

FIRE

Gateway to trustworthy ICT innovations in Europe



PROJECT FULL TITLE: Facilitate Industry and Research in Europe

GRANT AGREEMENT N. 318762

D7.2

End-user inputs to final pan-cluster strategy/research agenda

Due Date: M21

Main Author: AMETIC

Contributors: All partners

Dissemination: CO

Document Control Sheet

Project Number 318762

Project Acronym FIRE

Work-package:

Last Version:

Issue Dates:

Version 1 01/05/2014 *Initial version*

Version 3 06/11/2014 *Final version*

Classification

This report is:

Draft	
Final	X
Confidential	X
Restricted	
Public	

Table of contents

1 INTRODUCTION AND PURPOSE OF THE REPORT	5
2 CONTEXT	5
3 CHANGES FROM DRAFT RECOMMENDATIONS	5
3.1 Overview of the draft recommendations (D4.2)	5
3.2 Summary of recommendations	5
3.2.1 Themes.....	5
3.2.2 Topics	6
3.2.3 Domains	6
3.2.4 Themes – user focus.....	6
3.3 Suggested New Topics and observations from Advisory Board	7
3.3.1 Convenience.....	7
3.3.2 Embedded Security	7
3.3.3 Privacy of Connected Cars.....	7
3.3.4 Authentication.....	7
3.3.5 Securing personal information from Governments.....	7
3.3.6 Behavioural Analysis to address Insider Threat.....	7
3.3.7 Trusted Archival Services.....	7
3.3.8 Log Data Management for SCADA	7
3.3.9 Enhancing security information exchange	7
3.3.10 User-Centric design rather than technical security design.....	7
3.4 New topics from RN, ICN and IT industry reviewers.....	7
3.4.1 Hardware based security approaches/ embedded security	7
3.4.2 Supply chain security	7
3.4.3 Modelling	8
3.4.4 Lessons from Biology	8
3.4.5 Surveillance of vulnerable people by monitoring of health parameters, activity and life style	8



3.4.6 Social impact analysis of new ICT products and services. 8

1 INTRODUCTION AND PURPOSE OF THE REPORT

The aim of this report is to provide a description of the recommendations given by the end-users to feed the Pancluster Strategy Research Agenda.

This report represents Deliverable D7.2 from Task 7.1 of the FIRE project. This report is intended as an internal project report for use by the FIRE consortium and the European Commission.

2 CONTEXT

The first draft of the pan-cluster strategy and research agenda was presented to European Commission in the year 1. The objective for the year 2 was to submit it to the Advisory Board and other groups of stakeholders, in order to get their feedback to build the final version (deliverable D7.3).

3 CHANGES FROM DRAFT RECOMMENDATIONS

3.1 Overview of the draft recommendations (D4.2)

The draft research recommendations contained **32 Topics** which naturally grouped into **6 Themes** as below:

1. Establishing trustworthy relationships
2. Information privacy, assurance and cyber security
3. Addressing implications of trends in scale and complexity
4. Encouraging and supporting appropriate user behaviour
5. Proving fitness for purpose
6. Cross-Cutting research topics

The draft contained detailed reference to methodology employed in gathering User Needs that from the key domains identified in the statement of work:

- Energy
- Finance
- Health
- Mobile Communications
- and contributions relating to e-Government.

The draft acknowledged that there was a degree of subjectivity in linking research objectives to user needs rather than to technology and that it would be equally legitimate to base the Themes around key developments like Big Data, Cloud Computing and the Internet of Things (IoT). While acknowledging the importance of technology, the draft deliberately proposed focusing on research linked to needs in order to maximize the relevance of research to the non-research community.

3.2 Summary of recommendations

3.2.1 Themes

The reviewers supported the concept of grouping research topics into Themes. All recognized that there was some subjectivity in the grouping into themes. For some reviewers there was a question as

to whether the Themes should be technology based while others immediately supported the idea of themes being user-centric. After discussion all participants unanimously endorsed the approach of user-centric Themes.

Themes 1 to 5 were accepted by the reviewers although some minor text revision was recommended to enhance their crispness and clarity.

Theme 6 caused more comment and it was recommended that the topics in this area be placed under other Themes or discarded.

