Report on Deliverable D10.2

Strategic Analysis of the Supported Topics 2019

Workpackage		10		
Task		10.2		
Date of delivery	**Contractual**	Month 20 (July 2018)		
	Actual	Month 27 (February 2020)		
Code name		D10.2	Version 1	Draft ☐ Final ☒
Type of deliverable		Report		
Dissemination level		Public		
Contact(s)		Florence Quist	florence.quist@frs-fnrs.be	
WP/Task leader		Florence Quist	florence.quist@frs-fnrs.be	
EC project officer		Julian Ellis		
Publishable abstract		The report presents the analysis of the outcome of the funded projects in the Call 2014 topics: • Resilient Trustworthy Cyber-Physical Systems (RTCPS) • Human Language Understanding: Grounding Language Learning (HLU) It also gives insight into the evolution of those topics.		
Keywords		Strategic analysis, supported topics, Call 2014		

Content Table

1. Overview of CHIST-ERA III Task Related to D10.4

The task (T10.2) related to the deliverable 10.2 covers the strategic analysis for the topics funded by CHIST-ERA calls. This task entails an analysis of the results obtained by on-going projects and aims at the definition of suitable criteria for the identification of emerging research communities and their maturity. In addition, an analysis of the needs and opportunities of research projects for specifically identified topics is conducted in order to determine their compatibility with possible future ICT programmes. Deliverables of this task, D10.1 and following, will be made available to the FET community and other fora.

2. Analysis and recommendation for the process

a. Scope of Deliverable 10.2

In order to allow for maturation of both funded projects and topic, the deliverable 10.2 focuses on the topics of the Call 2014:

- Resilient Trustworthy Cyber-Physical Systems (RTCPS)
- Human Language Understanding: Grounding Language Learning (HLU)

Indeed, projects of the Call 2014 finished in 2019. During their lifetime, the corresponding research communities could form, exchange and present their vision of the future of their topics thanks to 4 editions of the CHIST-ERA yearly projects seminar.
This deliverable draws on the work performed in task 9.2 Project follow-up and monitoring (for projects from all calls except Call 2017) and in task 10.3 Project Seminar organisation.

b. Analysis of the Topic *Resilient Trustworthy Cyber-Physical Systems (RTCPS)*

i. Evolution of the Funded Projects

Four projects were funded in the RTCPS topic and the specific scope of each project is detailed in the table below:

Name	Project goals
COPES	***COnsumer-centric Privacy in smart Energy gridS*** Develop new technologies to protect consumer privacy, while not sacrificing the advanced control and monitoring functionalities of smart meters. The core idea is to overlay the original consumption pattern with additional physical consumption or generation, thereby hiding the consumer privacy sensitive consumption. The means to achieve this include the usage of storage, small scale distributed generation and/or elastic energy consumptions.
DYPOSIT	***Dynamic Polies for Shared Cyber-Physical Infrastructures Under Attack*** Tackling of the problem of large, shared CPS (cyber physical systems) infrastructures under attack. The project aims to develop a novel dynamic policies approach rooted in a socio-technical understanding of the complexity and dynamics of shared CPS fabrics under attack.
I-DRESS	***Assistive Interactive Robotic System for Support in Dressing*** Development of a robotic system that will provide proactive assistance with dressing to disabled users or users such as high-risk health-care workers, whose physical contact with the garments must be limited during dressing to avoid contamination.
SECODE	***Secure Codes to Thwart Cyber-Physical Attacks***

	Specification and design of error correction codes suitable for an efficient protection of sensitive information in the context of Internet of Things (IoT) and connected objects in order to mitigate passive attacks, like memory disclosure, and active attacks, like stack smashing.

Together, those 4 projects address issues on:

1. Information security
2. Human factors
3. Resilience
4. Personal information

From the progress reports by the participating teams and the review reports by the scientific experts appointed by CHIST-ERA, we can conclude that in general the projects progressed according to the initial plan and generated relevant results, as detailed in the table below:

Name	Project major outcomes
COPES	• Development of innovative privacy-preserving energy flow control strategies based on a Markov decision process approach using privacy measures based on mutual information or unauthorized Bayesian hypothesis testing
DYPOSIT	• Development of 5 software prototypes/CPS testbeds: ○ SENAMI: Selective Non-Invasive Active Monitoring for ICS Intrusion Detection ○ Specialised Vulnerability Scanner for Industrial Control Systems ○ CerberOS: a CPS Operating System for IETF Class-1 devices ○ MicroPnP, an integrated hardware, software, and networking solution ○ Model for dynamic change in an ICS security configuration ○ LASARUS: Lightweight attack surface reduction for legacy ICS
I-DRESS	• Development of 2 prototypes of single-armed robot dressing assistants ○ Human-human interaction study ○ Adaptation through multimodal interaction ○ Robot learning and task planning ○ Safety planning • Development of innovative software
SECODE	• Development of a software which automatically generates protections based on codes at compile-time

ii. Evolution of the Topic

As part of the Projects Seminar's format, the projects in the same topic were invited each year to reflect on their progress and on the key challenges that still need to be tackled in their specific field. They produced presentations that are made public and available from the CHIST-ERA website (http://www.chistera.eu/funded-topics). The following challenges were identified during the Projects Seminar 2019:

- Resilient trustworthy CPS
  - ✓ Under studied security and privacy risks
  - ✓ Evaluation of efficacy including human factors
- Embedded security, privacy and resilience
  - ✓ Generic security parameters
  - ✓ Study of Inner-Product masking codes at Byte/bit security level
  - ✓ Impact of code properties on security order

c. Analysis of the Topic *Human Language Understanding (HLU)*

i. Evolution of the Funded Projects

Six projects were funded in the HLU topic and the specific scope of each project is detailed in the table below:

Name	Project goals
AMIS	***Access Multilingual Information opinionS*** Development of a text, audio and video summarizing tool through the use of Automatic Speech Recognition (ASR). Cross-lingual sentiment analysis by using the previously developed tool and comparing the translated texts from different media addressing the same topic in different languages.
ATLANTIS	***Artificial Language understanding In robotS*** Understanding and modeling the very first stages in grounded language learning: how pointing or other symbolic gestures emerge from the ontogenetic ritualization of instrumental actions, how words are learned very fast in contextualized language games, and how the first grammatical constructions emerge from concrete sentences. Development of a global, computational theory of symbolic development.
IGLU	***Interactive Grounded Language Understanding*** Development of a robotic agent that will incorporate models of dialogues, human emotions and intentions as part of its decision-making process, through a developmental approach where knowledge grows in complexity while driven by multimodal experience and language interaction with a human. Development of advanced machine learning methods (combining developmental, deep and reinforcement learning) to handle large-scale multimodal inputs, besides leveraging state-of-the-art technological components involved in a language-based dialog system available within the consortium. Evaluations of learned skills and knowledge by using an integrated architecture in a culinary use-case, and novel databases enabling research in grounded human language understanding will be released.
M2CR	***Multimodal Multilingual Continuous Representations for HLU*** Design a unified DL architecture Address major HLU tasks by one unified architecture: speech understanding and translation, multilingual image retrieval and description, etc. Multiple languages and modalities
MUSTER	***MUltimodal processing of Spatial and Temporal ExpRessions*** Improvement of performance of automated understanding of human language: exploitation of visual and perceptual input in the form of images and videos coupled with textual modality for building structured multi-modal semantic representations for the recognition of objects and actions, and their spatial and temporal relations.
ReGROUND	***Relational Symbol Grounding through Affordance Learning*** Development of a novel approach to grounding that lifts it to the relational level. Application to a robot operating in a kitchen-like environment. The robot will be trained by being presented with a series of demonstrations involving inputs from multiple modalities (language and perception). Then, it will be evaluated by being placed in an unseen environment where it will be forced to adapt to its new setting and interpret, possibly unimodal input (i.e., only language or only perception), in order to correctly carry out the requested tasks.

Together, those projects address the following issues:

- Modeling of high-level semantic and pragmatic knowledge in a robust way
- Use of varied data and consideration of the situational context

From the progress reports by the participating teams and the review reports by the scientific experts appointed by CHIST-ERA, we can conclude that projects progressed generally according to the initial plan and generated relevant results, as detailed in the table below:

Name	Project major outcomes
AMIS	• Creation of a system that can translate and summarize video from a source language to a target language
ATLANTIS	• Development of a framework for the representation of how meaning comes about in context
IGLU	• Development of original algorithms for neural networks solutions with VQA and AQA • Implementation of the pipe line architecture for incremental learning – UNIZAR and of GUESWHAT?! for a VQA game
M2CR	• Creation of data an deep learning models to train systems for multi-modal and multi-lingual HLU tasks
MUSTER	• Advances in learning continuous multi-modal representations and studying their properties
ReGROUND	• Combination of language grounding, object anchoring and reasoning in a principled fashion though probability calculus

ii. Evolution of the topic

As part of the Projects Seminar's format, the projects in the same topic were invited each year to reflect on their progress and on the key challenges that still need to be tackled in their specific field. They produced presentations that are made public and available from the CHIST-ERA website (http://www.chistera.eu/funded-topics). The following challenges were identified in 2019:

- Topic major achievements and outputs
  - ✓ Modelling of the transfer between modalities across different contexts: positive results from mapping between and combining data of various modalities
  - ✓ Evaluation of system performance: designing tasks where meaningful evaluation is possible; subjective evaluations of entire systems and programs
- Upcoming challenges and needs
  - ✓ Affordances in grounded language learning
  - ✓ Embodiment and language learning agents
  - ✓ Identifying and modelling potentially multi-modal context
  - ✓ Designing the "right task" for the question being asked
  - ✓ Generalization from event-specific training – avoiding the learning of bias

3. General comments

Based on the scope of the supported topics and the progress and analysis of the funded projects about what still needs to be investigated, certain future calls from the ICT Work Programme 2018-2020 and EIC pilot Work Programme 2018-2020 are identified as being of interest to the CHIST-ERA Call 2014 research communities. The identified specific calls come in complement to the FETOPEN-01-2020 call.

