BUILDING SAFEGUARDS TECHNOLOGIES USING OPEN SOURCE SOFTWARE AND HARDWARE - LEARNING FROM THE MAKER MOVEMENT

M. KÜTT
Princeton University
Princeton, NJ, USA
Email: kuett@princeton.edu

Abstract

Safeguards technologies are typically developed by the Agency and national support programs. More and more, they rely on extensive software and information technology usage. Especially in these fields, recent years showed the advance of new approaches to foster innovation. There is increased use and development of open source software, where not only a software package is shared freely, but also the underlying source code. It is now a widespread way of developing and distributing new software. Similar to the software engineering process, hardware designs can be shared under open hardware standards. This, together with the maker movement, created very efficient innovation environments for people to develop new tools and projects.

In this paper, it will be analyzed how lessons learned from these areas could be applied to the development of new safeguards technologies. Open source approaches could potentially increase the number of participants helping developing tools. At the same time, they would allow to put verification and monitoring tools under external scrutiny, thus increasing trust and transparency. Lastly, they could increase the actual user community by lowering costs and access barriers to tools, helping capacity building as well as the daily operation. The paper will introduce the open source approaches and the maker community and discuss how safeguards technologies would benefit from integrating those ideas. As an actual example, a prototype gamma spectrometry information barrier, which was built using open source software and open hardware, will be introduced. In the end, the paper will lay out ways to implement the discussed approaches.

1. INTRODUCTION

Technology is a key component of IAEA safeguards activities; inspectors use equipment to acquire data during inspections and install it to remotely monitor facilities. Developing new technology and improving the existing technology are constant challenges. While the number of facilities and material under safeguards is rising, IAEA Department of Safeguards budget has remained relatively constant in recent years. To meet these challenge, the department modernizes its infrastructure and streamlines internal processes. Existing equipment is improved incrementally, and new emerging technologies are monitored for the possible use as safeguards tools. The different Member States Support Programmes play a central role for research and development of safeguards equipment [1, 2].

Clearly, the IAEA has requirements for its safeguards equipment which should not (and must not) be neglected or contradicted. Equipment needs exact calibration, careful tests and ruggedization for use in rough environments. It has to undergo special approval; IAEA member states need to accept tools to be used and the operators of inspected facilities need to certify equipment prior to use. Also, the equipment must be secured against external influences. Cheating possibilities by an inspected party must be avoided at all cost. At the same time, the inspected party has a high interest that the equipment does not have malfunctions, intentional or unintentional, that would lead to a wrong outcome of the inspection.

In this article, I make the case for the IAEA and the safeguards technology community to engage with ideas from the so-called maker movement, including open source approaches both for hardware and software development. Such an engagement could generate new impulses for research and development and give access to a broader community of experts. While this might sound radical, it is not. Hosting a Robotics Challenge in 2017 and a current challenge to improve Passive Gamma Emission Tomography are examples where the Department of Safeguards already employed maker movement ideas to improve safeguards technology [3].

There are good reasons for the success of the open source and maker movements in other fields, and the particular needs of the Agency overlap with some of their genuine strengths. Safeguards inspection often require the use of non-routine tools. Open source and maker movement commonly develop non-routine tool, driven by a norm of sharing, sharing tools, products and knowledge during and after the creative process. This led to a

product customization previously impossible to achieve, creation of new global communities, and innovations that became technological backbones of modern life. Today, companies are relying and producing open source software, for example social media companies like Twitter and Facebook. The research centre CERN has created a large repository for research hardware developed using open standards. And start-ups and established companies tap into the resource pool the maker movement offers, either through collaborations or by opening in-house makerspaces.

2. OPEN SOURCE SOFTWARE, OPEN HARDWARE AND THE MAKER MOVEMENT

To better understand how advantages for safeguards technology development can be derived from open source approaches for software and hardware, key characteristics will be outlined in this section. Both approaches were crucial elements for the start of what many call the maker movement, maker community or even maker revolution.

