Development of a Chip-Level Ultimate Security Device Using Reactive Composites

Florent Sevely, Lionel Seguier, Tao Wu, Fabien Mesnilgrente, Sylvain Pelloquin, Carole Rossi

Development of a Chip-Level Ultimate Security Device Using Reactive Composites

Florent Sevely
LAAS-CNRS, University of Toulouse
7, avenue du Colonel Roche
Toulouse France
Email: fsevely@laas.fr

Tao Wu
LAAS-CNRS, University of Toulouse
7, avenue du Colonel Roche
Toulouse France

Sylvain Pelloquin
LAAS-CNRS, University of Toulouse
7, avenue du Colonel Roche
Toulouse France

Lionel Seguier
LAAS-CNRS, University of Toulouse
7, avenue du Colonel Roche
Toulouse France

Fabien Mesnilgrente
LAAS-CNRS, University of Toulouse
7, avenue du Colonel Roche
Toulouse France

Carole Rossi
LAAS-CNRS, University of Toulouse
7, avenue du Colonel Roche
Toulouse France
Email: rossi@laas.fr

***Abstract*— We developed an Ultimate Security Device (USD) that can, in case of intrusion or external attack, blow up a safety-critical component such as memory device. The device consists of two active parts (1) a pyroMEMS ignites in a fraction of millisecond (2) a mass of reactive composite, both encapsulated into a printed hermetic cap and placed over the sensitive component to be protected. After the presentation of the design and integration of the USD, we demonstrated that 400 mg of reactive composite permits to irreversibly destroy the silicon chips (~118 mm^3) in less than 10 ms. This ultimate security device provides a speedy and automatic response and can be programmed for tunable actions (generation of pressure burst, heat, chemical species) to implement relevant emergency safety responses.**

Keywords— anti-tamper, anti-revere engineering, anti-hacking, energetic materials, nanothermite, PyroMEMS, circuit breaker, Al/CuO

I. Introduction

Infrastructures are moving towards more heterogeneous, intelligent, connected, user-centric and collaborative electronic systems. This evolution has also brought rapid growth of criminal activity that threatens citizens, businesses, and governments. Typically, software attack and hardware intrusion such as reverse engineering which intends to clone, pirate, or counterfeit a design, to develop an attack pose a great threat to national security and must be actively addressed. Anti-tamper technologies are as old as the economy but requires constant adaptation to new extremely complex topologies and to reverse engineering technique being constantly evolving [1]–[12]. The simplest anti-tamper and anti-reverse engineering solutions are based on cryptographic keys or software [5], security fuses [13] to prevent non-authorized access, reinforcement of the components' coating and encapsulation [6]–[8] to avoid housing opening. More sophisticated solutions may include anti-tamper sensors able to detect the type of tampering such as Hall-effect switches [14]. And, often, especially for safety-critical components in order to ensure an efficient protection, several different anti-tamper protections are integrated [12], [15]. All these anti-tamper technologies, while being effective and in constant evolution, can be cracked or bypassed. That is why, to prevent the reverse engineering or tampering of a safety-critical system, upon the detection of intrusion, an ultimate action must be quickly taken before. Possible response includes the shut down or disable the device [16], [17], erase critical parts of memory and physically destroy the device [18]–[20]. In this work, we exploit the high-pressurization capability of Al/CuO nanothermites based composites [21]–[23] to design and fabricate a miniature ultimate security device ideally suited to protect sensitive data or hardware against reverse engineering or hacking. A threat is detected, the so called, ultimate security device (USD) remains in sleeping-mode until the threat occurs or simply a risk is imminent. It is then triggered in less than 100 µs by an electrical command and destroy irreversibly the sensible component against hacking, attempt or misuse. A nanothermite based reactive composite was chosen as they are the only attractive sources of reliable and "dormant" energy, exhibiting long shelf life (decades) and able to very quickly deliver gas, heat through a self-sustained redox reaction. For context, the decomposition of thermites can produce ~4 MJ/kg, which approaches the combustion of hydrocarbon materials (~50 MJ/kg), whereas a modern chemical lithium-ion battery stores only 0.5 MJ/kg.

