Journal of Physics: Conference Series

PAPER • OPEN ACCESS

Use of augmented reality-enabled prototyping of cyber-physical systems for improving cyber-security education

To cite this article: Yu Skorenkyy *et al* 2021 *J. Phys.: Conf. Ser.* **1840** 012026

Use of augmented reality-enabled prototyping of cyber-physical systems for improving cyber-security education

Yu Skorenkyy, R Kozak, N Zagorodna, O Kramar and I Baran

Ternopil Ivan Puluj National Technical University, 56 Ruska Str., Ternopil, 46001, Ukraine

E-mail: skorenkyy@tntu.edu.te.ua

Abstract. The use of augmented reality-enabled scenarios in cybersecurity teaching is proposed in the article to respond to new requirements for the rapid adoption of new technologies and profound knowledge of cybersecurity issues by professionals. Implementation of project-type activities based on real cybersecurity issues in application fields of cyber-physical systems is suggested to improve the competence forming. A use-case of agricultural cyber-physical system of systems is discussed as a viable example of augmented reality-enabled prototyping of cybersecurity risk-aware architecture. The necessary steps are analysis of general and business-specific tasks on cybersecurity, creation of a list of competencies, formalized in educational standards and curricula, development of gaming scenarios for the formation of hard and soft skills, development of the scenario management system for AR interfaces. The system using AR tools can be easily adapted to different cybersecurity training activities. Industrial cyber-physical systems may be vulnerable due to insecure wireless connectivity, lack of encryption, inadequate access policy. The project-based learning complex is focused on the implementation of a data acquisition, storage and processing platform for new sensor networks and instruments. Representing all the diverse information on different layers will be greatly improved by use of the developed holographic projection AR tools.

1. Introduction

In industry and academia, multi-faceted use of cyber-physical Systems (CPS) which combine cybernetic and physical components in 3C (computation, communication and control) triad, includes sensing and monitoring environmental factors, tracking resources and tools, security management and more [18]. Offering easy physical access to data which in many cases are stored locally, CPS platforms are also prone to insecure wireless connectivity, lack of encryption, inadequate patching and slow reaction to exposed vulnerabilities as many CPS run their own operating systems and applications [12], [20]. The most topical issue is the privacy and cyber-safety problems for health-services-related CPSs which may be used not only as part of secured proprietary solutions but can also be connected to e-health sensor shields for Arduino or Raspberry Pi platforms by start-up developers, underestimating the information safety risks. Nowadays, the need of incorporating security aspects as essential functional requirements (see figure 1) into device development cycles is commonly acknowledged [2]. At the same time, training of the competent cybersecurity specialist is a costly and time-consuming endeavour. Many organisations have a shortage of skilled cybersecurity staff and the problem may further aggravate in future.

Cybersecurity issues affect every business, every organisation and every citizen. So far, educational systems do not match market demand for cybersecurity specialists and requirements to their competences with traditionally taught university graduates. A way to resolve such inconsistency is the technology-enhanced learning, especially the one with immersive augmented reality (AR) toolkit implemented [3], [8]. Cybersecurity education will essentially benefit from this, in particular, by improving motivation and computer-human interaction efficiency during the competence-building process. In the present paper we propose implementation of a holographic 3D projection as a layer in the AR tool for technology-enhanced training of cybersecurity students.