2.1. Open source software

Starting from a small niche, today open source software is used for key functions of the internet, including web servers, transfer and encryption protocols and web application frameworks. The open source movement did not only change software distribution, but also created a new way of software development. Software that is classified as open source software if it fulfils at least the three following conditions: The source code of the software – the human readable "recipe" of a program – is shared together with the executable files. Second, the software can be shared and reshared free of charge. Third, users and other developers can use the provided source code to make changes to the software and are allowed to publish them - either as new work, or by sending it back to original authors to be integrated in the original version of the software [4, 5].

The right to make changes to a software package does not imply that everyone can change the software at any time. In contrast, most successful open source projects have a clear decision-making structure to manage the development. New changes can be proposed, but only a limited group of people, sometimes only a single person, would accept these changes, after often rigid quality controls. The leading actor can also direct the future development by setting mile stones for upcoming releases. In case of disagreement of a large group of developers with the leadership, projects can split ("fork"). While this rarely happens, it is an important factor to empower code developers.

The open source characteristic is not only a constant status, but also has procedural aspects, addressing a very common problem of software development. Because of the complexity of programs and the inherent need to keep an overall design structure, the software development process cannot simply be accelerated by just adding more developers. Researchers showed that there are two possibilities for production models of software, the open source model and the proprietary model [6]. Open source software development is driven by two main forces. On one hand, there are companies who pay programmers to create open source software, or publish existing, previously proprietary software under open source licenses. On the other hand, there are also large numbers of volunteers, who develop open source software in their free time. Typical motivations for volunteers include personal needs for a particular tool, intrinsic motivation, possibility of becoming a member in a community and future economic rewards – e.g. improved job opportunities due to publicly posted work.

Examples for open source software are manifold. As part of the internet infrastructure, *Apache* and *Nginx* are widely used web server software packages. They are often run on servers powered by operating systems using the *Linux kernel*. The Linux kernel has been developed since the early 90ies, an early example of open source software. Today, it is used not only for servers and desktop computers, but for cell phones (as part of *Android*), many connected small devices forming the “Internet of Things”, and entertainment technologies (e.g. aircraft entertainment systems). Programming languages and compilers, the basis for new software development, are typically also developed as open source software projects. Probably most important for commercial use are so-called web-application frameworks like *AngularJS*, *Node.js*, *Ruby on Rails* or *React*. This are tools that allow websites to be interactive and to quickly add new functionality and are often integrated in commercial products. Most big social media companies use open source frameworks and contribute to their development. Especially start-ups benefit from the availability of such tools because it allows them to quickly deploy new ideas at low cost.

2.2. Open source hardware

Open source hardware, short open hardware, is derived from the successful practice of open source software. It has not yet reached similar widespread use, but applications are growing. Clearly, copying hardware – material objects – requires effort and resources, different from copying software, hence open source hardware does not require free distribution of the hardware itself. According to the "Open Source Hardware Definition", hardware can be called open source hardware when it is released with comprehensive documentation and necessary software. Derived works and free redistribution need to be permitted, too [7]. Documentation is comprehensive, it includes design information and information necessary to build the hardware, for example technical drawings, 3D model files, circuit schematics, component lists or assembly instructions. Similar to open source software, organized groups foster open hardware development. Founded in 2011, the Open Source Hardware Association (OSWHA) sets standards and organizes annual summits. Special online platforms allow people to share and discuss their projects (e.g. hackaday.com, hackster.io, thingiverse.com).

An early adopter of open source hardware standards in academia was the CERN research centre. It published a special open hardware license (CERN OHL) and provides and online repository for hardware designs, specifically for experimental physics facilities [8]. Joshua Pearce, founder of the Michigan Tech Open Sustainability Lab advocates more general for increased use of open hardware in laboratories [9]. In March 2017, the IEEE Robotics and Automation Magazine dedicated a full journal issue to the success of open hardware in the field of robotics, highlighting several innovations that were rendered possible due to widespread use of open hardware standards.