After the presentation of the USD concept and design, the fabrication of the miniature (0.4 cm^3) USD device is presented in detail. The testing achieved on several mounted USD on SD memories cards demonstrates 100 % success of data destruction when 400 mg of reactive composite are integrated into the USD. Results also show that the reaction time and efficiency highly depend on the reactive material loading, e.g. the mass of nanothermites deposited onto the pyroMEMS [24]–[26]. The USD presented in this paper offers important advantages for safety-critical components such as the use of harmless material or substance for human and the tunability of the response which depends on the mass and nature of reactive composite integrated into the device.

II. USD operation principle and design

Fig. 1 represents a schematic diagram of the proposed USD and the operational principle for destroying a memory containing sensitive and critical informations. As shown in Fig. 1(a), the USD is made of two stacked main active parts:

- one microscale electric initiators, pyroMEMS. It consists of a thin thermite layer deposited on a thin-film resistive layer. When a current is applied to the resistance, the nanothermite is ignited by the Joule effect and reacts to produce a spark.

- one mass of reactive composite made of a mixture of Al/CuO nanothermite with copper complex ($Cu(NH3)4(NO3)_2$, labelled CuC) which is deposited in a 3D printed reservoir.

Fig. 1(b) shows the operational principle of the device. The USD is placed onto a memory card to be protected (Fig. 1b (2)) and remains in sleeping mode for years until a threat is detected. When a threat is confirmed (Fig. 1b (3)), the pyroMEMS is ignited in less than 100 µs and further ignite the reactive composite (Fig. 1b (4)). The combustion of the reactive composite generates a heat and pressure burst that mechanically destroy the silicon memory chip (Fig. 1b (5)).

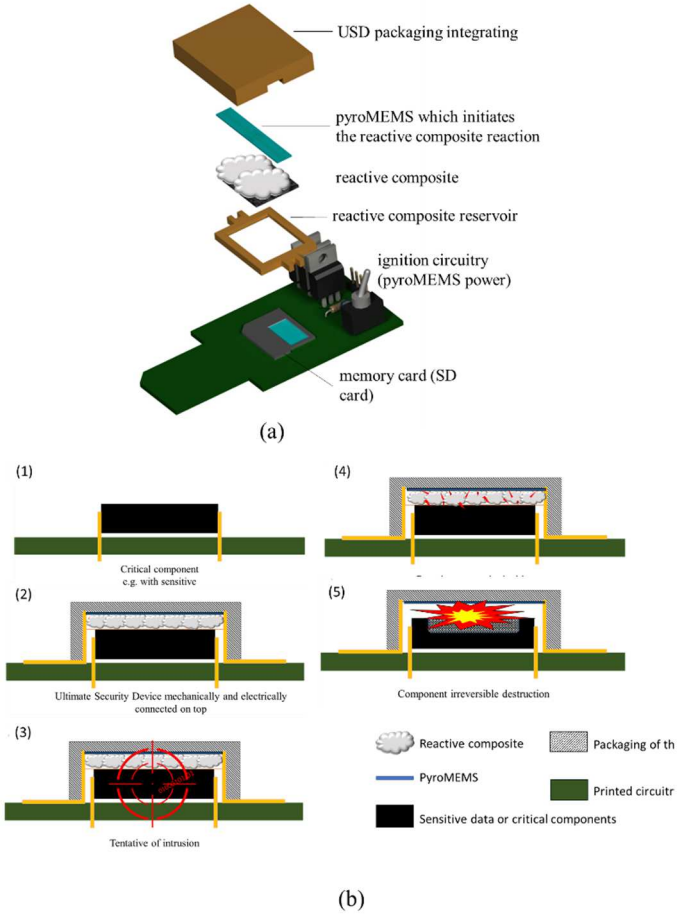


Figure 1. *Conceptual illustration of the USD operation principle. (a) Exploded view of the device, composed of a 2 stacked parts (a pyroMEMS and reactive composite printed in a reservoir). (b) Operating mechanism for utilizing the USD as a protecting device against the …. Of data contained in a memory.*

III. Fabrication and Assembly

PyroMEMS fabrication

A 500-µm thick 4-inch glass substrate is cleaned with oxygen plasma at 800 W for 5 min to remove surface contaminations. Next negative nLof photoresist (AZ nLof 2035, MicroChem Corporation, USA) is then spin coated and patterned using photolithography. Subsequently, 350-nm thick titanium and 300-nm thick gold layers are evaporated onto the surface and then patterned to define the Ti electrical resistor and Au electrical pads. Finally 13.9 mm² Al/CuO multilayer films are sputter deposited as described in [13], [27]–[29] on the micro-initiator directly in contact with the Ti electrical resistance (Fig. 2a).