Several reviewers felt that there was a potentially important Theme missing. It was variously described but encompassed embedded, distributed systems whose primary functions were control and monitoring. Terms like cyber-physical, embedded, SCADA, ICS, IoT were used in trying to capture this idea. Our new Theme 6 “**Cyber-Physical System Security**” is our attempt to capture these ideas.

3.2.2 Topics

Participants were highly supportive of the Topics that were proposed. They did make the following suggestions:

1. While acknowledging that the descriptions have arisen from end-users who use different vocabulary, it helps researchers if they are all written in a similar style.
2. Several reviewers proposed new Topics or extensions to Topics
3. In some of the review fora an opportunity was provided to identify the most important topics and these results are summarised in Section **¡Error! No se encuentra el origen de la referencia..**

We are grateful to our reviewers for their time and for the detailed consideration that they gave to the draft research agenda and have responded to the suggestions as followed:

1. We have re-drafted all the Topic descriptions using the approach of first describing the issue and then outlining the need for research. We have aimed to use non-domain-specific terminology in doing so.
2. We have accepted the proposed new Topics and this has resulted in 8 additions to the number of Topics.
3. The summary of Topics is presented in **¡Error! No se encuentra el origen de la referencia..**

3.2.3 Domains

Both the project Partners and our reviewers felt that better coverage of the Government domain may be beneficial. The project agreed to add a further section on user requirements derived from Government and to extend the limited observations that had been gathered and which had been drawn from e-Government only. These will be included separately in a further revision of the user requirement document (D3.2).

3.2.4 Themes – user focus

We thank our reviewers for their exploration of the best way of aggregating Topics into a smaller number of more manageable, headings or Themes. Following the discussion we are encouraged by the endorsement of the user-centric approach which we carry forward in this document.

3.3 Suggested New Topics and observations from Advisory Board

The following items were offered as suggestions by the project's Advisory Board for consideration in the Research Agenda. Some of these will be incorporated as new Topics; others will provide additional text for existing Topics.

3.3.1 Convenience

This has been added as Topic 33 in Theme 4.

3.3.2 Embedded Security

This has been added as Topic 34 in new Theme 6.

3.3.3 Privacy of Connected Cars

This has been added as Topic 35 in new Theme 6.

3.3.4 Authentication

This has been added as Topic 36 in Theme 1, separating people-based authentication from that of authentication of things.

3.3.5 Securing personal information from Governments

This is a new item from the domain of Government and has been added as Topic 37 in Theme 2.

3.3.6 Behavioural Analysis to address Insider Threat

This has been added as Topic 38 in Theme 4.

3.3.7 Trusted Archival Services

This has been added as Topic 39 in Theme 2.

3.3.8 Log Data Management for SCADA

This is covered in Topic 15.

3.3.9 Enhancing security information exchange

This is covered by Topics, 7,10,24,25, 27 and 36.

3.3.10 User-Centric design rather than technical security design

This is covered in Topic 20.

3.4 New topics from RN, ICN and IT industry reviewers

The following potential new Topics were proposed by the reviewers and the following actions have taken place:

3.4.1 Hardware based security approaches/ embedded security

This area was suggested by Advisory Board and incorporated in new Topic 34.

3.4.2 Supply chain security

Cyber security of parts in the supply chain e.g. recycled IT parts (SC, etc.), as the forensic provenance of hardware is important. It is incorporated in Topic 29.

3.4.3 Modelling

Where is the modelling environment in these topics? Modelling is included within suggested research activities but not always explicitly.

- The Research Network will be asked whether there are important research needs relating to underpinning modelling capabilities that should be highlighted perhaps as stand-alone topics.

3.4.4 Lessons from Biology

For example, can we learn from the evolution of the immune response to infection when it comes to dealing with Malware? There has been research in this domain e.g. US Department of Homeland Security funded research into Nature-Inspired Cyber Health.

- The Research Network will be asked whether this is an area where further research investment would add value.

3.4.5 Surveillance of vulnerable people by monitoring of health parameters, activity and life style

This has similarities to Topic 8 and Topic 19 but has some subtly different nuances and has been added as new Topic 40

3.4.6 Social impact analysis of new ICT products and services.

This has been incorporated into revised wording for Topic 8 which covers broadly similar objectives.