functional Goals



Goal-Oriented RE for Safety and Security CPS

Who?

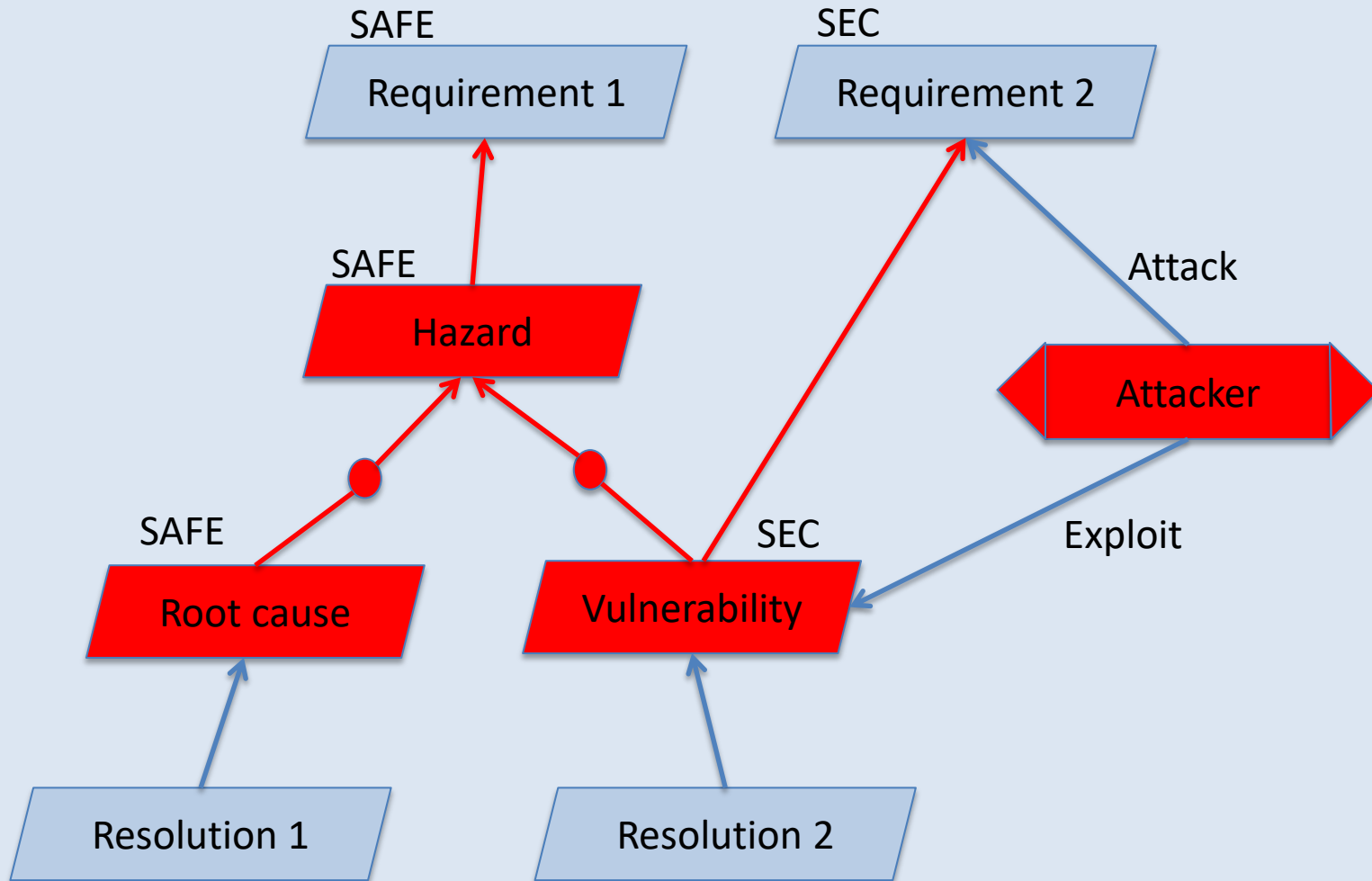
Why?



