Aerospace Technology Congress, 8-9 October 2019, Stockholm, Sweden
Swedish Society of Aeronautics and Astronautics (FTF)

Additive Manufacture at Industrial Aeronautical and Defence Area: How to control the production of a good and some questions related copyright intellectual property performance at an embargo scenario

Juan Manuel Iglesias Pascual* and José Valentin Iglesias Pascual**

*E-mail: unifjpascual@fei.edu.br jose.pascual@metodista.br
*R&D, SaveInProcess SBC SP/Brazil **Professor Doctor UMES, SBC SP/Brazil

Abstract

One question raised in this exploratory work with focus on how assure that the Additive Manufacture, AM, let's say 3D printing, produced part fits all the requirements, to fulfil the demands of warranty and performance to assure the proper operation of the system in that this part is included and how to perform the traceability of them. Some other important points in this discussion, regarding the digital files and the parts produced from those files or by files produced from scanned 3D parts, include among others: Copyright and Patent issues, Licensing private or Public (GPL), Creative Commons (CC). Other important topics are about customer adapted production, support licenses i.e. the AM techniques recommend by the supplier of the system to produce a specific part to fulfil the requirements of the system. Traceability of this production and Digital Right Management (DRM) since suppliers are demanded regarding the International Traffic in Arms Regulations (ITAR) and Export Administration Regulations (EAR). Embargo statements frequently are needed for humanitarian and geopolitical reasons and ensure the fulfilling dimension and scope and demands of an embargo sanction are a trick challenge. The AM could be an opportunity or a threat in this issue. The point surrounding the 4.0 industry is how to define and control the permission to copy and some kind traceability of the produced goods e.g. IoT and "IP or DOI mark", but the ontology logical data and right technological and legal model must be defined. However, if those goods, the spare parts or additional ones, will not be controlled, they potentially could be produced by the entity or nation under embargoes sanctions or some undisclosed ally. The other concerns regarding AM solutions are about software to control in some extent the production of some good and with the possibility that the supplier of the product restrict the production at the buyer as an undeclared embargo, one option is private blockchain key shared by the supplier of the technology able to be AM, the customer and a trusted third part.

Keywords:Defence-aerospace Additive Manufacture Intellectual Property ontology

1 Introduction

The history of the Additive Manufacturing, mainly regarding the 3D printing, has more than a century and the solutions been becoming more complex [1]. One of the very first references and patents was done in the end of the XIX century by BLANTHER [2]. The current possibilities for several different applications are enormous with different technologies, niches and materials commercially available, since the first commercial stereolithography in 1980s [3] [4] [5]. The efforts to do this technology closer to students occurs at different levels and sometimes include the participation of the community [6] or develop the improve professional capabilities by online training. [7]

The standard file exchange format is stl, Stereo Lithographic or Standard Tessellation Language [8] and is usually described as a succession of tiny layers [9]. Other files formats used are: 3MF, AMF, SPE-NC, STEP, each one has some specificities. [10].

Additive Manufacture (AM) is changing the production standards and the value chains in an unprecedented way [11] [12] [13]. Its distribution sometimes is geographically dispersed, in some scenarios it could be in clusters and then 4.0 industry pops up some considerations about regional ecosystem influence [14] and also RISE Research Institutes of Sweden [15], there are also discussion about frameworks and threats and opportunities. [16]

2 Acceptance of AM

The field of AM is becoming more professional and the normalization is a good metrics of this. In Brazil one of the

DOI
10.3384/ecp19162024

groups is the ABNT/CCE 261, the author is currently working in this group, with ABIMAQ/FIESP that works in the normalization in this field in groups with ISO and ASTM. Some standards try to develop an unambiguous and specific the vocabulary on this field, at least for its current situation [17] [18], others the documentation [19] and several other subjects important for the development technology and diffusion of this manufacture. This effort to making clear the concepts and the basic validations makes the traceability and quality something more real since the concepts and definitions will be at list very similar. The market presents several suppliers of powder solutions for AI [20]