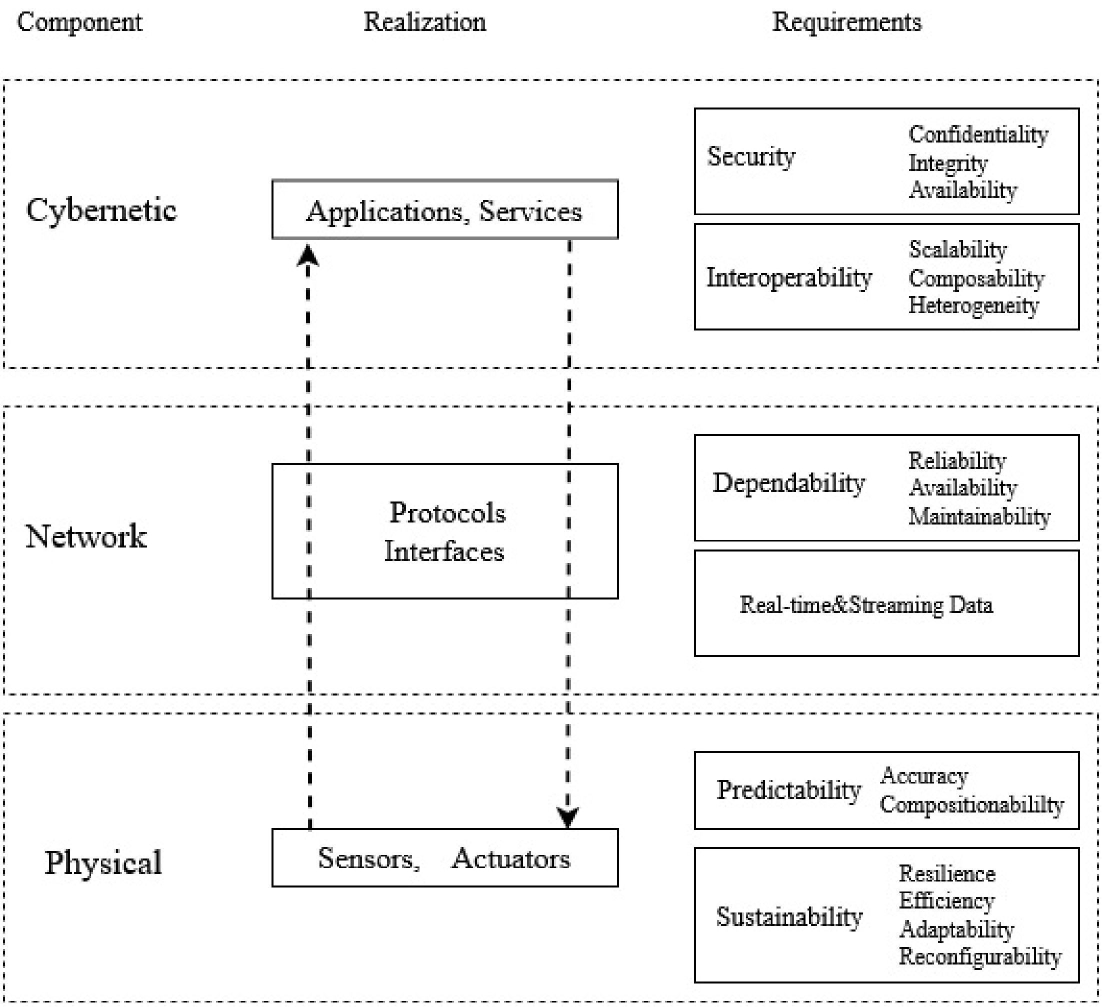

Figure 1. Functional requirements to cyber-physical System realisations.

2. Methodology improvements in cybersecurity training

Currently, technical training is the major trend in cybersecurity education. Oftentimes, university study programs do not include development cycle requirements, professional standards and regulations. At the same time, flexibility is needed for modern cybersecurity specialist and the technical skills are relatively easy to master using available IT tools. While considering specific cybersecurity subjects in which the intensive interaction of instructors and students is required, urgency of the problem increases. In modern day industries, business processes impose new requirements for the rapid adoption of new technologies by a professional with knowledge of cybersecurity issues and procedures. Educational methodologies are to provide cross-disciplinary technology competencies and project experience.

The difficulties of cybersecurity education have been resolved by the NICE Framework of Building Blocks for a Capable and Ready Cybersecurity Workforce [16] shown in figure 2. The use of game forming the set of required competences, skills and abilities may be the appropriate method of implementing this framework into study program. Use of augmented reality interfaces, as well as special scenarios with the content intended to reflect the context [7], [19], environment and roles are needed for the representation of particular professional activities. The necessary steps are analysis of general and business-specific tasks on cybersecurity, creation of a list of competencies, development of gaming scenarios for the formation of hard and soft skills, development of the scenario management system for AR interfaces. The proposed game scenario model, shown in figure 3, is to be implemented into software system architecture.