There are a number of companies who sell open hardware products. Although all of the design information is public, they are typically able to make a profit, providing high quality manufacturing. For their products, companies encourage users to suggest improvements, and integrate them into the production process quickly. The Italian company *Arduino* has been founded in 2003 to design and produce small micro controller boards at affordable prices. All board designs are publicly available, and have been reproduced by various manufacturers, still the original company remains profitable. With a similar concept, the 3D printer company *Lulzbot* created a 3D printer based on the RepRap Open Hardware 3D printer design. The company sells 3D printers, which could also be copied. Other companies operating with similar strategies include *Sparkfun* and *Adafruit*, both providers of electronic components installed on easily accessible breakout boards.

2.3. What are they making? Makers and makerspaces

In 1998, Neil Gershenfeld, the director of the MIT Center for Bits and Atoms, started teaching a class "How to Make (almost) Anything", which was a great success. The class allowed students to develop projects using manufacturing tools they normally had no access to. Surprisingly to the organizers, the motivation was often not research, but personal ideas. A few years after the first class, Gershenfeld started to create "fab labs", places for personal fabrication. First labs were opened as part of an MIT outreach project, and were among the first makerspaces [10].

Cost reductions for key manufacturing tools and the invention of new ones, e.g. 3D printing, made radically different ways of product development possible. Innovation by individuals has been made easier, often outside of classical research and development departments. Makerspaces provide tools and are important locations for sharing ideas, designs and knowledge among other community members. Makerspaces in libraries and academic institutions are also created to educate people, using a hands-on approach. By opening in-house makerspaces for employees as well as for outsiders, companies apply the approach, too. Starting from a small hobbyist scene, the maker movement has established itself as a credible platform for creation and manufacturing of new ideas. As the production methods are very suitable for customized, low volume production, "the new manufacturing mode enables [...] a mass market for niche products" [11].

Three key components can be said to make up the maker movement: The *maker*, an, often self-chosen, identity of the people behind the movement. Anyone can be a maker. *Making* is the activity or set of activities necessary for the creative production of artefacts. Often, such production involves programming, engineering skills and the use of electronics but it is not limited to that. Knitting and stitching are often-cited non-electronic examples. *Makerspaces* are the physical locations where the activity is carried out and new activities can be

learned. The term is also describing the community related to the physical space, which values other maker's ideas and allows for the exchange of knowledge [12].

But the maker movement goes beyond spaces and makers. Important for the development from the early beginning was the "Make" magazine, founded in 2005 and the continuously expanding series of "Maker Faires", which now reaches several hundred thousand people annually. The faires are large places for makers to meet beyond the makerspace. They are also venues for hobbyists to meet professionals, as many companies participate in these events. A small Maker Faire was hosted in 2014 at the Obama White House, which was part of a larger set of activities of the previous U.S. administration to actively embrace and support the maker movement [13].

Early makerspaces were called hackerspaces, and activities and identities were called hacking and hackers accordingly. If distinguished, hackerspaces are more related to creating software and computer programs than physical artefacts. In this context, the term hacker is positive, and has nothing to do with the common interpretation of hackers as criminals in cyberspace. A hack is the material practice of a hacker, a creative act that brings new solutions or ideas into the relationship between technology and society [14]. Making can be seen as the generalized form of this – creative production of physical artefacts. Common to both is the deeply embedded norm that the result should be shared, should be used to teach others and can be improved by others.

Makerspaces would be nothing without the access to tools. Recent advances in manufacturing technology made it possible that machines previously only available in factory settings are no accessible in desktop versions – similar to the transition from mainframe computers to desktop computers in the information technology world, democratizing manufacturing. The list of tools includes 3D printers, laser cutters, water jet cutters, CNC mills for a variety of materials including metal and wood, common workshop tools, knitting and stitching machines, printers, welding machines and solder irons. Makerspaces not only provide tools but offer handling courses and safety trainings. Besides safety considerations and consumable supplies, there is typically no limitation to the use of machines – no organizational hurdles that could slow down the creative process.