The impact in the economy is diversified and improving the logistic tools, supporting of the maintenance by Additive Manufacture could be made ease by some kind of parts' library, e.g. gaskets and O-rings [21] [22]

Evolution of the basic paradigms of intelligent manufacturing and some questions regarding Human – Cyber-Physical Systems [23]. As it is very active area and in continuous evolution its ontology is not fully defined and perhaps increases will be possible, e.g. what could be the difference between a printer and a robot. If we accept that they tend to be very similar, perhaps concepts as *cobots* will appear [24]. Industry 4.0 is a wide concept and include several prominent technologies and the research in the subject is a hot topic with risks and opportunities [25] [26].

3 Security and Intellectual Property

Some concepts about intellectual property (IP) looks diffuse and the legal concepts even in daily subjects [27]. Otherwise some items must be subject of some control, like the *Liberator* printed gun [28] include in printers [29] [30]. Oher considerations are the safety or integrity of the produced part [31] [32], the ideal mark to track a good must be invisible at the produced part [33]. Some very specific characteristics of one equipment, let's say some trend some noise, distortion could be used to link the produced part with the printer, that trace the authenticity and quality of individual parts [34]. A different approach could be print a QR code, with some tracer chemical with or not blockchain connection [35], some discussions about the custody chain of the blockchain information was also supplied. There are considerations to keep safe the file 3D part and some encryption technics as discrete cosines transforms was proposed [36], the labelling or marking the parts to improve the traceability of the SS316L produced parts is reported elsewhere [37]. This tracking or identification tag is not a consensus but in a Scenario of embargo or of restriction use of Defence/aeronautical parts perhaps labelling could become a normal practice.

Forensics of AM equipment is possible and is becoming a trend [38] [39].

Vulnerability assessment of the manufacturing enterprise process monitoring in manufacturing systems. AM process is raising several questions about the safety in the physical and net chain and attack vectors, <.stl> extension files, are mentioned in the literature [40] [41]. The monitoring for parts and process authentication and verification of the design integrity could be performed by several different ways, destructive or not [42].

Security features for additive manufacturing in electronic files is one approach to keep some additional control of the AM process [43] [44].

To track the integrity of the production system several possibilities are idealized e.g. by the monitoring sound and noise at the manufacture island or by tracking the pattern of energy consumption of the motors and actuators in the shop [45] [25]

4 Aerospace and Defence industries and BDS questions

Systems and Software for Supporting Decisions based on AM Technologies in the Context of Defence are discussed elsewhere [46] [47] [48] [49] and a review of Laser Engineered Net Shaping (LENS) with pictures of some parts produced by this technology. [50]

Boycott, Divestment, and Sanctions (BDS) and its power of refusal could be a weapon or one of the tools to control or at least try to positioning about an issue [51]. The big challenge is more political than technical, the logistics to execute this process is difficult and several times involves crossing gray areas. To make it effective, it is necessary to ensure that both the scope and the objectives are clear, regular checks must be carried out to achieve goals and objectives. The purpose of this paper is to discuss and propose means to implement the sanctions envisaged, when proposing or implementing an embargo or restriction of productive capacity, it should be clear that the credibility of supervision and sanctions is the key to success [52]. With a technology that eventually facilitates the movement of manufacturing clusters the game of cat and mouse does not get simpler the surveillance and sanctions at an BDS scenario.

5 Proposal of this paper

The authors' proposal on intellectual property deals with safety issues in industry 4.0 so as not to limit its potential but aiming to improve quality and seek to ensure quantification and traceability in the production of a good in a third-party manufacture island / client. In our view the issue to be addressed in this commercial, political and legal arena, is how to manage and if appropriate block the production of a manufacturing cluster.

Obviously, this premise is made considering that the part is made with a protocol and / or "recipe" defined by the technology supplier and thus satisfactorily and consistently meets the safety and reliability requirements of the system where this part is inserted. If the customer, or final user, try

by its own risk or some illegal way produce the part will be more challenging to implementation any BDS. Technically, two broad classes of solutions can be considered, which ideally could not be done without tools like digital right management (DRM) and / or blockchains solutions and Internet of the Things (IoT):

Hardware: propose a topology in an IoT environment with a firewall designed to maintain communication in only 3 clouds (end user / client "C", Supplier of the technology "S" and trust one "T" chosen by "C" and "S") to track the production.

