2019

Artificial Intelligence in the Aviation Manufacturing Process for Complex Assemblies and Components

Elena Vishnevskaya
Embry-Riddle Aeronautical University, navarrj1@erau.edu

Ian McAndrew
Capitol Technology University

Michael Johnson
The Boeing Company

Artificial Intelligence in the Aviation Manufacturing Process for Complex Assemblies and Components

IOP Conf. Series: Materials Science and Engineering **689** (2019) 012022 doi:10.1088/1757-899X/689/1/012022

Artificial Intelligence in the Aviation Manufacturing Process for Complex Assemblies and Components

McAndrew Ian, Vishnevskaya Elena, and Johnson Michael

[1] Capitol Technology University, Chichester, England
[2] Embry Riddle Aeronautical University, Bitburg, Germany
[3] The Boeing Company, North Charleston, SC, USA

Email: irmcandrew@captechu.edu; navarrj1@erau.edu; Michael.E.Johnson17@Boeing.com

Abstract. Aviation manufacturing is at the leading edge of technology with materials, designs and processes where automation is not only integral; but complex systems require more advanced systems to produce and verify processes. Critical Infrastructure theory is now used to protect systems and equipment from external software infections and cybersecurity techniques add an extra layer of protection. In this research, it is argued that Artificial Intelligence can reduce these risks and allow complex processes to be less exposed to the threat of external problems, internal errors or mistakes in operation.

1. Introduction

Commercial aircraft are now complex systems with parts, sections and components designed and produced globally. Commercial aircraft Assembly is more than classic assembly of bolting or joining parts together, systems are integrated, and automation is a foundation of all stages in manufacture. Many machine tool companies supply ‘turn-key’ systems that are controlled remotely to produce sub-assemblies. Directly, these are operated on-site, and local maintenance personnel ensure any concerns addressed immediately. When larger scale problems need sorting the software fixes may be completed remotely; this is potentially an infection point for a problem. Fig 1. below, shows a nosecone sub-assembly for an aircraft and indicates the complexity of the manufacturing both in terms of size and process.

Figure 1. Automation used in assembly for an aircraft nosecone.

2. Problems for consideration

There are several principal problems facing complex aviation automation that might result in damage, problems or long-term reliability concerns. On the basic level it could be a simple scratch on a component surface that leads to a fatigue crack of one where tooling is broken that results in risks to human lives. These can be categorized as: disgruntled employee, errors in operational use, deliberate external or internal control to cause immediate damage, deliberate external or internal control to cause damage at a later date and combinations of the latter two [1]. This research paper and research focuses on the last three stated. In theory, the production could be halted or even sabotaged by hackers; to damage the equipment. Such actions will make the equipment unusable or change tolerances and inspection values, which will approve components that need rejecting.

Aviation manufactures are aware of these concerns and have not been slow to react. Cybersecurity is key and applied at all stages of the development; both internally and externally. Likewise, Critical Infrastructure planning is now fundamental for all new equipment and software. Collectively these both attempt to prevent access and, if gained, access it will limit what could be changed [2]. They are not foolproof and as experience shows not a guarantee. Artificial intelligence offers possibilities to add a third and more effective layer of protection to the complete process. Additionally, neural networks are systems where decision making can be achieved to localize error detection or problem identification. System that can and should be used to compliment the detection are available but seldom, if ever, fully applied. This paper discusses the advantages and how they can work. It is a seminal research with the aim of incorporating manufacturing quality into the decision making process.