Different organizational forms exist for maker spaces. They can be run by the user community itself, being organized as non-profit organizations. Other makerspaces are run for profit, collecting membership fees from users and charging them for supplies and training sessions. Several "Tech Shops" were successful for a number of years but went out of business recently. Many makerspaces can also be found attached to schools and universities, and there is a large group of public libraries that offer spaces for the local community to explore creative ideas. The directory at hackerspaces.org currently lists more than 1400 active spaces, the list of fab labs at the website of the Fab Foundation has more than 1300 fab labs in over one hundred countries.

In recent years, companies started to create their own makerspaces, both for internal use as well as for use shared with others. Their engagement is often motivated by the attempt to overcome "Joy's" law, which states that "[n]o matter who you are, most of the smartest people work for someone else". The law is commonly attributed to Bill Joy, co-founder of Sun Microsystems [15]. Reaching out to the maker community can help integrating additional minds to a companies' talent pool. For example, software giant Microsoft has a project called "The Garage", resembling early stories of Silicon Valley companies that were founded in garages. Employees of Microsoft can use this space to work on their ideas. SAP, a company for enterprise software, started a series of "Next Gen Innovation Labs" in partnership with universities and other academic institutions, focusing on projects that can help to achieve the 17 UN Global Sustainability Goals. Not only companies open such venues, since a few years also the U.S. space agency NASA has a makerspace "Ames Space Shop" connected to its Ames research center. It is open to NASA employees and the local community [16]. A study by the auditing and consulting company Deloitte in 2013 suggested ways for companies to take advantage of the maker movement in general [17].

Crowd-source development challenges have an overlap with the maker movement, too. Such challenges are events where a larger group of people works on previously defined tasks. Tasks can range from very narrow to broad topics, and the time frame of the events differs, too. For some challenges, participants work on their own for a longer period of time, up to years. For other challenges (often called "hackathons"), people meet and work on projects only for a couple of days or even hours, and present immediate results.

3. PRACTICAL EXAMPLES: BUILDING VERIFICATION TECHNOLOGY

In recent years, I was part of several projects that developed verification technology in Princeton University's Nuclear Futures Laboratory. The laboratory is equipped with a variety of tools typical for maker spaces, or access to those tools is within easy reach. Open source approaches are used by the laboratory both as research resources as well as ways to publish and share developments. Two of recent research projects will be described in the following. Both for teaching students as well as the actual research, incorporating aspects of the maker movement proved to be very insightful and helped with development speed and quality of solutions.

3.1. Information Barrier Experimental

Measurements carried out as part of inspections can generate sensitive information that must not be shared with inspectors. Host countries put such restrictions in place due to national security interests. Similar restrictions can be introduced by civilian facility operators to protect certain design specifics and intellectual property. Information barriers are devices that can record classified or protected information and transform the data into non-restricted outputs, like a combination of red and green lights. An IAEA instrument with an integrated information barrier was the Cascade Header Enrichment Monitor. To avoid revealing proprietary information, it only reported go/no-go statements [18].

Two prototype information barriers for warhead confirmation measurements, called information barrier experimental (IBX) and IBX II were developed Spring 2016 and Fall 2017, respectively. Both were designed as template-matching systems to confirm that multiple items are identical to one another. The systems use a standard low-resolution sodium-iodide scintillation detector and photomultiplier (Canberra/Mirion Technologies Model 802) to perform passive gamma spectrum comparison. Based on two recorded gamma spectra, one for a template and a second one for an inspected item, the devices decide whether both measurements are similar (match) or different (fail). Similar systems could be developed and used for safeguards measurements, for example to safeguard fissile material of weapon origin.

IBX is a functional prototype to be for algorithm testing (cf. Figure 1). It is based on the Red Pitaya single board computer running Linux and using Python scripts for data analysis. The Red Pitaya has two fast analog inputs (125 million samples/s) and a Field Programmable Gate Array to be used for data processing. Additional parts built were a custom enclosure and front panel, and a high voltage board [19].

FIG. 1. Information Barrier Experimental (IBX). Front panel and user interface (left), experimental setup with mock-up warhead (right).