At Figure 1 presents a adapted Swedish tapestry, with a similar BDS clouds schema.

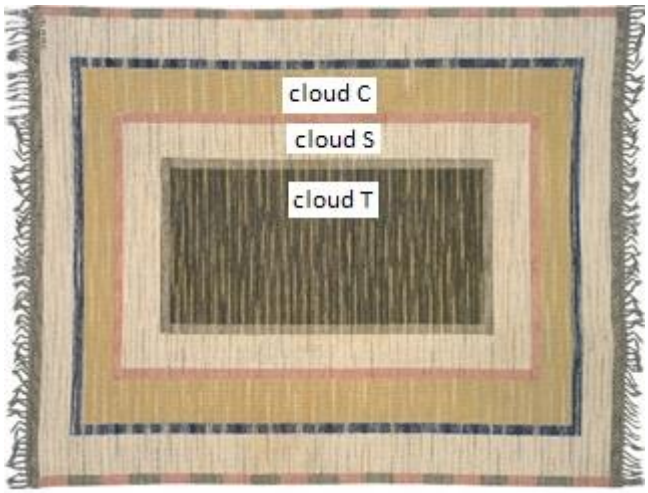

Figure 1: adapted Swedish tapestry represents similar BDS clouds.

Source: Nazmiyal Antique Rug Gallery, NYC

Software: The manufacturing files and instructions would be stored with the Trust one "T" and would be decoded and processed by a trusted channel in the manufacturing island for a defined amount of selected parts. So, this approach, would be, at least in ideal world, able to run in an untrusted environment to achieve a security goal.

Filev [53], schematics at Figure 2 and Figure 3, presents the innovation solutions to isolate the industrial area by firewall and or co-supervision at cloud computing and used at EXPOMAFE 2017 and 2019. FEI's University also participate of the exposition of Cluster with multiprotocol communication, with emphasis on OPC-UA and MTConect at **EXPOMAFE 2019 (https://www.expomafe.com.br/en/Home.html)** an initiative of The Brazilian Machinery and Equipment Builders' Association (ABIMAQ http://www.abimaq.org.br/site.aspx/abimaq-en).

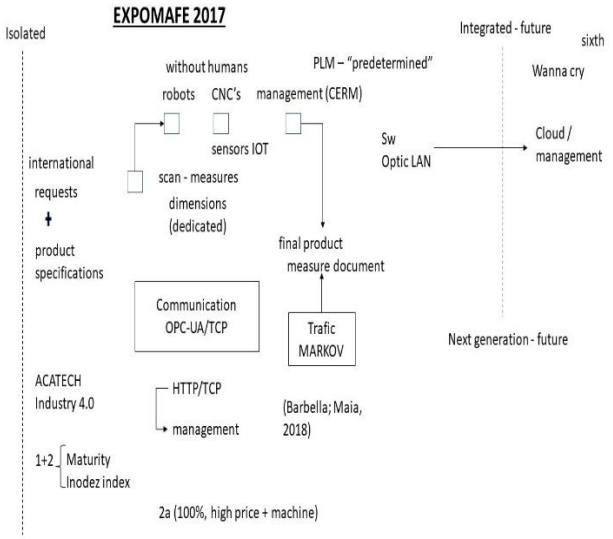

Figure 3: Conceptual architecture for an AM unit.

Source: Authors.