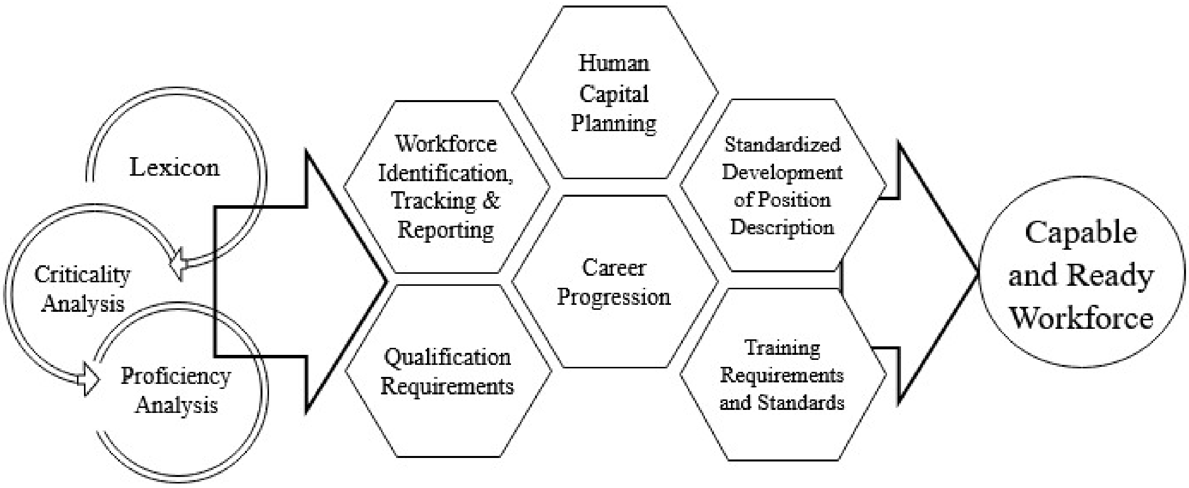

Figure 2. NICE Framework of Building Blocks for a Capable and Ready Cybersecurity Workforce.

For development of a particular set of competences needed to protect a large-scale cyber-physical system from a complex and well-organised cyber-attack, a game scenario can be elaborated along the scenario model shown in figure 3. This will allow modelling the strategic nature of intelligent attackers, design techniques for prediction of attacks and devising countermeasures [6], [15]. The concept of the scenario model has been elaborated by authors to assure essential competencies forming in the process of professional trainings of cybersecurity students as well as major parts of the serious game scenarios. The latter are based on the specific objectives and modules of the study program and define interactions of student, instructor and the context-aware system which is to be responsible for handling various data collected by sensors and obtained through user-machine interfaces. The same context-aware system functional is being developed to assure interaction with knowledge base, maintenance and updates of the interactions history and user-specific dataset for effective training activities control. All actors involved into activity, for example, a cybersecurity incident simulation, are subjects to tracking and multivariate analysis based on the data accumulated by various sensors, human-computer interaction history and the knowledge base of the learning management system.

3. Concept of AR use for learning tools enhancement

There are studies about implementation of augmented reality tools in education (see [3], [8] and references therein), in particular, natural sciences [13] and vocational training [9]. However, AR has not been used in cybersecurity education until now. AR use for data visualisation in cybersecurity creates an immersive interface, which facilitates comprehension of a process – the effect not achievable by 2D visualisation tools. Elaboration of new (advanced and accelerated) teaching and training programs with implemented AR tools has a potential to solve the problem of insufficient supply of skilled cybersecurity professionals.

VR and AR data visualisations are currently used in industry, to enable intuitive and efficient human-machine interactions [10], [17] as well as for workforce training [5]. In real time, AR superimposes images of real objects with virtual images or computer-generated text. The system using AR tools can be easily adapted to different categories of cybersecurity training elements that would make adaptation of new employees easier and help them to catch new terminology faster. For example, for a network or computer system the relevant analytics can be presented visually so the cybersecurity professional may assess in real-time what the data are communicating and whether any risks are present.