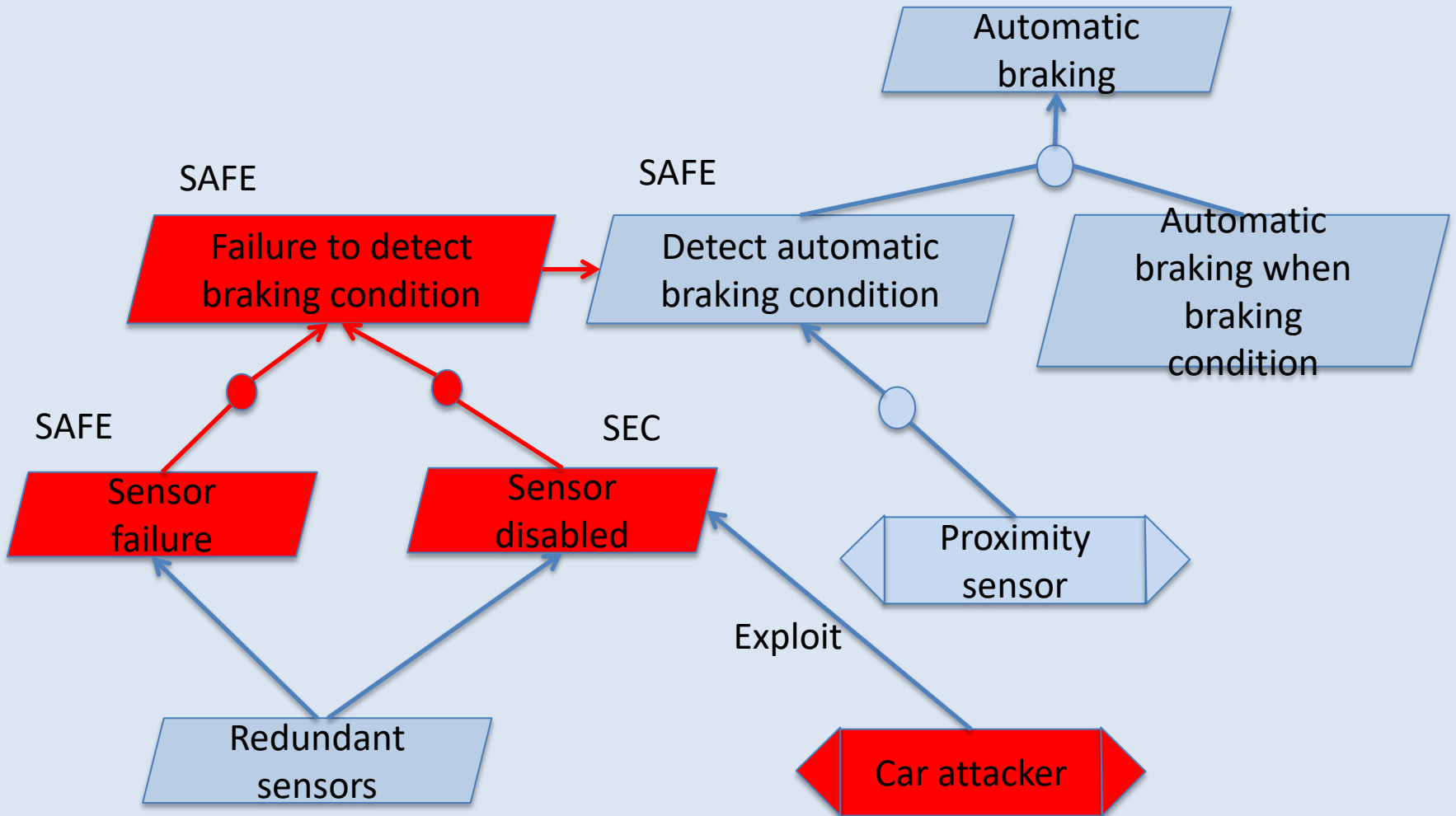
How?

What?

