Proceedings of the Annual General Donald R. Keith Memorial Conference
West Point, New York, USA
May 2, 2024
A Regional Conference of the Society for Industrial and Systems Engineering

Enhancement of Medium Caliber Munitions Manufacturing Through Anticounterfeiting

Allen Dasilao, Cody Lominac, John McKenna, Bryson Stricker, and Phillip Bond

Department of Systems Engineering,
United States Military Academy,
West Point, NY 10996

Corresponding author's Email: bryson.w.stricker.mil@army.mil

Author Note: The team would like to express our sincere gratitude to the members of Joint Program Executive Office Armaments & Ammunition (JPEO A&A) who helped guide us through this senior capstone project. These members include LTC Paul Santamaria, MAJ Daniel Oesterheld, Kaitlyn Tani, Nicholas Malinowski, and MAJ Shane Kohtz. Additionally, the views expressed herein are those of the authors and do not necessarily reflect the position of the United States Military Academy, the Department of the Army, or the Department of Defense.

Abstract: The JPEO A&A together with the Fuze Division from Development Command (DEVCOM) Armaments Center is transitioning from mechanical to electronic fuzing across a broad spectrum of munitions, including medium caliber (e.g., 40mm) high and low-velocity grenades. The client requested an examination of the project to determine if concerns existed. A risk analysis of this initiative identified two potential risks: component obsolescence and component counterfeiting. The approach to combatting obsolescence is Commercial off the Shelf (COTS) components. The Department of Defense (DoD) strategy for combatting counterfeiting is Supply Chain Risk Management (SCRM). Counterfeiting can include recycling, relabeling/repackaging, low-spec components, cloning reverse engineering, forgery, and structural modification. Methods to combat these include aging detection, physical unclonable functions, scanning acoustic microscopy, and ultra-fast optical lasers. However, these methods may not be sufficient to address the most dangerous counterfeiting scenarios.

Keywords: Anticounterfeiting, Medium Caliber, Fuze, Integrated Circuit

1. Background

The Joint Programs Executive Office Armaments and Ammunitions (JPEO A&A) together with the Fuze Division from DEVCOM Armaments Center is transitioning from mechanical to electronic fuzing. The rationale for transitioning to electronic ordnance goes back to at least 1955 (Hudson, 1955). Through electronics, the functionality of the fuzes can be dramatically increased. Fuzes perform two essential functions. First, they prevent the inadvertent activation of the sequence of events that culminates in system detonation until specific conditions exist. In mechanical fuzes, this is typically achieved by leveraging the rifling in a barrel and centripetal force to physically rotate one object in relation to another. Then, the rapid acceleration as the object is launched creates a rearward force (set-back) that arms the weapon. Only when both conditions (rotation and setback) are met is the system armed. The second function of the fuze is to complete the detonation chain when the end effects conditions are met, such as achieving a certain height over the ground or making physical contact with an object. Electronic fuzes could have both electrical and mechanical components or be strictly electrical. In a completely electrical fuze, no components are physically moving in relation to each other. Sensors embedded on the integrated circuit board identify when the activation conditions have been met. The research team identified two potential concerns with a completely electronic fuze. Either the fuze fails to identify that the activation conditions exist (e.g., the weapon has been correctly launched and is at the correct distance over the target but fails to detonate) or the fuze activates in response to misinterpreted or intentionally created false conditions. Authenticity would mitigate both scenarios. Private industry performs different methods to conduct quality assurance on Integrated Circuit boards. Some of the methods used by these companies include Counterfeit Detection, Deep Learning, Ultrasound, Laser, and Failure analysis. These methods can mitigate but not eliminate the risk.

2. Qualitative Risk Analysis

This analysis focused on medium caliber munitions but could be expanded to more lucrative targets such as artillery and missiles. The team identified two categories of potential risk associated with electronic fuzing: obsolescence and

counterfeiting. Mechanical fuzes are immune from both. That is, if the intellectual property, machining capacity and materials exists, the components can be produced. The relatively high processing costs, provide little incentive for counterfeiting.