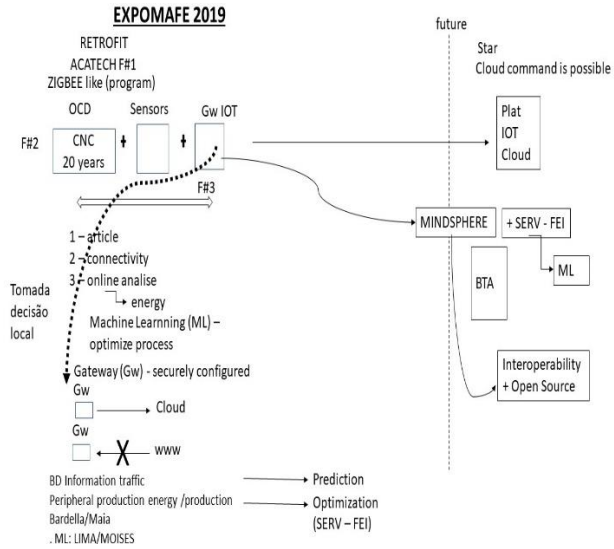

Figure 3: Conceptual architecture for an AM unit.

Source: Authors.

Conceptual architecture for AM unit, at Figure 2 and Figure 3, shows the importance integrating concepts about, open IOT, BDS clouds, machine learning and interoperability BTA.

The question to handle is what is, the more interesting architecture for intellectual protection and for a more restrictive scenario like as Defence industry or other specific ones that could be subject to embargo discussion, and sanctions that could be implemented after. Both approaches have their pros and cons, while in the hardware-focused option the manufacturing island would open the external inspection? Would it be technically feasible?

The archive virtual warehouse solution, with assurance of its integrity, would probably be more effective in avoiding "unwanted mirror" production units, since the production will be dependent of a file and instructions that will be managed by the three parts agreement. The basic idea is the files won't be able to duplicate and each batch need a new set of instructions and files to produce a very specific amount of parts, some newspapers are already produced in a similar way [54].

The point is that under embargo or conflict between the parts the solution the production's island architecture will be designed to not allow the operation, that will be stopped becoming inoperative if 2 of 3 clouds does not authorize the production.

On the other side of this solution, the part "C" cluster would be sure that the manufacturing process would not be altered without its knowledge, this is an inherent risk to current systems since the STUXNET and incidents where one relied on a security that proved to be fallacious. [55] [56]

Put that the recipe/files for production protocol will be shared by the three clouds, and just work together. The target is how to implement this at the hardware level and the net level and discuss this approach from the supply chain perspective.

Having made these considerations the safest, and most certainly the most complex, would be that the files could be segmented among the three participants of this agreement. In this way with the simultaneous input of the 3 participants the material would be produced. In case of a sanction and / or boycott, client "C" would only have his share of the files and thus should not be able to continue to produce the item in a clear formal and transparent sanction and / or boycott condition.

6 Final Conclusions

The AM becomes an important player at the logistic and supply chain due it's flexibility, capability for handle several materials, for production line its implementation is not so ease due questions related as price mainly due the raw material and for the printer and accessory units. For special parts or prototypes and small quantities the acceptation of this technics is bigger every day.

The question about how to guarantee the intellectual property and copyright is a fuzzy are with several questions raising tighter with the dissemination of the Additive Manufacturing / 3D printers. The perception is that some items area not challenging to by produced in this way, let's say use to copy and then how to control the copyright? The other side are the critical and complex parts that are difficult to produce and to copy and they could be represented for parts for aeronautic Defence and aerospace, those critical items that represent high tech and could be subject of BDS are the object of this paper and how to control its production. The technology is under continuous evolution and the supply chain, legislation must address those questions.

References

[1] E. OZTEMEL and G. SAMET, "Literature review of Industry 4.0 and related technologies," *Journal of Intelligent Manufacturing*, pp. 1-56, 24 Jul 2018.

[2] D. L. BOURELL, J. J. BEAMAN, M. C. LEU and D. W. ROSEN, "A Brief History of Additive Manufacturing and the 2009 Roadmap for Additive Manufacturing: Looking Back and Looking Ahead," in *US – TURKEY Workshop On Rapid Technologies, September 24 – 24, 2009*, 2009.

[3] ,. C. LEINENBACH, "Material Aspects in Metal Additive Manufacturing Challenges, Opportunities, Visions," in *LANL Workshop*, Santa Fé, 2015.