Topic	Relevant Horizon 2020 Work programme : ICT, EIC pilot and Secure societies WP 2018-2020
RTCPS	• **ICT-50-2020: Software Technologies** Specific Challenge: The increased complexity of present and emerging ICT systems poses several challenges at software and hardware level including new requirements in terms of integration and cybersecurity. Users require seamless connectivity, abundant computing power and unlimited access to data independently of the underlying infrastructure. Increased levels of adaptability is becoming more and more essential in modern ICT systems in order to manage the needs of highly complex and dynamic environments pushing for continued development and operation (DevOps). Increasing trust, security, reliability while keeping system performance and reducing energy consumption has become non trivial, in a world where billions of devices processing zetabytes of data have to be managed and increased transparency in algorithmic decision making is required. It is therefore required to find new ways of managing this unprecedented complexity in software systems throughout shortened lifecycle: from requirements analysis and design, to development and testing and up to deployment and operations across highly heterogeneous and dynamically self-reconfiguring systems. • **SU-DS02-2020: Intelligent security and privacy management** Specific Challenge: In order to minimise security risks, ICT systems need to integrate state-of-the-art approaches for security and privacy management in a holistic and dynamic way. Organisations must constantly forecast, monitor and update the security of their ICT systems, relying as appropriate on Artificial Intelligence and automation, and reducing the level of human intervention necessary. Security threats to complex ICT infrastructures, which are multi-tier and interconnected, computing architectures, can have multi-faceted and cascading effects. Addressing such threats requires organisations to collaborate and seamlessly share information related to security and privacy management. The increasing prevalence and sophistication of the Internet of Things (IoT) and Artificial Intelligence (AI) broadens the attack surface and the risk of propagation. This calls for tools to automatically monitor and mitigate security risks, including those related to data and algorithms. Moreover, storage and processing of data in different interconnected places may increase the dependency on trusted third parties to coordinate transactions. Advanced security and privacy management approaches include designing, developing and testing: (i)security/privacy management systems based on AI, including highly-automated analysis tools, and deceptive technology and counter-evasion techniques without necessary human involvement; (ii) AI-based static, dynamic and behaviour-based attack detection, information-hiding, deceptive and self-healing techniques; (iii) immersive and highly realistic, pattern-driven modelling and simulation tools, supporting computer-aided security design and evaluation, cybersecurity/privacy training and testing; and (iv) real-time, dynamic, accountable and secure trust, identity and access management in order to ensure secure and privacy-enabling interoperability of devices and system • **SU-ICT-02-2020: Building blocks for resilience in evolving ICT systems** Specific Challenge: Algorithms, software and hardware systems must be designed having security, privacy, data protection, fault tolerance and accountability127in mind from their design phase in a measurable manner, taking into account future-proof, advanced cryptographic means. Relevant challenges include: (a) to develop mechanisms that measure the performance of ICT systems with regards to cybersecurity and privacy and (b) to enhance control and trust of the consumer of

	digital products and services with innovative tools aiming to ensure the accountability of the security and privacy levels in the algorithms, in the software, and ultimately in the ICT systems, products and services across the supply chain.
HLU	• **ICT-46-2020: Robotics in Application Areas and Coordination & Support** Specific Challenge: While robots originated in large-scale mass manufacturing, they are now spreading to more and more application areas. In these new settings, robots are often faced with new technical and non-technical challenges. The purpose of this topic is to address such issues in a modular and open way, and reduce the barriers that prevent a more widespread adoption of robots. Four Priority Areas (PAs) are targeted: healthcare, inspection and maintenance of infrastructure, agri-food, and agile production. In each of these PAs it is critical to develop appropriate autonomous capability that has impact on the efficiency of key applications in the PAs and moves beyond the current state of the art. This capability is built from core technologies and is proved and tested through pilot demonstrators that embed within real or near real environments. User needs, safety, ethical, gender, legal, societal and economic aspects should be addressed in order to raise awareness and take-up by citizens and businesses. Privacy and cybersecurity issues, including security by design and data integrity should also be addressed, where appropriate. • **ICT-47-2020: Research and Innovation boosting promising robotics applications** Specific Challenge: Robotics enables a significant part of the economic impact of AI by delivering physical intelligence. Logistics, Healthcare, Agri-Food, Inspection and Maintenance, Mobility, Construction, Decommissioning; all require physical intelligence, for example in object manipulation. Physical intelligence is derived from combinations of underlying functional capabilities and developing these capabilities beyond the state of the art depends on fundamental R&D&I which crosses between technical domains, for example into materials research or human interaction. It is therefore important to enhance the capability of robots by exploring and developing the opportunities offered by novel technical developments related to physical intelligence