Reactive composite formulation and printing

4.83 g (0.02 mol) of copper nitrate trihydrate is dissolved in 10 mL of distilled water followed by addition of 15 mL of 25% aqueous ammonia solution (0.24 mol). The final product (powder) [30] is separated via vacuum filtration and dried in an oven (Carbolite Gero, England) at 70 °C. The as-synthesized CuC powders are milled using a Retsch CryoMill machine using alumina grinding balls (diameter: 25 mm). Milling parameters are: frequency of 30 Hz (30/s) for 10 min while equipped with liquid N_2 cooling. In parallel, 91 mg of aluminum nanopowders (Al, average particle size: 80 nm, purity: 69 % purchased from Novacentrix, USA) and 203 mg of copper oxide (CuO, average particle size: 100 nm purchased from Merck, Germany) are mixed with 86 mg of milled CuC powder and dispersed in 20 mg of polymer polyvinylpyrrolidone (PVP) and ethanol (4 ml) and then stirred 45 minutes in a sonication bath cooled by ice. It has to be noted that the equivalence ratio for the CuC over Al/CuO nanopowder is 25%. PVP enables a good dispersion and stabilization of the nanoparticles [31] (Fig. 2b). The reactive composite is then deposited into the USD reservoir using a volumetrically controlled dispenser: the precision of the deposition is 6 µL, e.g. 1.14 mg.

Reservoir and external packaging fabrication

The USD packaging is made in two parts:

- The external packaging which is a rectangular cap in dimensions adapted to fit on the component to be protected. At its bottom, a trench is designed to host and electrically connect the pyroMEMS.
- The second part is a rectangular reservoir with two functions: block the pyroMEMS in its trench and store the reactive composite.

On the side of both parts, holes let the pyroMEMS electrical contact to go through the packaging and to the printed circuit board *(PCB)* described in next section. Both parts were printed in Nylon *(Z-NYLON, Zortrax, Poland)* using a 3D printer (*Zortrax M300plus*). Photos are given in Fig. 2c. 3D printing technology were chosen because it offers a good resolution (±0.09 mm) while being low cost and fast for prototyping. Nylon offers a good compromise between cost and thermal and mechanical resistance.

Printed circuit board (PCB)

The circuitry (Fig. 2e) is a basic capacitive discharge circuit that is able to initiate the pyroMEMS in less than 100 µs. It is composed of 3 transistor MOS *(MOSFET, Canal-N, 20 A 60 V TO-220AB, 3 pins, ON Semiconductor, Malaysia & MOSFET, Canal-P, 14 A 100 V TO-220AB, 3 pins, Infineon, Germany*) and a10 µF chemical capacitor *(Capacitor RS PRO, 10µF, 63V c.c., Taiwan)*. This circuit is powered by a lab. power supply *(Agilent U8031A, Agilent technologies, Malaysia)* and driven by an *Arduino prototyping board*.

Assembly

For the demonstrations, we chose a commercial *Transcend SDHC memory Card 8GB,* so called SD card *(Transcend, Taiwan)* It offers the advantage to be easily readable and programmable with a computer. Its packaging made in Epoxy resist reinforced with silica, making the packaging is resistant to heat and pressure. Therefore, we first open a 4 × 10 mm² squared window into the packaging to access to the Si memory, taking care to not destroy the internal wires bonding and electrical connexions, nor the passive components and the silicon chip that constitutes the memory. This step is done by chemical etching using nitric acid, HNO_3. The prepared SD card is then checked, programmed and mounted and connected on the printed circuit board shown in Fig. 2e.
In a second step, the electronic components are welded on the PCB. At last, the USD is assembled with the PyroMEMS, filled with the reactive material then sealed with cellophane. After its preparation, the USD is mounted on the SD, soldered and attach to the printed PCB.
A photo of the USD mounted on the SD is shown in Fig. 2f.