3. Review of techniques used to protect process

Cybersecurity has evolved in the last decade to be something that was considered and added with passwords to a whole industry that is adapting to ever more advanced attacked from governments and individuals. As expectations increase the use of passwords have been shown to be ineffective and many still use passwords that are predictable. Reports have shown that systems could be immediately be made more robust by 80% is Admin access was prevented. This research is more on the utilization than practical solutions. Systems needs minimum characters, special characters and numbers but still these are ‘cracked’ and by ever more advanced methods by hackers that could be from foreign governments, multi-nationals or individuals. Wi-Fi hopping is just one example of how *hackers* try to keep ahead of protections systems. Even government defense systems have been breached at times and these are with budgets for Cybersecurity far in excess of most industrial organizations. The reported security breaches are not publicized as much and probably not a main target currently; however, this is likely to change. Many manufacturers could find that their complete system is externally *infected* and unable to operate [3]. Regardless of the size of the company a Cyber-attack could potentially bankrupt any company or hold it to ransom for a release fee. As Cyber protection increases and the acceptance of prevention is not high, the concept of Critical Infrastructure (CI) has been added to systems. The concept is that if access gained to a system by unauthorized personnel then the scope of the damage possible is minimized and the system will recognize these actions and shut down their access or isolate to with the intention to stop. These plans can be physical, for example, access to areas and for remote access that a stealth approach is adopted to hide systems and limit what they can actually control and change [4]. CI is adding protection to manufacturing that compliments Cybersecurity, collectively, it creates two barriers; these are still effective but not making a fool proofing to give total confidence. Most literature will address defense, banking, food, transport and utilities but not commercial manufacturing. As a sector, manufacturing is not as advanced as others are and leaves vulnerabilities, see Fig 2 below.

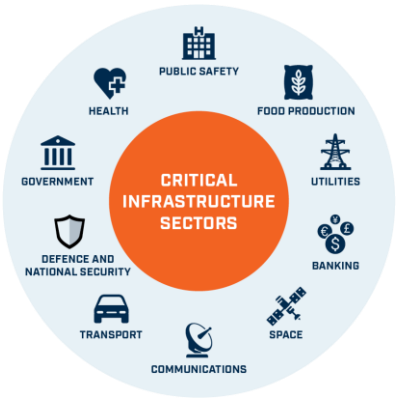

Figure 2. Principal Critical Infrastructure sectors.

Parallel to Cyber protection and Critical Infrastructure the subject of Artificial Intelligence (AI) is being researched and advanced for control systems in many sectors and uses. Manufacturing needs systems that not only make the system work but in ways that will enhance the operation and efficiency. Neural networks process information in the same biological way as a human brain. The interconnections allow for advantages and speed of processing [5]. Artificial neural network is one where there are many simple units of nodes each may have their own local processor. All this local units are connected by unidirectional channels, connections, which carry numeric data. All units work on a local level and with that data from these local unidirectional connections. Learning by example is the approach used as in the biological learning of humans. For example, if sending a signal to stop a motor operating is not effective, the signal will be sent by other connections to achieve the desired output.

Training is the basis for artificial neural networks and is generally classified as supervised or unsupervised. The former is where input and output values are given, and these are compared to make a logical decision from the local data [6]. When no inputs or outputs given it is unsupervised. These systems are autonomous as work logically as a child might identify an object. Unsupervised is ideal where human use skill to recognize but are not always able to clarify the decisions made each time [7]. Patterns are identified and remembered that the next time the correct decision is made instantly. Manufacturing is an example of where operators learn the process and identify errors or omissions. A good example is when we walk away from a car and close the door without looking back; the sound or lack of sound tells us of the output closed correctly.

—Neural Networks, NN, are massive parallel computation structures. This allows calculations to be performed at a high speed, making real-time implementations feasible, an important aspect of both protecting against cyber-attacks and cyber attackers attempting penetrate systems. Artificial neural networks, ANN, are useful in control systems where conventional approaches are not satisfactory. In fact, artificial neural systems are widely used nowadays in a variety of industrial control systems [8]. A large number of applications of ANN to robotics, failure detection systems, nonlinear systems identification and control of nonlinear dynamical systems have been proposed in recent years. Neural network models are known as an efficient and accurate tool for simulating manufacturing processes and as manufacturing systems become more complex their need is greater [9].

Neural networks is one of the applications in the cognitive science of AI. Neural networks are computing systems that are modelled after the brain's mesh-like network of interconnected processing elements (neurons). Interconnected processors operate in parallel and interact with each other. See figure 3 below.

These systems:

- allows the network to learn from the data it processes;
- recognizes patterns and relationships in data; and
- assists in the effective operation of any system.