2.1 Obsolescence

Modern weapon systems take years to design, technologically mature, integrate, assemble, test, and manufacture. Components selected in the design phase must be tested and verified both as components and as part of subsystems. The time from when a Major Defense Acquisition Program (MDAP) becomes a program (typically MS B) to Initial Operating Capability (IOC) is called Portfolio Cycle Time (PCT). In 94 MDAPS the median PCT is 6.2 years (Hastings & Houston, 2020, p 28). Aircraft programs, such as the V-22 (22 years) and F-22 (14.5 years) can be two to three times longer. Figure 1, below, is a histogram of MDAP PCT since 1997.

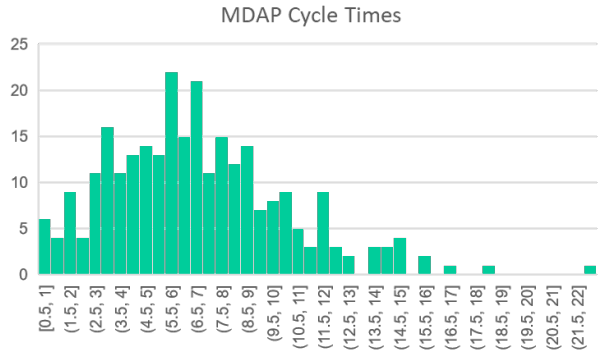


Figure 1 Portfolio Cycle Times of MDAPS Since 1997

Once acquired, systems may be retained for decades. The BGM-71 TOW reached IOC in 1970. The KC-135 began service in 1957. Up to 70% of a program's life cycle costs are Operations and Sustainment (Operations and Support Cost-Estimating Guide, 2014). The DoD's primary mitigation strategy to prevent obsolescence is to purchase COTs components. Rather than attempt to drive manufacturing of electronic components to suit the relatively small volume for defense systems, the strategy is to leverage the private sector's profit-driven initiatives. However, this innovation can mean that systems designed decades ago cannot acquire replacement parts no longer produced. The Navy's Office of Diminishing Manufacturing Sources and Material Shortages noted that from 1986 to 1993 the number of obsolescence notifications had increased from 200 to 7,000 (Pyett, Abbot, 1997). "Often, later in the lifecycle, obsolescence issues will force the DoD to look outside the original approved suppliers, to unapproved aftermarket suppliers who are subject to less programmatic oversight" (Army Materiel Command, 2018, p. 13). In other words, **obsolescence drives counterfeiting**. The Missile Defense Agency (MDA) created a checklist for suppliers to mitigate obsolescence risk. In an interview, the Manager of Quality, Safety, and Mission Assurance at the MDA identified the need to develop this checklist to monitor component availability and improve supply chain reliability.

2.2 Counterfeiting

Within the private sector, increased profit is a major driver of counterfeiting. Counterfeiters typically seek to make a small profit over a large volume of components. As of 2014, an estimated 1% of semiconductors were counterfeited, but the huge volume in the global market translates to an estimated $100 Billion per year in lost revenue to genuine manufacturers (Guin, et al. 2014). Counterfeit material poses a significant threat to the supply chain. It encompasses unauthorized copies or substitutes that deviate from the legally authorized manufacturer's specifications. Examples include the sale of used items as new, misrepresentation of capabilities beyond original specifications, variations in material construction from advertised details, and the incorporation of unauthorized features or capabilities, such as added malicious functions or modified firmware, not intended by the original equipment manufacturer or original component manufacturer. The presence of counterfeit materials can compromise the integrity and reliability of products, emphasizing the need for stringent measures to detect and prevent their infiltration into the supply chain (AMC, 2018).

The risk of counterfeit components can logically be split into two categories. The first being the component is made cheaply to make more profit at the risk of functionality and/or reliability. This would mean the product could be a 'dud.' That is, it fails to perform its intended function. The relatively low volume and long lifecycles of DoD fuzes suggests that a counterfeiter would have less of an opportunity for profit (e.g., recycling previously used parts). Absent wide-spread non-functionality, the impact was assessed as being less severe. The DoD Federal Acquisition Regulations System (DFARS)

addresses this risk through a process called Supply Chain Risk Management (DoD Instruction 4140.67 DoD Counterfeit Prevention Policy). For the purposes of this analysis, it is termed 'Failure Mode A.'