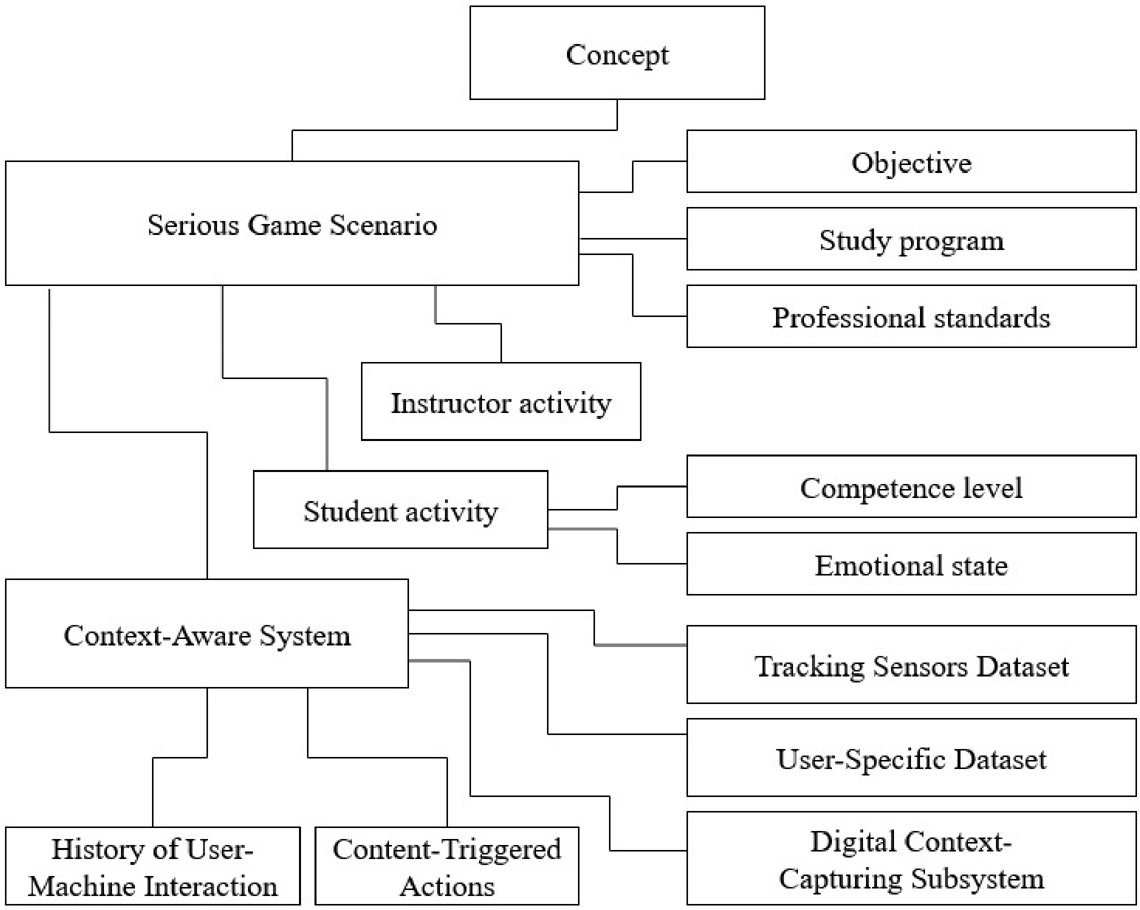

Figure 3. Serious game scenario model for cybersecurity training project.