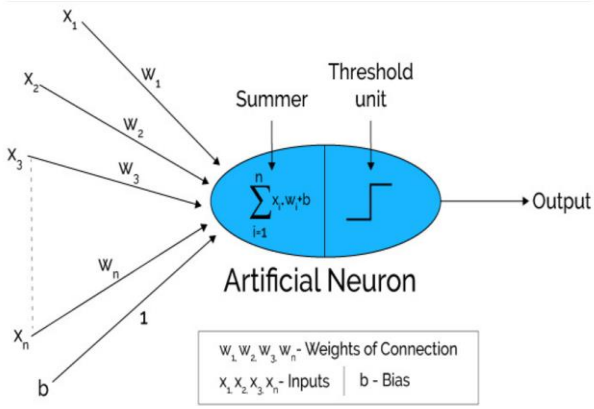

Figure 3. How Artifical Neural Networks operate.

In the 1980s, a new development in programming paradigms appeared that we know now as artificial neural systems, ANS. This was possible with faster computer processing times and that the microelectronics could incorporate localized IC to have input and output devices remotely in a system to suit the needs and designs [10]. It is only recently that these are becoming more widespread in all walks of industry. They work by:

- being based on the fundamental way the brain processes its information from its senses and knowledge stored;
- models solutions by training simulated neurons connected in a network to make the output dependable;
- similar to an analog computer using simple processing elements connected in a highly parallel manner;
- processing elements perform Boolean / arithmetic functions in the inputs; and
- key feature is associating weights with each element.

Initially, they were used in military and advances applications due to the costs and technical support. Nowadays, through the developments and drive for power systems they are becoming more widespread. It has been suggested that these will become core of all systems when security and intelligence needed [11]. In aviation manufacturing the final assembly is usually with main components made globally. Boeing have supplies in south America, Australia, Europe and these components can be major parts. For example, AIRBUS, has its wings flown in from Wales and assembled in France and German factories. Quality at all stages needs controlling and what is critical is that variations between parts and within parts needs to be consistent. Monitoring this and ensuring that they are protected from direct or indirect data corruption is now paramount. Inspection is not quality, using the full range of technology is now the minimum and that does not guarantee success and robustness from the problems stated above. Advantages of ANS:

- Nets can extrapolate and interpolate from their stored information;
- Nets have plasticity; and
- Excellent when functionality is needed long-term without repair in hostile environment – low maintenance.

ANS are not suited for number crunching or problems requiring optimum solution as is often needed in manufacturing, for example, direct measurements and comparisons to technical drawings. They do not make inferences but searches for underlying patterns [12]. Artificial neural networks is a popular methodology with lots of practical and industrial applications, from prediction models and control of turbines to industrial ANN control of calcinations processes. Identifying patterns can be a statistical

science on its own leading to the subject now addressed as data analytics.

The goal is not to build a human brain or even try to fully replicate, rather to support analysis of complex processes for modern systems, manufacturing and applications.

4. Analysis of artificial neural networks

Manufacturing in the civil aviation sector has been behind the advances of the principal CI industries as shown in fig. 2. The potential for crippling problems in the short, medium and long term is significant and most companies have accomplished minimal research. An external hacker that gained control or access to a manufacturing system could program the robots and machines to make movements at speed, which result in the destruction of the equipment and prevent any further work. Research has shown and argued Artificial Neural Network overseeing the system (ANN), Cyber and CI aspects that are embedded from the start in the design may offer benefits but fail to identify fully [13]. The AI aspects need to be incorporate at the launch stage of production to record, analyze and store this data that constantly can be used to compare and make decisions and at all stages of the lifespan the aircraft is produced. First, unsupervised training will be needed if used in addition for the start of production; although supervised training might be needed and useful for improving the system faster. Any security infections have the potential to control the process, alter tolerances or accept rejected parts. How this integrates in individual systems cannot be determined until a review related to Cyber and CI is applied to a specific process and forms the basis for the future work.