[4] M. N. ISLAN, H. GOMER and S. SACKS, "Comparison of dimensional accuracies of stereolithography and powder binder printing," *Int J Adv Manuf Technol*, pp. 3077 - 3087, 2017.

[5] ASTM, "ASTM F42/ISO TC 261 Develops Additive Manufacturing Standards," ASTM, [Online]. Available: https://bit.ly/2LsaUhg. [Accessed 05 Feb 2019].

[6] D. DUMOND, S. GLASSNER, A. HOLMES, D. C. PETTY, T. AWISZUS, W. BICKS and R. MONAGLE, "Pay it forward: Getting 3D printers into schools," in *IEEE Integrated STEM Education Conference*, PRINCENTON, 2014.

[7] MITxPRO, "Additive Manufacturing for Innovative Design and Production," 2019. [Online]. Available: https://additivemanufacturing.mit.edu/.

[8] J. GARDAN, "Additive Manufacturing technologies: state of art and trends," *Internation Journal of Production Research*, vol. 54, no. 10, pp. 3118-3132, 2016.

[9] A. Gebhardt and J.-S. Hotter, "Additive Manufacturing : 3D Printing for Prototyping and Manufacturing," 2016.

[10] E. PEI, M. RESSIN, R. CAMPBELL, B. EYNARD och J. XIAO, "Investigating the impact of additive manufacturing data exchange standards for re-distributed manufacturing," *Progress in Additive Manufacturing*, pp. 1-14, 12 Jun 2019.

[11] E. BLACKWELL, T. GAMBELLl, V. MARYA och C. SCHMITZ, "The great re-make: Manufacturing for modern times," 2017.

[12] M. HANNIBAL and G. KNIGHT, "Additive manufacturing and the global factory: Disruptive technologies and the location of international business," *International Business Review*, pp. 1116 - 1127, 2018.

[13] T. JOHNSTON, T. D. SMITH and J. L. IRWIN, Additive Manufacturing in 2040 Powerful Enabler, Disruptive Threat, RAND Corporation, 2018, p. 31.

[14] M. GÖTZ and B. JANKOWSKA, "Clusters and Industry 4.0 – do they fit together?," *European Planning Studies*, vol. 25 (9), pp. 1633 - 1654, 2017.

[15] RISE Research Institutes of Sweden, "ADDITIVE MANUFACTURING AT RISE IVF," [Online]. Available: https://bit.ly/2KMu8il.

[16] M. STEHN, I. WING, T. CARLILE, J. DICHAIRO and J. MARIANI, "3D opportunity for adversaries Additive manufacturing considerations for national security," Deloitte Development LLC, 2017.

[17] ISO/ASTM, *52921 (ASTM F2921) under revalidation*, 2013.

[18] ABNT/ISO, *Manufatura aditiva - Principios Gerais - Terminologia*, CEE 261/ Manufatura Aditiva, 2018, p. 25.

[19] ASTM, "The Global Leader in Additive Manufacturing Standards," ASTM, West Consohocken, 2017.

[20] SCHMOLZ + BICKENBACH Group, *Printdur® Metal powder for Additive Manufacturing*, Witten, 2018-016.

[21] H. KIM, M. CHA, B. C. KIM och D. MUN, ”Part library-based information retrieval and inspection framework to support part maintenance using 3Dprinting technology,” *Rapid Prototyping Journa*, vol. 25, pp. 630-644, 2019.

[22] R. AUGUSTSSON and D. BECEVIC, "Implementing Additive Manufacturing for Spare Parts in the Automotive Industry A case study of the use of additive manufacturing for spare parts," CHALMERS UNIVERSITY OF TECHNOLOGY, Gothenburg, 2015.

[23] Z. JI, L. PEIGEN, Z. YANHONG, W. BAICUN, Z. JIYUAN och M. LIU, ”Toward New-Generation Intelligent Manufacturing,” *ENGINEERING*, vol. 4, pp. 11-20, 2018.

[24] A. R. SADIK and B. URBAN, "An Ontology-Based Approach to Enable Knowledge Representation and Reasoning in Worker–Cobot Agile Manufacturing," *Future Internet*, vol. 9, no. 90, 2017.