The goal for IBX II very different – proving the possibility to build an information barrier using vintage computing hardware, in this case an Apple IIe with the MOS 6502 8-bit processor. CPUs designed in the distant past, at a time when their use for sensitive measurements was never envisioned, drastically reduce concerns that the other party implemented backdoors or hidden switches on the hardware level. Hardware built for IBX II included a high voltage board and a signal processing board with analog-to-digital conversion, both designed as Apple IIe extension cards. Software was written in 6502 assembler. Tests have shown that the device is a reliable gamma spectrometer and could fulfil the job of an information barrier [20].

The development of IBX/IBX II did not take place in an actual maker space, but utilized similar tools and relied heavily on other open source developments. Although none of the participants of the project were initially experts in hardware design, the hands-on approach and help from others allowed us to achieve working prototypes in less than three months. The Red Pitaya board is a result of a crowd funding campaign in 2013 and is advertised as "open instruments for everyone" [21]. The software that is used to record the incoming pulses (traces) was based on an open source project by two other scientists - Matjaz Vencelj and Peter Ferjančič [22]. A university owned laser cutter and a CNC mill was used to build the custom designed enclosure.

Similarly, for IBX II, aspects related to the maker movement were crucial to the success of this project. The Apple IIe with its eight expansion slots is an excellent prototyping platform. Since its market introduction, users used this "hackability" to develop a large variety of expansion cards. The system is well documented, both in terms of the hardware specifications as well as the operating system software. Parts of the analog signal processing board were inspired by design information published by the UK-Norway initiative. This initiative jointly built and tested an information barrier – though it cannot be considered a full open source hardware device, schematics and part lists are available online [23]. The open source software *linapple-pie*, an Apple IIe emulator, was essential for the assembler software development. Using the emulator, tests could be carried on modern computers, and because the source code to the emulator has been available it was possible to add functions to emulate the actual behaviour of the new extension cards.

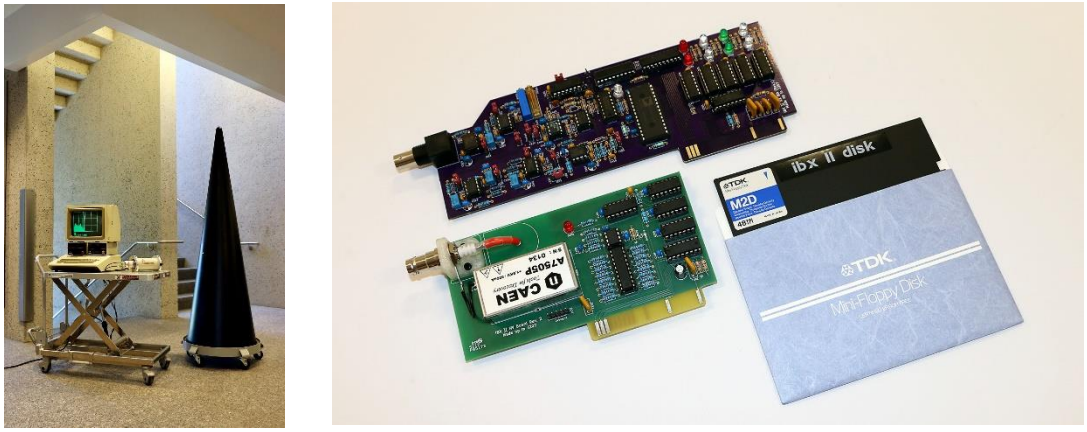

FIG. 2. IBX II - "Vintage Verification." Typical measurement setup with mock-up warhead (left), two Apple IIe extension cards and 5¼" floppy disk with system software (right).

3.2. Robots for Safeguards Applications

Recent work of our group in Princeton also involved the use of robotics, particularly for safeguards applications. Neutron detecting robots could be used to detect clandestine efforts to produce highly-enriched uranium (HEU) during on-site inspections of gas centrifuge enrichment plants. Two scenarios were considered: In the first scenario, some product feed is internally diverted to a small special cascade producing HEU. This would require some pipework to be done, the HEU product could for example be stored in a container hidden in a centrifuge. In the second scenario, the natural uranium feed to a cascade would be replaced with a feed of lowly-enriched uranium, resulting in the cascade producing HEU at the product side. We developed a neutron detector to be mounted on a robot that could detect both scenarios. Results are shown in a different paper presented at this symposium [24].