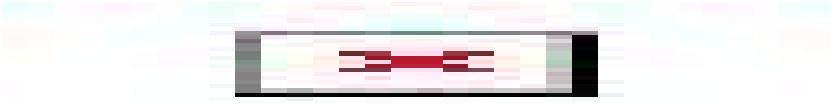
An alternative and more pernicious avenue could be to negatively affect system functionality (either randomly or on command) or to introduce unintended functionality (e.g., prematurely detonate on command). Termed Hardware Trojan Horses, these "maliciously modified parts are emerging as one of the major threats for embedded device security" (Balash, Gierlichs, & Verbauwhede, 2015). With hidden and essentially undetectable functionality pre-programmed into the electronic component any number malicious actions, such as exploding when fuzed, are possible. Moreover, once activated, the unpredictable system behavior could effectively eliminate an entire class of weapons (e.g., separately fuzed indirect fire) until an effective root cause analysis is conducted and corrective actions are devised. While deemed extremely unlikely, this risk was labeled as high severity. For the purposes of this analysis, it is termed 'Failure Mode B.' Unlike Failure Mode A above, despite extensive research, the team was not able to identify any DoD anti-counterfeiting process addressing this risk.

3. Quantitative Risk Analysis

One tool for risk management Failure Mode and Effects Analysis (FMEA). The scales used below for the FMEA is adapted from Quality Management in Plastics Processing (Kent, 2016). FMEA can use the following steps:

1. List the possible ways the component might fail
2. Evaluate the Severity (S) and estimate the Likelihood (L) and inability to Detect (D)
3. Find the Risk Priority Number (RPN) where RPN = S x L x D
4. Consider ways to reduce any numbers that are high

Table 1. Criteria for RPN Selection



The team requested Subject Matter Expert review/comment on the identified Threats. Table 1 below reflects the consensus or feedback received.

Table 2. Quantitative Risk Analysis

Threat	(S)	(L)	(D)	RPN	Comment
Obsolete component. Electronic component exceeded its life expectancy and must be replaced. It is no longer made by legitimate sources. Alternatives have a higher failure rate.	2	2	1	4	Failures would result in non-detonation. Lot inspections and other SCRM processes would reduce total risk
Counterfeit component. Supplier replaces component with lesser quality resulting in higher failure rate (Failure Mode A)	2	1	1	2	Existing SCRM processes are specifically designed to prevent this. If it occurred, lot segregation would reduce total risk.
Counterfeit component. Third-party actor intentionally replaces a component with another component that has a hidden function. (Failure Mode B)	10	1	10	100	A component with hidden functionality (e.g., premature detonation), is nearly undetectable. This functionality could make similar systems unusable until corrected.

4. Risk Response

4.1 DoD Risk Response Processes

The DoD primarily addresses obsolescence by purchasing COTS. The central strategy to address counterfeit components is stringent adherence to Defense Federal Acquisition Regulation Supplement (DFARS) clauses and Department of Defense Instructions (DoDI), such as DFARS 246.870 and DoDI 4140.67, which emphasize embedding counterfeit prevention measures in contractual agreements (Army Material Command, 2018). Procurement from authorized sources is prioritized, complemented by robust physical inspection and testing protocols as outlined in Department of the Army Pamphlet 702-20, particularly for items identified as high-risk (U.S. Department of the Army). These procedures are

meticulously documented to ensure a thorough audit trail. Furthermore, the DoD advocates for a culture of knowledge sharing and continuous improvement through specialized training and collaboration platforms like the Government-Industry Data Exchange Program (GIDEP) and the Parts Data Repository (PDREP), facilitating the dissemination of critical information and best practices across the defense supply chain. In cases where purchases from non-authorized sources are unavoidable, detailed risk assessments are mandated, along with adherence to testing standards set by organizations such as the Society of Automotive Engineers (SAE), referencing standards like SAE AS5553 for counterfeit electronic parts detection. Additionally, the Missile Defense Agency (MDA) implements supplementary measures for integrated circuit (IC) testing, including construction analysis, X-Ray scanning, and avoidance of brokers, with deviations triggering supply chain reviews to ensure authenticity and reliability of components. More recently, the MDA developed a checklist for SCRM assessment, involving 82 individual scoring criteria for components to minimize the risk of acquiring counterfeit components. The DAU subsequently adopted this checklist for other programs. Collectively, these risk management techniques are termed Supply Chain Risk Management (SCRM). SCRM attempts to mitigate both counterfeiting and obsolescence risk by selecting components and suppliers that are less likely to be counterfeited (by managing suppliers) or become obsolete (by managing supply).