Up to now, various AR user interface types have been developed, including traditional screens or monitors, windows and windshields, head-mounted displays including helmets and facemasks, glasses, etc. The largest share belongs to handheld AR displays of smartphones due to their unmatched portability, improved cameras, high quality displays, increased computing power. Eyeglasses with AR technology (Google Glass, Vizix, Optinvent, Meta-Space, Reckon Jet) have also received much attention but are now in decline due to privacy issues. Every of the mentioned AR technologies creates a 2D image, which is very similar, but not true representation of real world. Visual perception may misinform the user, observing the 2D picture, about real environment, as it happens with anamorphic optical illusions. A projection holography (more precisely, a false hologram technique) implementation as a layer into an augmented reality pattern is desirable for instructional design in cybersecurity training.

AR can also enhance a development of new intuitive methods to design complex systems and networks based on human-computer kinetic interaction. The holographic 3D environments to be built and tested are to enhance human abilities in different engineering fields as well as in creative endeavours. Not only spatial and temporal dimensions are to be visualised by the designed holograms but also other measurable properties, extending natural human senses and improving decision-making procedures. Among possible augmented reality interfaces, those using 3D false holograms for mixing virtual and real objects have not received sufficient attention. As a realisation of such holographic AR interfaces, half-silvered mirrors can be used as see-through displays in which users can see reflections of themselves and surrounding objects mixed with rear-projected virtual content. The most widely used methods make use of Microsoft Kinect system to determine user position and align virtual objects to reflections of the real ones. Capturing position, movement and collective behaviour of users require intensive exchange of data between sensors and servers, with data pre-processing, sorting and anonymization. In our Cyber-Physical Systems Laboratory, a 45˚ polymer pyramid screen and a video projector (high-definition display) are used to create 3D holograms. Currently, only pre-recorded videos and animations are transformed into 3D false holograms. The setup can be used for full-fledged cybersecurity training or prototyping [11], [14]. Improvement of the current setup configuration can be achieved by adjustment of light transmittance with additional partially transparent films [1], [4].

4. Agricultural CPSoS use case for AR-enabled CPS prototyping

In modern times climate changes as well as soil pollution, erosion and devastation make conditions for organic food production by agricultural means quite severe. To improve agricultural products quality, input efficiency, environmental sustainability and farmer income, the information technology solutions are being adopted in agriculture. Besides enacting machinery and irrigation systems, sensors can provide essential information for decision-making for social networks of farmers, agronomists, managers and customers. Availability of and advancements in Internet of Things sensors and communication devices allows acquisition of complete and informative data and their real-time analysis for fast and effective implementation of localised actions. Real time processing of data acquired by software-defined dynamic networks of sensors will allow faster and more efficient management of agricultural businesses, energy saving and quality improvements for a range of stakeholders. Within this study an approach has been developed for the provision of real-time digital services to smallholder farmers, agricultural and food-processing businesses and customers. This use-case, based on real datasets obtained from one of agricultural holdings as well as surveillance data from satellite images taken by Sentinel-2 and Landsat 8, available through the Application Programming Interface, and raw multi-spectral images provided by the Parrot Sequoia+ camera of SKIF unmanned aerial vehicles, can serve as a testing ground for prototyping cyber-physical systems within cybersecurity risks-aware design flow.

The project-based learning complex is focused on the implementation of a data acquisition, storage and processing platform for new sensor networks and instruments, able to remotely detect crop and soil properties in real time and facilitate or make informed decisions quickly and autonomously. It is to enhance the ability of an agronomist and a farmer to correctly evaluate the current state of a crop, make informed decisions and authorise appropriate and timely actions. Agricultural vehicles-based and stationary sensors allow one to remotely obtain information about current and past weather conditions, accumulated temperature and precipitation, soil temperature and moisture, visualise vegetation cover and calculate the most common indicators for assessing vegetation progress over time. Unmanned Aerial Vehicles (UAV) which allow both high spatial resolution and on-demand timing of aerial passes and quadcopters used as an auxiliary instrument for smaller and fragmented areas to be monitored directly from ultra-low altitudes, may be misused if the controls confidentiality is compromised, therefore represent the security-critical component in the agricultural cyber-physical system of systems (CPSoS). For example, unauthorised access to the UAV flight control must be immediately blocked and potentially damaging instructions must be identified and corrected or ignored. The framework prototype is to be designed to allow building dynamic networks of wireless sensors and actuators for agricultural purposes, segmenting data for local processing or transmitting to data warehouses or data lakes for storage and further processing. For a digital farming platform with a distributed system of personal workstations, sensors at different levels, highly specialised controls, moving units, warehouses, applications enabling business decisions by managers etc, the cloud solutions meet the needs for the heterogeneous distributed architecture. Representing all the diverse information on different layers will be greatly improved by use of the developed holographic projection AR tools. For example, for the specific task of coordination in a drone swarm, every single drone communicates not only the data collected from the crop but also its individual position and velocity. The latter are not informative for a human operator but are crucial for the CPSoS to guarantee fulfilment of both interoperability and predictability requirements (see figure 1). Representing all the diverse information on different layers as a superimposed content can be greatly improved by use of the developed holographic projection AR tools.