[25] C. BAYENS, T. LE, L. GARCIA, R. BEYAH, M. JAVANMARD and S. ZONOUZ, "See No Evil, Hear No Evil, Feel No Evil, Print No Evil? Malicious Fill Patterns Detection in Additive Manufacturing," in *Proceedings of the 26th USENIX Security Symposium*, Vancouver, 2017.

[26] M. K. THOMPSON, G. MORONI, T. VANEKER, G. FADEL, I. CAMPBEL, I. GIBSON, A. BERNARD, ,. J. SCHULZ, P. GRAF, B. AHUJA and F. MARTINA, "Design for Additive Manufacturing: Trends, Opportunities, Considerations and Constraints," in *CIRP Annals Manufacturing Technology*, 2016.

[27] M. WEINBERG, ”3 Steps for Licensing Your 3D Printed Stuff,” 2015.

[28] W. A. WINDLE, "ADDITIVE MANUFACTURING: PREPARING FOR THE REALITY OF SCIENCE FICTION," Homeland Security Digital Library, Monterey, 2015.

[29] ALA American Library Association, "3-D Printing in Libraries: Policies & Best Practices," Chicago, 2018.

[30] T. MODEGI, "Proposal for 3D-Printing Regulation Technique in Fabricating Illegal Objects Using Feature-vector Based Matching Algorithm of 3D Shapes," in *SICE Annual Conference*, Tsukuba, 2016.

[31] M. YAMPOLSKI, T. R. ANDEL, J. T. McDONALD, W. B. GLISSON and A. YASINSAC, "Intellectual Property Protection in Additive Layer Manufacturing: Requirements for Secure Outsourcing," in *PPREW-4 Proceedings of the 4th Program Protection and Reverse Engineering Workshop*, New Orleans, 2014.

[32] M. YAMPOLSKIY, A. SKJELLUM, M. KRETZSCHMAR, R. A. OVERFELT, K. R. SLOAN och A. YASINSAC, ”Using 3D printers as weapons,” *International Journal of Critical Infrastructure Protection*, pp. 58-71, Sept 2016.

[33] V. ITIER, W. PUECH och A. BORS, ”CRYPTANALYSIS ASPECTS IN 3-D WATERMARKING,” i *IEEE International Conference on Image Processing (ICIP)*, Paris, 2014.

[34] F. PENG, J. YANG, Z.-C. LIN and M. LONG, "Source identification of 3D printed objects based on inherent equipment distortion," *Computers & Security*, vol. 82, May 2019.

[35] Z. C. Kennedy, D. E. Stephenson, J. F. Christ, T. R. Pope, B. W. Arey, C. A. Barretta and M. G. Warner, "Enhanced anti-counterfeiting measures for additive manufacturing: coupling lanthanide nanomaterial chemical signatures with blockchain technology," *Journal of Materials Chemistry C*, no. 37, pp. 9570-9578, October 2017.

[36] G. N. PHAM, J.-H. PARK, O.-H. KWON, H.-J. SONG, S.-H. LEE, K.-S. MOON, S.-T. KIM, Y.-R. CHOI och K.-R. KWON, ”Selective Encryption for 3D Printing Model in DCT Domain,” i *ICUFN 2018*, 2018.

[37] T. NIENDORF, F. BRENNE, M. SCHAPER, A. RIEMER, S. LEUDERS, W. REIMCHE, D. SCHWARZE and H. J. MAIER, "Labelling additively manufactured parts bymicrostructural gradation – advancedcopy-proof design," *Rapid Prototyping Journal*, vol. 22, no. 4, pp. 630-635, 22 May 2015.

[38] V. GARCIA och C. VAROL, ”Digital forensics of 3D printers,” i *2018 6th International Symposium on Digital Forensic and Security (ISDFS)*, Antalya, Turkey, 2018.