In Fig. 4 below shows an advanced automation by a robot that is controlled externally, locally by the system and also maintenance when needed. If controlled externally and the cyber protection breached, and critical infrastructure compromised there are several main problems or risks that need evaluation. Typical manufacturing systems could be changed that results in tolerances widened and thus rejects made and accepted [14]. If these are allowed to be used on an aircraft the potential for a disaster is compounded. Risk might evaluate these situations; identifying these risks if random or controlled is near impossible. Today's governments, companies and individuals are threats to aviation manufacturing. This ignores, as stated above, disgruntled and former employees.

Considering current manufacturing system architecture where Cyber and CI are integrated to control a complete system; the result is one where specified task, protocols and stages are completed in order and manner. If an artificial neural network is added as a top-level control that may initially be set to be a supervised system and eventually an unsupervised system that its role will be multi-faceted [15]. First, supervised ANN will be used to identify the basic concerns and activities to meet requirements. This would include a closed-loop on inspection to individual inputs for unsupervised teaching. Secondly, patterns, changes in patterns and outliers in the process can be identified for possible concerns and corrections. Thirdly, the times when software updates, remotely or locally, can be recognized and local concurrence at a high authority level will ensure any breaches are minimal or identified immediately. Finally, there should be no accessible externally to the ANN to prevent cyber-attacks. This latter comment is easy to state but forms the pivot of the problem to be solved.

Perhaps, its greatest role will be in unsupervised training for trends and comparison in component manufacture, assembly and testing. A full in-depth investigation is currently not complete and this research reports on the feasibility and implications of how the architecture can be employed that meets all three needs.

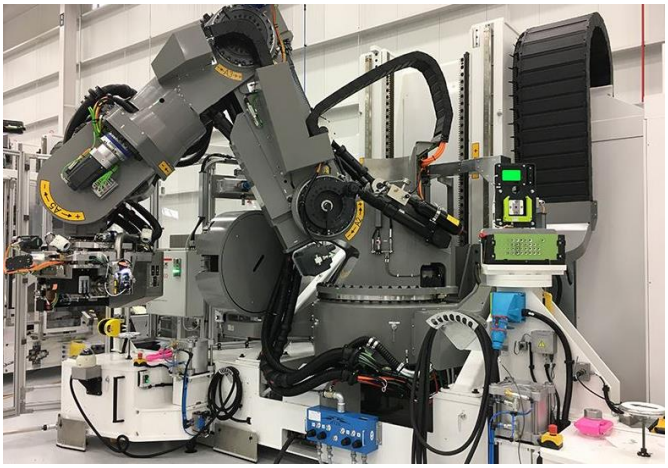

Figure 4. Automation as a sub-assembly within a larger system controlled locally and remotely.

Fig 5. below shows another aviation example where two identical processes are used. Consider the comparison possible for this data with unsupervised training of the information. Not just in manufacturing to pass inspection but long term. The life, maintenance, reliability and breakages of these aviation parts will be recorded for 30 years whilst commercially used. Given this data can be cross-referenced for its complete life variations in dimensions, interactions of measurements and success offers immediate, medium-term, long-term and life feedback of the parts to truly enable quality to be integrated at every level of use and predict future problems based of numerical analysis not probability.

Figure 5. Identical manufacturing processed.

Manufacturing in commercial aviation is a process that is expensive, extremely long-term in planning and one where mistakes and errors have huge consequences for all [16]. Every time a new aircraft is planned the finances needed are values approaching above the complete turn-over financially for several years and profits need forecasting over 30 years lifespans. Boeing's B 737 Max may yet result in significant restraints to the company, if this error was externally caused a company might never recover financially. Unlike other industries the aviation success depends significantly on reputation for safe products. The complexity now is at a level where control must extend beyond classic ways and explore advanced ways where the tasks can offer more than human control and dynamic feedback to support and identify needed actions. The potential to be inclusive in the design and quality stages can further enhance the complete system. Systems need evolving more to adapt and improve as technology changes and advances. Civil aviation manufacturing is such a sector and without adopting new technology a company will become globally redundant.