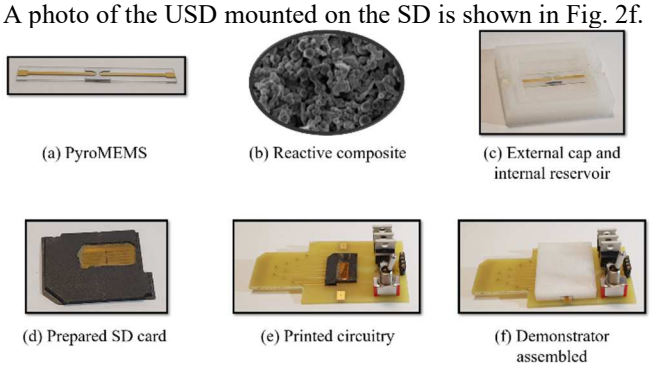
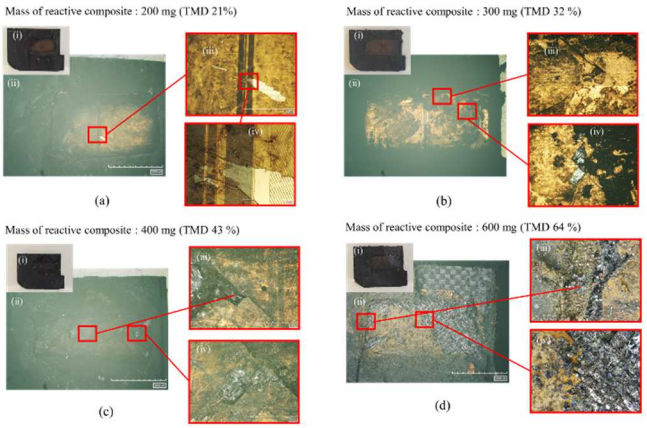


Figure 2. Photo of (a) the pyroMEMS, (b) the reactive composite reserved in a vial, (c) the packaging and reservoir fabricated in Nylon by 3D printing, (d) the prepared SD card memory, (e) Printed circuit board with the electrical schema, (f) On-Chip Ultimate Security Device fully assembled on a memory card for demonstration.

IV. Characterization

Several demonstrators was prepared and tested with 5 different masses of reactive composite, corresponding to different compaction rates expressed in % TMD (1) : 100 mg (TMD% = 11%), 200 mg (TMD% 21.26%); 300 mg (%TMD = 32%); 400 mg (%TMD = 43%); 600 mg (%TMD = 64%). After the ignition and reaction of the reactive material, the demonstrators were opened and SD cards observed visually and using a Microscope *Hirox RX-100* with a ×20 and ×140 magnification (Fig.6 iii). All pictures were taken using a multi-focus technique allowing us to see rifts / trenches in a full reconstituted picture without any blur. Results are summarized in Fig. 6 for configurations 200 mg, 300 mg, 400mg and 600 mg. Results are given in the form of photos of the SD cards after the tests: (i) a non-magnified, (ii) magnification ×20, (iii) and (iv) ×140 magnification. photo 100 mg configuration was not given as the SD card remains intact after the test.

$$\%\text{TMD} = \frac{\text{mass of reactive composite}}{\text{TMD} \times \text{volume of the reservoir}} \times 100 \qquad (1)$$



Where TMD is the theoretical density of the reactive composite, calculated equal to 3.51 g/cm³ and the volume of the reservoir is 268 mm³.

Figure 3. Photos of the SD cards after the tests.

It was observed that with 600 mg, the SD card became fully destroyed: a part of the packaging was torn out and most of the silicon chip was pulverised. When not pulverised, the silicon features rifts and holes (Fig. 3d (iii) and (iv)). This result therefore confirmed the feasibility of our concept as we destroyed the silicon component with all the data in it. With 400 mg, some parts of the silicon chip were pulverized and rifts run across the chip. Although the damages are less intense than using 600 mg of reactive composite, the SD was enough damaged and the data totally destroyed. With 300 mg we observe some cracks into the silicon chip and some shard have been torn off (Fig. 3b (iii) and (iv)). The silicon surface is covered by superficial scratch but the SD card remain unbroken and data can be read. The test has failed. With 300 mg, the SD remain totally intact and therefore tests have failed. These tests not only validated the allowed us to determine the minimum amount of energetic material needed to destroy a silicon chip and to make it unreadable. With only 400 mg of reactive material we archived our goal.