[39] D. BRADFORD MILLER, W. B. GLISSON, M. YAMPOLSKIY, Kim-Kwang and R. CHOO, "Identifying 3D printer residual data via open-source documentation," *Computers & Security*, vol. 75, pp. 10-23, Jun 2018.

[40] L. D. STURM, C. B. WILLIANS, J. A. CAMELIO, J. WHITE och R. PARKER, ”Cyber-physical vulnerabilities in additive manufacturing systems : A case study attack on the .STL file with human subjects,” *Journal of Manufcturing Systemas*, pp. 154-164, Jul 2017.

[41] Z. Xu and Q. ZHU, "Cross-Layer Secure Cyber-Physical Control System Design for Networked 3D Printers," in *American Control Conference (ACC)*, Bonston, 2016.

[42] T. KOMOLAFE, W. TIAN, G. T. PURDY, M. ALBAKRI, P. TARAZAGA and J. CAMELIO, "Repeatable part authentication using impedance based analysis for side-channel monitoring," *Journal of Manufacturing Systems*, vol. 51, pp. 42-51, 2nd Apr 2019.

[43] F. CHEN, G. MAC och N. GUPTA, ”Security features embedded in computer aided design (CAD) solid models for additive manufacturing,” *Materials & Design*, pp. 182 - 194, 2017.

[44] M. DAWSON, ”Cyber Security in industry 4.0: The Pitfalls of Having Hyperconnected Systems,” *Journal of Strategic Management Studies*, vol. 10, pp. 19-28, 22 Oct 2018.

[45] S. B. MOORE, J. GATLIN, S. BELIKOVETSKY, M. YAMPOLSKIY, W. E. KING and Y. ELOVICI, "Power Consumption-based Detection of Sabotage Attacks in Additive Manufacturing," 2017.

[46] D. S. GONZÁLEZ and A. G. ÁLVAREZ, "AM Manufacturing Feasibility Study & Technology Demonstration EDA AM State of the Art & Strategic Report," Fundación Prodintec, 2018.

[47] J. A. SAUCEDO-MARTíNEZ, M. PÉREZ-LARA, J. A. MARMOLEJO-SAUCEDO, T. E. SALAIS-FIERRO and P. VASANT, "Industry 4.0 framework for management and operations: a review," *Journal of Ambient Intelligence and Humanized Computing*, vol. 9, pp. 789 - 801, Jun 2018.

[48] E. N. ROTHMAN and A. ZIMMERMAN, "Editors’ Introduction," *RADICAL HYSTORY Review*, pp. 1-23, 1 May 2019.

[49] A. BUSACHI, J. ERKOYUNCU, P. COLEGROVE, R. DRAKE, C. WATTS, F. MARTINA, N. TAPAGLOU and H. LOCKETT, "A system approach for modelling additive manufacturing in defence acquisition program," in *11th CIRP Conference on Intelligent Computation in Manufacturing Engineering, CIRP ICME '17*, 2018.

[50] A. B. BUSACHI, J. E. ERKOJUNCU och COLEGROVE, ”Modelling Applications of Additive Manufacturing in Defence Support Services,” Cranfield University, 2017.

[51] M. HEDGES och N. CALDER, ”Near Net Shape Rapid Manufacture & Repair by LENS,” NATO, Neuilly-sur-Seine, 2006.

[52] D. FRUCHART, P. HOLTON, S. T. WEZEMAN, D. STRANDOW and P. WALLENSTEEN, "United Nations Arms Embargoes - Their Impact on Arms Flow and Target Behaviour," SIPRI Arms Transfers Project, Solna, 2007.

[53] R. FILEV MAIA, Interviewee, *Impressions on information security at manufacturing islands in the 4.0 industry.* [Intervju]. 12 Jun 2019.

[54] K. Van SYCKLE, ”See how the Times gets printed and delivered,” 2018.

[55] Ernst & Young LLP, ”Cybersecurity for Industry 4.0 Cybersecurity implications for government, industry and homeland security,” Kolkota, 2018.

[56] INCIBE, ”Emerging Threats to industrial Control Systems,” 23 Aug 2018. [Online]. Available: https://bit.ly/32eeVMy.