Testing of the developed models of CPS components and contents will be performed to check and set-up both functional and non-functional (e.g., efficiency, reliability, security, etc.) technical requirements (figure 4), identify usability problems. Realisation of such a training method, in our opinion, will increase student’s motivation and allow him or her to develop the needed competences, experience and soft skills. The choice of an agricultural CPSoS use case as the first example of a project-type activity for cybersecurity training is caused by the abundance of data needed for creation of realistic serious game scenario and the growing importance of cyber-physical systems in agriculture. In principle, for every use case with sufficient amount of data collected for model elaboration and tuning the corresponding serious game scenarios and requirement analyses can be designed.

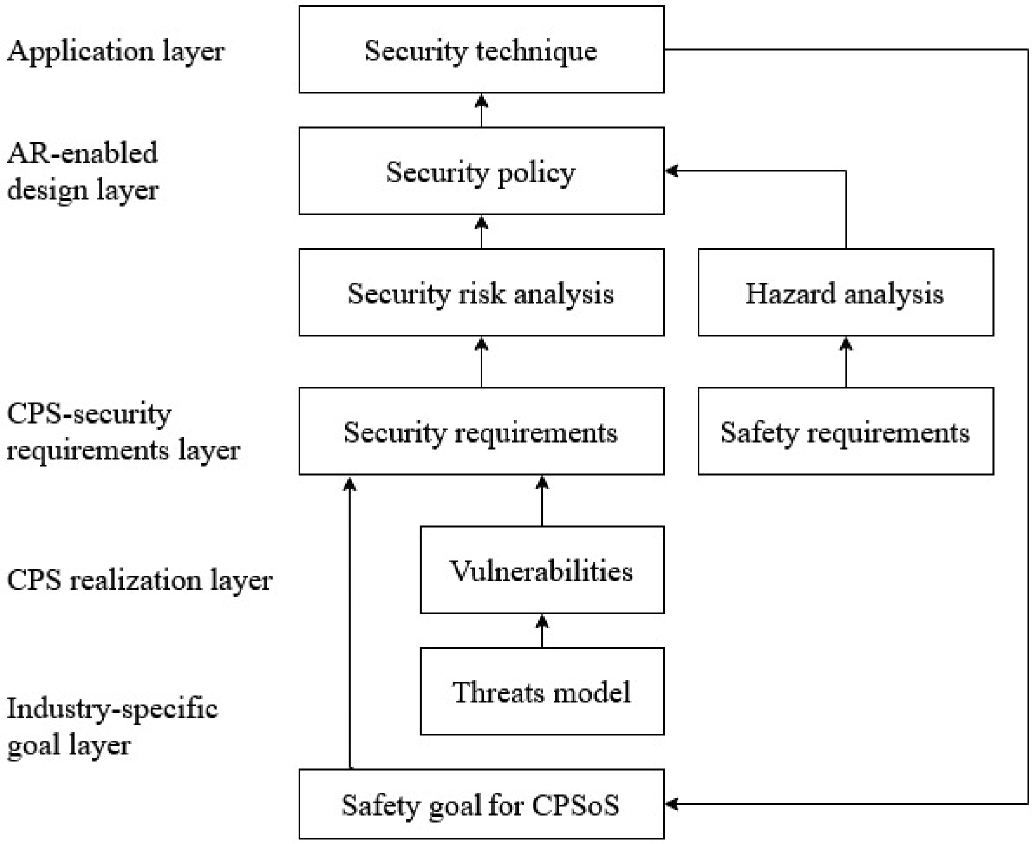

Figure 4. Requirement analysis schema for design of agricultural CPSoS cybersecurity.