Currently, only simulations have been performed for the neutron detector. In parallel, a smaller robot has been built using Geiger-Müller counters to detect gamma radiation. This robot is used to develop and test the SLAM (simultaneous localization and mapping) functionality, as well to improve the navigation and search algorithms used to find radioactive sources.

Similar to the information barrier development, the robot was developed in a "maker way". The small robot uses the *Turtlebot 3* robotics kit. Designed as a platform, it provides all necessary components to build robots for a large variety of applications, making it easy to design and 3D print enclosures for the Geiger counters that were attached to the robot. The Geiger counter model and electronics was inspired by the *Safecast* project, a big crowd-sourced data collection project that collects radiation data worldwide and was started in the

aftermath of the Fukushima accident [25]. On the software side, the robot is based on the *Robot Operating System (ROS)*, a large software framework to control robots. It includes packages for motor controls, SLAM, mapping tools, and navigation tools. Expansion to include other sensors is easy, too, allowing a small addition to provide every count recorded by a Geiger counter a data package in ROS. All developments were made available at a maker platform, hackaday.com [26]. The project will continue, the next step being the construction of the neutron detecting robot. We will continue to rely on work by others, but also contribute back to the community.

4. CONCLUSION

This article tries to build a bridge between two very different worlds: On one hand, the development process of IAEA safeguards equipment, equipment that has to be tested, calibrated and approved to be used by inspectors providing evidence of compliance or non-compliance with crucial international agreements. On the other hand, the maker movement – individuals using manufacturing tools for creative production, often for personal use and often in a seemingly unorganized, unstructured and uncontrolled way. Applied with necessary caution, lessons from the maker movement have interesting benefits for the development of IAEA safeguards equipment.

Projects in makerspaces lead to quick results, because prototyping is fast, several iterations of a project can be in a very short time. Although time is mostly not a constrain for IAEA safeguards equipment, certain international events or diplomatic breakthroughs can lead to new safeguarding requirements that need to be met quickly. Relying on existing open source technology and employing a development process that includes maker elements could help here to achieve timely completion of development and testing process.

IAEA inspectors use highly customized niche products, currently produced at high cost. At the same time, this is just the type of product development makerspaces excel at making. Developing customized, individual objects is one of the key motivations for people to join and work in a makerspace. In addition, using open source standards for software and hardware increases transparency and trust. If everyone has the chance to understand the underlying principles of an inspection equipment, e.g. by reading the source code, vulnerabilities could be found easier compared to proprietary tools. Relying on freely shared tools is a way to reduce costs for the Agency and sharing in-house developments can contribute to international capacity building. Joy's law – there is always more talent outside of an organization – applies to the Agency, too. Connecting to the maker community could create access to larger community of knowledge. Due to its open character, the maker movement fosters collaboration, removes barriers and enables knowledge exchange beyond those related to an organization.

Implementation of lessons from the maker movement can take many forms. The most comprehensive embrace of the maker movement would be the opening of an IAEA makerspace dedicated to development of safeguards equipment. This could start with a project inviting makers to the IAEA, or to collaborate closely with existing places in Vienna. On a smaller scale, a measure to raise interest in and gain feedback from other development communities is to publish software as open source software and share hardware designs, if safely possible and not restricted due to proprietary reasons. As a limited, controlled start, design information for a single piece of equipment could be published, accompanied with a public challenge to improve this device, or a public search for existing, currently overlooked, vulnerabilities. This would provide an interesting test case for future information sharing. More passive forms of engagement are possible, too. The process to acquire new tools and technologies are acquired could include exploration of existing open source alternatives as a first step. It would be possible to actively suggest such explorations for future acquisitions and integrate respective provisions in research and development plans for member states support programs.

ACKNOWLEDGEMENTS

The author wishes to express his appreciation to Zia Mian and Sébastien Philippe for reviewing the manuscript and suggesting improvements and corrections.