5. Summary

In this paper it has be argued that Critical Infrastructure and Cybersecurity techniques offer protection to aviation manufacturing up to a certain level. Artificial Intelligence with the focus on artificial neural network offers a level that adds protection and a unique dimension to learn and prevent both deliberate external and internal actions and identify trends to improve the process. Furthermore, this approach has benefits as feedback to suppliers, utilizing lessons from start-up problems to assist quality and reliability. As risks to systems increases then systems must be prepared and ever improving. Artificial Neural Networks is one dimension that can assist and offer additional benefits.

References

[1] Acemoğlu, D. and P. Restrepo (2017) Robots and jobs: Evidence from the US. https://voxeu.org/article/robots-and-jobs-evidence-us (Accessed on 30 July 2019)
[2] Cybersecurity Tech Accord (2018). Available from: www.cybertechaccord.org (Accessed 29th June, 2019).
[3] O'Brien, J & Marakas, G, (2006) Management Information System, McGraw Hill ISBN 0-07-111629-X
[4] Nydegger, R., & Enides, C. (2017). The psychology of work: Changes in the 21st century. International Business & Economics Research Journal, 3rd Qtr. 16(3), 197-203. Retrieved July 9, 2019, from DOI https://doi.org/10.19030/iber.v16i3.9993
[5] Haykin, S. (1994). Neural Networks, a Comprehensive Foundation. Macmillan, New York, NY.
[6] Beale, R. and Jackson, T. (1990). Neural Computing, an Introduction. Adam Hilger, IOP Publishing Ltd : Bristol. (ISBN 0-85274-262-2)
[7] Dayhoff, J. E. (1990). Neural Network Architectures: An Introduction. Van Nostrand Reinhold: New York.
[8] S. Jauhar, B. Chen, W. Temple, X. Don, Z. Kalbarczyk, W. Sanders, D. Nicol. "Model-based cybersecurity assessment with nescor smart grid failure scenarios". In 2015 IEEE 21st Pacific Rim International Symposium on Dependable Computing (PRDC) 2015 Nov 18 (pp. 319-324). IEEE.
[9] Buschle, M., Holm, H., Sommestad, T., Ekstedt, M. and Shahzad, K., 2011, June. A Tool for automatic Enterprise Architecture modeling. In International Conference on Advanced Information Systems Engineering (pp. 1-15). Springer, Berlin, Heidelberg.
[10] S. Noel, J. Ludwig, P. Jain, D. Johnson, R. Thomas, J. McFarland, & B. Tello. "Analyzing mission impacts of cyber actions (AMICA)." In NATO IST-128 Workshop on Cyber Attack Detection, Forensics and Attribution for Assessment of Mission Impact, Istanbul, Turkey, 2015.
[11] Lemaire, L., Lapon, J., De Decker, B. and Naessens, V., 2014. A SysML extension for security analysis of industrial control systems. In 2nd International Symposium for ICS & SCADA Cyber Security Research 2014 (pp. 1-9). BCS Learning & Development Ltd.; North Star House, North Star Avenue, Swindon, SN2 1FA, UK
[12] Wang, Y. N., Lin, Z. Y., Liang, X., Xu, W. Y., Yang, Q., & Yan, G. F. On modeling of electrical cyber-physical systems considering cyber security. Frontiers of Information Technology & Electronic Engineering, 17(5), 465-478, 2016.
[13] D. Liu. "Systems engineering: design principles and models." Boca Raton, FL: CRC Press 2015
[14] North Carolina State University Laboratory for Analytic Science website: https://ncsu-las.org/research-areas/sensemaking/ (Accessed on 30 July 2019)
[15] Le, T. (2018) Bridging Cybersecurity Skills Gap Through AI. Available from:https://www.scmagazine.com/home/opinions/bridging-the-cybersecurity-skills-gap-through-ai/
[16] Kagermann, H., Helbig, J., Hellinger, A., and Wahlster, W., "Recommendations for Implementing the Strategic Initiative Industrie 4.0: Securing the Future of German Manufacturing Industry; Final Report of the Industrie 4.0 Working Group," Forschungsunion, 2013. medium, provided the original work is properly cited (CC BY 4.0).