5. Conclusions

Nowadays, business processes and industrial developments impose new requirements for professional training and higher education. Demand of cybersecurity specialists is constantly growing but their training is expensive and time-consuming, which tendency is likely to grow with increasing complexity of cybernetic systems. In particular, widely used CPS platforms may be vulnerable due to insecure wireless connectivity, lack of encryption, inadequate access policy, etc.

Despite the urgency of cyber-attack prevention, personal data protection, e-finance fraudulence, there are still no immersive visualisation systems for development of competencies in information security.

The suggested concept of mapping of AR-assisted serious game scenarios onto competency framework and new 3D user interfaces (physical devices) can improve the situation. The necessary steps for the serious game design are analysis of general and business-specific tasks on cybersecurity in connection of specific competencies, formalized in educational standards and curricula and development, on this basis, of the scenario management system for AR interfaces. AR tools can be easily adapted to different project-type activities in cybersecurity training. Within this study an approach has been developed for serious game scenario design and cybersecurity requirements analysis for modern agricultural businesses with intense use of information technology with inherent cybersecurity risks. The project-based learning complex is focused on the implementation of a data acquisition, storage and processing platform for new sensor networks and instruments. Representing all the diverse information on different layers will be greatly improved by use of the developed holographic projection AR tools.

Creating a framework for implementation of AR tools into educational curricula and training scenarios can provide faster and more effective training methodologies of new and certification training of acting IT professionals in the field of cybersecurity. Moreover, an approach based on AR tools eliminates barriers between professionals of different qualifications and makes the coordination within a team easier. Instruments for enriching experiences and mutual knowledge exchange during the (real or simulated) incident prevention or vulnerability detection are very promising for cybersecurity education and professional training.

The proposed approach can also foster the tech-enabled teaching in general by facilitating development of AR educational resources (including distance learning, computer-aided design, customer assistance) which will provide a leverage for many innovative industries, in particular due to increased resilience towards the cybersecurity risks, enabling effective and secure remote work toolkit development for creative industries.

References

[1] Akşit K, Lopes W, Kim K, Shirley P and Luebke D 2017 Near-eye varifocal augmented reality display using see-through screens *ACM Transactions on Graphics* **36** 189 URL https://doi.org/10.1145/3130800.3130892

[2] Arias O, Wurm J, Hoang K and Jin Y 2015 Privacy and Security in Internet of Things and Wearable Devices *IEEE Transactions on Multi-Scale Computing Systems* **1** 99–109 URL https://doi.org/10.1109/TMSCS.2015.2498605

[3] Bacca J, Baldiris S, Fabregat R, Graf S and Kinshuk 2014 Augmented Reality Trends in Education: A Systematic Review of Research and Applications *Educational Technology & Society* **17** 133–49 URL https://www.jstor.org/stable/jeductechsoci.17.4.133

[4] Bimber O and Raskar R *2007 Spatial Augmented Reality: Merging Real and Virtual Worlds* (New York: A.K. Peters/CRC Press) URL https://doi.org/10.1201/b10624

[5] Damiani L, Demartini M, Guizzi G, Revetria R and Tonelli F 2018 . Augmented and virtual reality applications in industrial systems: A qualitative review towards the industry 4.0 era *IFAC-PapersOnLine* **51** 624–30 URL https://doi.org/10.1016/j.ifacol.2018.08.388

[6] Hamman T, Hopkinson K M and McCarty L A 2017 *Applying Behavioral Game Theory to Cyber-Physical Systems Protection Planning* (Intelligent Data-Centric Systems, Cyber-Physical Systems) ed Song H, Rawat D B, Jeschke S, Brecher C (Cambridge: Academic Press) chapter 17 pp 251–64