4.2 Private Industry Risk Response Processes

Private industry consumes many orders of magnitude more electronic components than the DoD. Typically, commercial product life cycles are relatively short compared to DoD systems. Changing consumer demand requirements in the highly competitive electronic products industry implies that obsolescence is not a strong driver. In fact, planned obsolescence is a strategy designed to ensure a product is useless within a relatively short timeframe. For example, historically the replacement cycle for smartphones has been between two and three years (Kenton, 2022). The most likely concern for private industry is counterfeiting. More specifically, Failure Mode A. However, the risk of Failure Mode B does exist. In 2012, using a technique called Pipeline Emission Analysis (PEA), researchers were able to identify hidden commands and ‘backdoor’ passkey on military-grade Field Programmable Gate Array (FPGA) chips. With this information, an attacker can “disable all the security on the chip, reprogram crypto and access keys, modify low-level silicon features, access unencrypted configuration bitstream or permanently damage the device” (Skorobogatov & Woods, 2012). In other words, it is already possible for an actor to embed a “new backdoor or Trojan” to components that could be used for arming weapons. Private Industry, which has a different risk profile, is investigating numerous approaches to combat their risks.

4.2.1 Physical Unclonable Functions

Physical Unclonable Functions (PUFs) are components within an integrated circuit (physical) that translate inputs into outputs (function) in a way that is fixed to that specific hardware instance and is incapable of being reproduced (unclonable) (Kareem, 2021). PUFs are primarily used for two distinct functions, authentication, and obfuscation. For authentication, PUFs can be used to authenticate an integrated circuit’s identity by matching complex physical characteristics, rather than storing the identity in digital memory. This can be especially useful, as authenticating ICs using cryptographic primitives can be very costly, while PUF authentication techniques can be utilized by “even to extremely resource constrained platforms,” (Suh, 2007). The other function PUFs are useful for is obfuscation. For an organization attempting to prohibit an adversary or competitor from reverse-engineering their product, they must keep in mind that said adversary or competitor is highly likely to obtain physical access to the product. So, to prevent reverse engineering/counterfeiting of the product, a widespread practice is using hardware obfuscation. Hardware obfuscation involves using PUFs to conceal/obscure an IC’s true functionality to protect the intellectual property embedded in the product (Kareem, 2021). It is important to keep in mind that while this method protects the intellectual property within the integrated circuit, it will not stop the product itself from functioning, should an adversary utilize it.

4.2.2 Hardware Metering

Another common method for integrated circuit anticounterfeiting is hardware metering, with methods including combinational logic encryption, IC testing, and circuit camouflaging. Combinational logic encryption refers to the modification of an integrated circuit’s design, so that it only operates as intended when a set of “key inputs” are set to the correct values, similar to a locking mechanism or a password (Subramanyan, 2015). In order for an adversary or potential counterfeiter to gain access to the intellectual property of the IC, they would need to determine the values for all key inputs, which can be very costly, reducing the chances of counterfeiting. To prevent against counterfeit techniques such as the implementation of low-spec components, organizations using ICs can utilize a number of testing techniques to determine the quality of the product, including but not limited to, automated testing built into the manufacturing process itself, digital testing, mixed signal, and radio frequency testing (Grochowski). Finally, circuit camouflaging is another good method of preventing IC reverse-engineering. In any integrated circuit, each logic gate belongs to one of three categories – Exclusive

OR (XOR), Not-And (NAND), and Not-Or (NOR). A camouflaged gate's category cannot be determined through reverse engineering. From the viewpoint of a potential counterfeiter attempting to reverse engineer an integrated circuit, the camouflaged gate can belong to any one of the possible categories, however when inputs are applied to the gate in the original camouflaged gate, it still performs as intended. (Massad, 2015).