REFERENCES

[1] IAEA Department of Safeguards, IAEA Safeguards – Serving Nuclear Non-Proliferation, September 2018.
[2] FOURNIER, V. Safeguards Equipment: What's in an Inspector's Luggage? (2016), https://www.iaea.org/newscenter/news/safeguards-equipment-whats-in-an-inspectors-luggage.
[3] IAEA, IAEA Challenge (2018), https://challenge.iaea.org/.
[4] STALLMAN, R.M., LESSIG, L., GAY, J., Free Software, Free Society: Selected Essays of Richard M. Stallman, GNU Press, Boston (2002).
[5] Open Source Initiative, The Open Source Definition (2007), https://opensource.org/osd.
[6] WEBER, S., The Success of Open Source, Havard University Press, Cambridge, MA (2004).
[7] GIBB, A. Building Open Source Hardware – DIY Manufacturing for Hackers and Makers, Addison-Wesley, Upper Saddle River (2015).
[8] European Organization for Nuclear Research (CERN), Open Hardware Repository (2018), https://www.ohwr.org.
[9] PEARCE, J.M., Building research equipment with free, open-source hardware, Science. **337** 6100 (2012) 1303-1304.
[10] GERSHENFELD, N., FAB – The Coming Revolution on your Desktop – From Personal Computers to Personal Fabrication, Basic Books, New York (2005).
[11] ANDERSON, C., Makers: The New Industrial Revolution, Crown Business, New York (2012).
[12] HALVERSON, E.R., SHERIDAN, K.M., The maker movement in education, Harvard Educational Review, **84** 4 (2014) 495-504.
[13] The White House, A Nation of Makers (2014), https://obamawhitehouse.archives.gov/nation-of-makers.
[14] LEVY, S., Hackers – Heroes of the Computer Revolution, Dell Publishing, New York (1985).
[15] LAKHANI, K.R., PANETTA, J.A., The principles of distributed innovation, Innovations: Technology, Governance, Globalization **2** 3 (2007) 970-112.
[16] National Aeronautics and Space Administration (NASA), About Us – Ames Space Shop (2015), https://www.nasa.gov/centers/ames/spaceshop/about.
[17] HAGEL, J., BROWN, J.S., KULASOORIYA, D., A movement in the making, Deloitte University Press (2013).
[18] CLOSE, D.A., MACARTHUR, D.W., NICHOLAS, N.J., Information Barriers - A Historical Perspective, Los Alamos National Laboratory, LA-UR-01-2180 (2001).
[19] KÜTT, M., GÖTTSCHE, M., GLASER, A., Information barrier experimental: Toward a trusted and open-source computing platform for nuclear warhead verification, Measurement, **114** (2018) 185-190.
[20] KÜTT, M., GLASER, A., Vintage verification: Building an information barrier with the Apple IIe and the MOS 6502, (59th Annual Meeting of the Institute of Nuclear Materials Management, Baltimore, MD, USA, 2018).
[21] Red Pitaya, Open Instruments for Everyone (2013) http://www.kickstarter.com/projects/652945597/red-pitaya-open-instruments-for-everyone.
[22] VENCELI, M. (Jozef Stefan Institute, University of Ljubljana), Personal Communication, 2015 and https://github.com/Grozomah/trigger.
[23] UK Norway Initiative, Trust in Verification Technology—A Case Study: The UK-Norway Information Barrier (2016), http://ukni.info.
[24] GOLDSTON, R.J., GLASER, A., KÜTT, M., LANDGREN, P., LEONARD, N.E., Autonomous Mobile Directionally and Spectrally Sensitive Neutron Detectors (IAEA Safeguards Symposium, Vienna, Austria, 2018).
[25] Safecast Project, Bgeigie Nano (2018), thttps://blog.safecast.org/bgeigie-nano/.
[26] LANDGREN, P., KÜTT, M., GeigerROS – A ROS enabled Geiger counter radiation sensor for easy robotic use (2018) https://hackaday.io/project/158327-geigerros