[7] Karpiński M, Korchenko A, Vikulov P, Kochan R, Balyk A and Kozak R 2017 The etalon models of linguistic variables for sniffing-attack detection *9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)* pp 258–64 URL https://doi.org/10.1109/IDAACS.2017.8095087

[8] Kiv A E, Shyshkina M P, Semerikov S O, Striuk A M and Yechkalo Yu V 2020 AREdu 2019 – How augmented reality transforms to augmented learning *CEUR Workshop Proceedings* **2547** 1–12

[9] Lavrentieva O O, Arkhypov I O, Kuchma O I and Uchitel A D 2020 Use of simulators together with virtual and augmented reality in the system of welders' vocational training: past, present, and future *CEUR Workshop Proceedings* **2547** 201–16
[10] Liu C, Cao S, Tse W and Xu X 2017 Augmented Reality-assisted Intelligent Window for Cyber-Physical Machine Tools *Journal of Manufacturing Systems* **44** 280–86 URL https://doi.org/10.1016/j.jmsy.2017.04.008
[11] Lukman Khalid C M, Fathi M S, Mohamed Z 2014 Integration of cyber-physical systems technology with augmented reality in the pre-construction stage *Proceedings of 2014 2nd International Conference on Technology, Informatics, Management, Engineering & Environment (TIME-E 2014)* pp 151–56 URL https://doi.org/10.1109/TIME-E.2014.7011609
[12] Lyu X, Ding and Yang SH 2019 Safety and security risk assessment in cyber-physical systems *IET Cyber-Physical Systems: Theory & Applications* **4** 221–32 URL https://doi.org/10.1049/iet-cps.2018.5068
[13] Nechypurenko P P, Stoliarenko V G, Starova T V, Selivanova T V, Markova O M, Modlo Ye O and Shmeltser E O 2020 Development and implementation of educational resources in chemistry with elements of augmented reality *CEUR Workshop Proceedings* **2547** 156–67
[14] Omidshafiei S, Agha-Mohammadi A, Chen Y F, Ure N K, Liu S, Lopez B T, Surati R, How J P and Vian J 2016 Measurable Augmented Reality for Prototyping Cyberphysical Systems: A Robotics Platform to Aid the Hardware Prototyping and Performance Testing of Algorithms *IEEE Control Systems Magazine* **36** 65–87 URL https://doi.org/10.1109/MCS.2016.2602090
[15] Orsini G, Bade D and Lamersdorf W 2015 Context-Aware Computation Offloading for Mobile Cloud Computing: Requirements Analysis, Survey and Design Guideline *Procedia Computer Science* **56** 10–17 URL https://doi.org/10.1016/j.procs.2015.07.169
[16] Petersen R, Santos D, Smith M C, Wetzel K A and Witte G 2020 Workforce Framework for Cybersecurity (NICE Framework) *NIST Special Publication 800-181 Revision 1* (Gaithersburg: National Institute of Standards and Technology) URL https://doi.org/10.6028/NIST.SP.800-181r1
[17] Qiu C, Zhou S, Liu Z, Gao Q and Tan J 2019 Digital assembly technology based on augmented realityand digital twins: a review *Virtual Reality & Intelligent Hardware* 2019 **1** 597–610 URL https://doi.org/10.1016/j.vrih.2019.10.002
[18] Song H, Rawat D, Jeschke S and Brecher C 2017 *Cyber-Physical Systems: Foundations, Principles and Applications* (Cambridge: Academic Press)
[19] Soylu A, De Causmaecker P and Desmet P 2009 Context and adaptivity in pervasive computing environments: Links with software engineering and ontological engineering *Journal of Software* **4** 992–1013
[20] VPMmentor 2018 Privacy and Security Assessment of Smart Wearable Gadgets *Report* URL https://www.vpnmentor.com/wp-content/uploads/2018/07/CI4S-Final-report_VD6-21-2018-.pdf