4.2.3 SAM/Ultra-Fast Optical Lasers

The Scanning Acoustic Microscopy method uses acoustic waves to scan an IC to detect deficiencies. It is a more mature technology than the UF laser method. While it is non-contact, it still presents some risks. Primarily, there is a trade off with resolution and penetration. If you need a higher resolution for the IC, then the waves will not penetrate as far. A smaller IC would also require higher frequencies with the same result (Hölzl, Wiesner, Zagar, 2012). As integrated circuits have changed over time, they have consistently gotten smaller and more powerful. In terms of risks and the emphasis on physical testing and inspections, as ICs approach the nanometer level, they become harder and harder to see in detail. However, using Ultra-Fast Optical Lasers, researchers have been able to see at the submicron level. This method also produces greater spatial resolution than nearly all other forms of scanning IC components. The strengths of this method are that it will maintain relevance as it can see down to a level we are not manufacturing yet. It also has shown the ability to see all the way down to the sub micrometer level with clear resolution. However, this method's greatest drawbacks are that it is a recent technology meaning it needs further maturing before it is ready for the production line. It also generates an immense amount of data that most computer and IT systems cannot handle, (Hölzl, Wiesner, Zagar, 2012).

4.2.4 Emerging Technologies

X-Ray Crystallography is a technique for determining the atomic structure of a crystal. Researchers used this technique to show how certain amino acids linked into protein chains create unique scatter patterns. These patterns essentially prove that a protein has the correct sequence (Vergara, Lorber, Zagari, Giege, 2002). As part of the research, it becomes clear that crystal growth responds to the conditions under which it was grown. In much the same way that each snowflake is unique because each descends under completely different growing conditions, crystals grown on a chip could be designed to create unique patterns for each chip. Other research indicates that each electronic component may have unique a unique Radio-Frequency (RF) DNA, "that the small-scale variations in the physical structure of each unique integrated circuit will similarly induce recognizable features in any unintentional emissions" (Cobb, et al, 2010). Still others propose using organic material with recognizable DNA chains as proof of authenticity.

All these experimental approaches point to identifying the authenticity of the component irrespective of the supply chain. With a fingerprint on the chip itself, not only could the authenticity of the chip be readily identified, but it could also be designed to show that no subsequent alteration has occurred at any point in the supply chain. Since the pattern is not replicable, the known fingerprint of any chip could be openly published.

5. Conclusions

Risk responses typically include Avoid, Transfer, Mitigate, and Accept. Mitigation strategies discussed above address Failure Mode A but do not address Failure Mode B. A Quantitative Risk analysis suggests Failure Mode B, while extremely unlikely, can have catastrophic consequences. It is already possible to introduce Trojan Horses to even military-grade electronic components. Current processes that private industry uses to address counterfeiting discussed above are better, but expensive. In an interview with Charles (Chuck) Peltier, Manager of Quality, Safety and Mission assurance for the Missile Defense Agency, it appears that programs do not significantly budget for anticounterfeit techniques, either during acquisition or in O&S. Although the Missile Defense Agency performs some destructive and non-destructive testing, more testing capability is desired. The Defense Acquisition University notes that Test & Evaluation funds typically comprise only 3% and 7% of the program budget (DAU, n.d.) and very little, if any, is dedicated to IC testing. Consequently, the risk response for Failure Mode A is a combination of Transfer (to suppliers) and Mitigation, but the response for Failure Mode B is currently Accept.

6. Recommendations

Simply increasing the program budget for acquisition efforts containing electronic components does not seem sufficient. A piecemeal approach to a potentially wide-spread concern, such as counterfeiting, is unlikely to achieve the level of performance necessary to mitigate the threat. The technologies are expensive and time-consuming. The processes involved require an elevated level of expertise. Emerging technologies are even more expensive and require even more expertise. Since one of the key aspects of electronic components is the level of commonality. This commonality spans all DoD services.

Consequently, it seems likely that a separate branch of the DLA could be established and funded to function in a tiered testing system. Individual programs would not have to design their own anticounterfeiting strategy. The excessive cost of the testing equipment would thereby be mitigated. There would be two tiers of testing, tier one testing would be the destructive and the more intense testing. After the ICs have been verified for use, they will then be purchased in mass quantities for DoD use. A central facility could be the processing capability for all ICs and electronic components used by the DoD. Programs would design IC to align with existing capability and inventory to improve commonality and economies of scale. Developing the means to fingerprint individual components would make a centralized verification site (e.g., using crystallography) more efficient and would greatly reduce risk.

7. References

Army Material Command. (2018) Counterfeit Parts and Materials Prevention Program Guidebook.