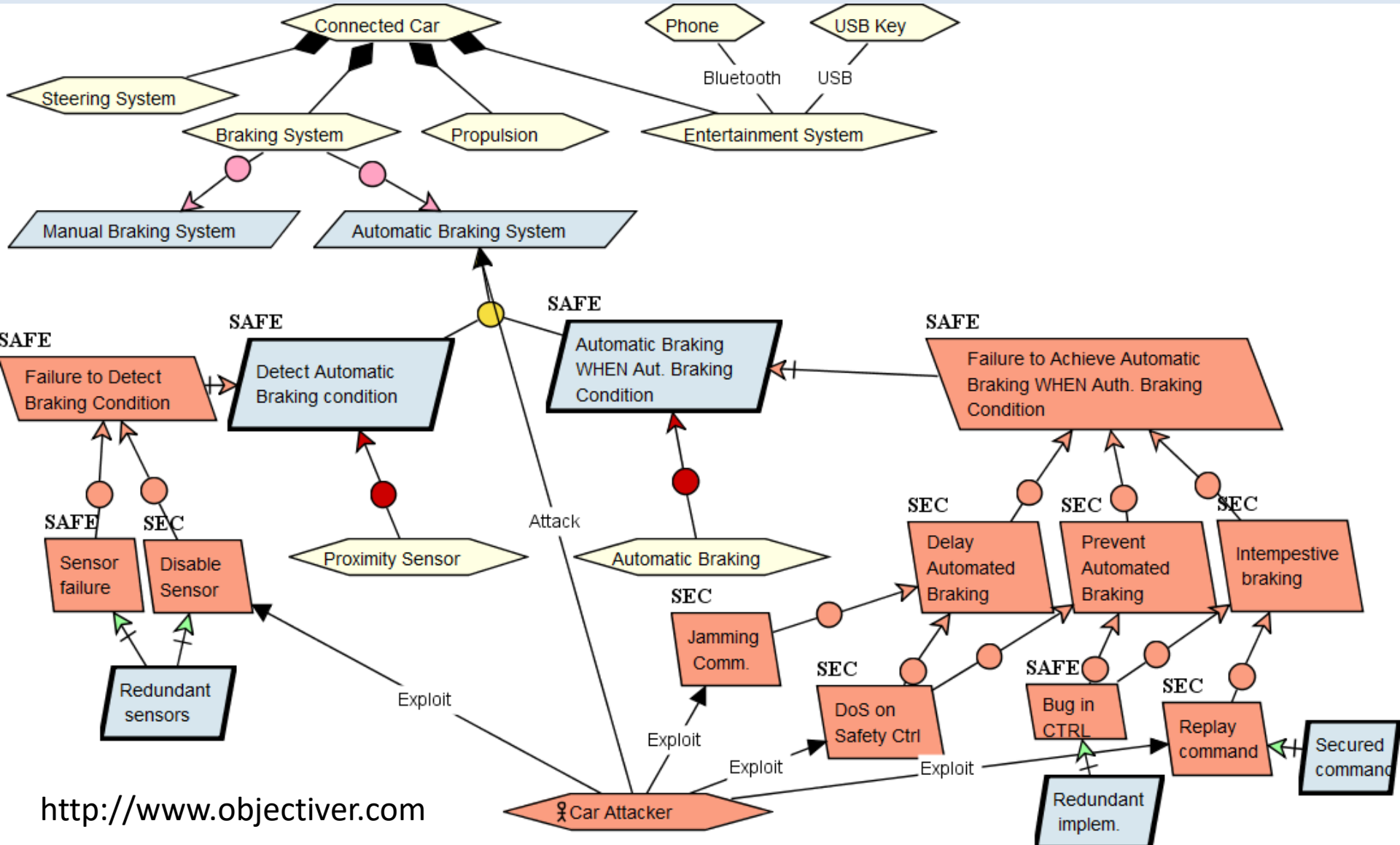
Combining Safety and Security



Attack Tree on Safety Function



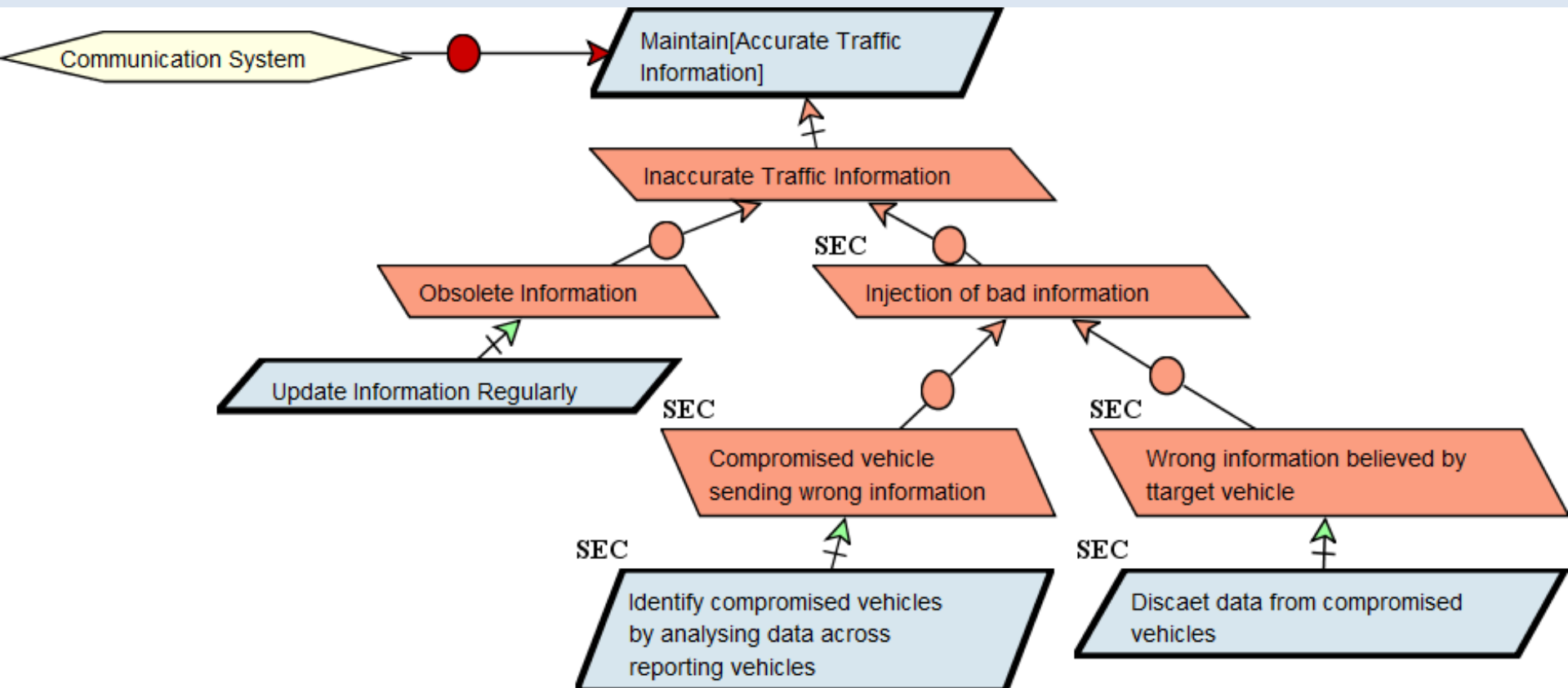
Attack tree on Safety Function



Conclusions and Future Work

- Growing trend to connect the related cyber-physical systems to the Internet
 - exposes connected CPS to new threats
- Co-engineering approach for addressing safety and security requirements in connected CPS
 - goal-oriented requirements engineering for initial specification of security and safety properties
 - safety and security properties
- Automotive case study showing how to model security threats on safety goals
- Future work:
 - Safety and security compliance obligations
 - How to deal with update of security functions at design/run time

Analysis of Distributed Security Problem



How often do Attacks Happen?

De Denise.Francis@stfc.ac.uk ☆

← Répondre

→ Transférer

📁 Archiver

🗑 Indésirable

🗑 Supprimer

Autres ▾

10:47

Sujet **Data Breach Notification**

Pour Moi ☆

Dear Philippe Massonet ,

On 10 November STFC was informed of a cyber-attack by unknown perpetrators against our Event Booking service <https://eventbooking.stfc.ac.uk/> which resulted in a data breach. A copy of the user registration database was extracted. As this database contains your personal information we have a duty under the Data Protection Act to inform you of this incident. The Information Commissioners Office has also been informed.

What personal data is involved?

Name

Address

Telephone Number

Email Address

User ID and password for this service (passwords were encrypted)

Dietary Requirements

What action has already been taken?

STFC have already changed the password associated with your login to this service. If you wish to change your password to regain access, please use the "I've forgotten my password" option within the Login area.