Balasch, J., Gierlichs, B., & Verbauwhede, I. (2015, August). Electromagnetic circuit fingerprints for hardware trojan detection. In *2015 IEEE International Symposium on Electromagnetic Compatibility (EMC)* (pp. 246-251). IEEE.

Defense Acquisition University (n.d.). Life Cycle Cost. Retrieved from Life Cycle Cost (LCC) | www.dau.edu

Hölzl, P. A., Wiesner, T., Zagar, B. G., Quality assurance for wire connections used in integrated circuits via magnetic imaging, 2012 IEEE International Instrumentation and Measurement Technology Conference Proceedings, Graz, Austria, 2012, pp. 2051-2056, doi: 10.1109/I2MTC.2012.6229127.

Guin, U., Huang, K., DiMase, D., Carulli, J., Tehranipoor, M., Makris, Y. (2014, 15 July). Counterfeit Integrated Circuits: A Rising Threart in the Global Semiconductor Supply, 102,8. Proceedings of the IEEE. DOI: 10.1109/JPROC.2014.2332291

Hastings, C., Houston K. (2020, 15 September). *Updates to Selected Analyses for the Performance of the Defense Acquisition System Series*. https://www.acq.osd.mil/asda/ae/ada/docs/PDAS%202019%20Excerpts_Final%20-cleared.pdf

Hudson, C. M. (May-June 1955). Electronics For Ordnance. Ordnance, 39, 210. Electronics for Ordnance on JSTOR

Kareem, H., & Dunaev, D. (2021, June 23). Physical Unclonable Functions based Hardware Obfuscation Techniques: A State of the Art. 2021 16th Iberian Conference on Information Systems and Technologies (CISTI). http://dx.doi.org/10.23919/cisti52073.2021.9476669

Kent, Robin. (2016). Quality Management in Plastic Processing. Retrieved 22 April. https://www.sciencedirect.com/science/article/abs/pii/B9780081020821500083

Kenton, W. (2022). Whiat is Planned Obsolescence? How Strategy Works and Example. Investopedia. Retrieved 22 March. https://www.investopedia.com/terms/p/planned_obsolescence.asp

Massad, M. E., Garg, S., & Tripunitara, M. (2015). Integrated Circuit (IC) Decamouflaging: Reverse Engineering Camouflaged ICs within Minutes [PowerPoint Slides]. Network and Distributed System Security, New York University, University of Waterloo. https://www.ndss-symposium.org/wp-content/uploads/2017/09/06IC.slide_.pdf

Massad, M. E., Garg, S., & Tripunitara, M. (2015). Integrated circuit (IC) Decamouflaging: Reverse engineering camouflaged ICs within minutes. Proceedings 2015 Network and Distributed System Security Symposium. http://dx.doi.org/10.14722/ndss.2015.23218

Office of the Secretary of Defense, Cost Assessment anf Program Evaluaiton, 2014. *Operation and support Cost-Estimating Guide*. os_guide_v9_march_2014.pdf (osd.mil)

Pyett, B., Abbot, G. (1997). Diminishing Manufacturing Sources and Material Shortages: Solutions to Obsolescence in Microcircuits: Executive Research Project.

Skorobogatov, S., Woods, C. (2012). Breakthrough silicon scanning discovers backdoor in military chip.

Subramanyan, P., Ray, S., & Malik, S. (2015, May). Evaluating the security of logic encryption algorithms. 2015 IEEE International Symposium on Hardware Oriented Security and Trust (HOST). http://dx.doi.org/10.1109/hst.2015.7140252

Suh, G., and Devadas, Srinivas. (2007). Physical unclonable functions for device authentication and secret key generation. In Proceedings of the 44th annual Design Automation Conference (DAC '07). Association for Computing Machinery, New York, NY, USA, 9–14. https://doi.org/10.1145/1278480.1278484

U.S. Department of the Army. (2023). Counterfeit Risk Management Product Assurance Handbook: Army regulation 702-20.

U.S. Department of the Army. (2023). Counterfeit Risk Management Product Assurance Handbook: Department of the Army Pamphlet 702-20.

Vergara, A., Lorber, B., Zagari, A., Giege, R. (2002). Physical aspects of protein crystal growth investigated with the Advanced Protein Crystallization Facility in reduced-gravity environments: Acta Crystallographica.