STFC have also undertaken a thorough security assessment of the service and have implemented additional security measures to defend against future cyber-attacks.

Any further advice?

- If the password used for this service is also used for other cloud services e.g shopping or banking, I recommend that you change those passwords as soon as possible.
- Please be extra vigilant for Phishing attacks that may utilise the data found within the database to attempt to extract further personal information from you.
- If you wish to have your data removed from this service, please inform the STFC Information Management Team (STFCInformationManagement@stfc.ac.uk)

Contact Information:

STFC Data Protection Team - STFCInformationManagement@stfc.ac.uk

ICO contact details - <https://ico.org.uk/global/contact-us/>

Further fraud information can be found on the Action Fraud Police web site <http://www.actionfraud.police.uk>

IoT Security Standards

- <http://www.infosecurity-magazine.com/news/us-government-releases-new-iot/#.WDCTUu539uQ.linkedin>
- Recent: <https://www.dhs.gov/securingtheloT>
- Automotive: National Highway Traffic Safety, Administration (NHTSA) recently released guidance on Cybersecurity Best Practices for Modern Vehicles. http://www.nhtsa.gov/About-NHTSA/Press-Releases/nhtsa_cybersecurity_best_practices_10242016
- Railway:

Recommendations for Dealing with Safety and Security in Connected CPS

- Second approach is the most conservative for safety critical systems like transportation
 - Not bring much change in current practices in safety procedures
- Most reasonable choice seems to be the co-engineering
 - Important costs for companies due to the duplication of processes, methods, tools and the need of many synchronization between the approaches
 - Considering security at the service of safety might result in wrong priorities
 - Safety as a means of improving security will not achieve the safety objectives of CPS.

Combining Safety and Security