V. Conclusion

The concept of a chip-level ultimate security device based on nanothermite composite has been demonstrated: we successfully destroy in ~5 ms a memory card and its containing data. The fabricated made to measure device is 29 mm wide & 34 mm long and simply mounted onto the safety-critical component. 400 mg of reactive composite permits to destroy physically all the silicon chip, but the energetic response can be adapted by tuning the mass of reactive powder depending on the level of destruction desired and the type of component to neutralize.

VI. Ackowledgements

The authors acknowledge support from the European Research Council (H2020 Excellent Science) Researcher Award (grant 832889 – PyroSafe). This work was also supported by LAAS-CNRS technology platform, a member of Renatech network. We acknowledge the French Defense Agency DGA which partially funds F.S. scholarship.

VII. References

[1] I. McLoughlin, "Secure Embedded Systems: The Threat of Reverse Engineering," in *2008 14th IEEE International Conference on Parallel and Distributed Systems*, Melbourne, VIC, Dec. 2008, pp. 729–736. doi: 10.1109/ICPADS.2008.126.

[2] H. A. Müller, K. Wong, and S. R. Tilley, "Understanding software systems using reverse engineering technology," in *Object-Oriented Technology for Database and Software Systems*, WORLD SCIENTIFIC, 1995, pp. 240–252. doi: 10.1142/9789812831163_0016.

[3] Z. Lin, X. Zhang, and D. Xu, "Automatic reverse engineering of data structures from binary execution," in *Proceedings of the 11th Annual Information Security Symposium*, West Lafayette, IN, Mar. 2010, p. 1.

[4] M. Hassan, A. M. Kaushik, and H. Patel, "Reverse-engineering embedded memory controllers through latency-based analysis," in *21st IEEE Real-Time and Embedded Technology and Applications Symposium*, Apr. 2015, pp. 297–306. doi: 10.1109/RTAS.2015.7108453.

[5] G. Ozsoyoglu, D. A. Singer, and S. S. Chung, "Anti-Tamper Databases," in *Data and Applications Security XVII: Status and Prospects*, S. De Capitani di Vimercati, I. Ray, and I. Ray, Eds. Boston, MA: Springer US, 2004, pp. 133–146. doi: 10.1007/1-4020-8070-0_10.

[6] L. Li, P. Wang, and Y. Zhang, "Design of anti-key leakage camouflage gate circuit for reverse engineering based on dummy vias," *Microelectronics Journal*, vol. 90, pp. 163–168, Aug. 2019, doi: 10.1016/j.mejo.2019.06.006.

[7] A. R. Desai, "Anti-Counterfeit and Anti-Tamper Hardware Implementation using Hardware Obfuscation," Thesis, Virginia Tech, 2013. Accessed: Sep. 01, 2021. [Online]. Available: https://vtechworks.lib.vt.edu/handle/10919/23756

[8] Z. Guo, M. Tehranipoor, D. Forte, and J. Di, "Investigation of obfuscation-based anti-reverse engineering for printed circuit boards," in *Proceedings of the 52nd Annual Design Automation Conference*, New York, NY, USA, Jun. 2015, pp. 1–6. doi: 10.1145/2744769.2744862.

[9] S. Chen, J. Chen, and L. Wang, "A Chip-Level Anti-Reverse Engineering Technique," *J. Emerg. Technol. Comput. Syst.*, vol. 14, no. 2, p. 29:1-29:20, Jul. 2018, doi: 10.1145/3173462.

[10] S. Chen, J. Chen, D. Forte, J. Di, M. Tehranipoor, and L. Wang, "Chip-level anti-reverse engineering using transformable interconnects," in *2015 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFTS)*, Oct. 2015, pp. 109–114. doi: 10.1109/DFT.2015.7315145.

[11] M. Shiozaki, R. Hori, and T. Fujino, "Diffusion Programmable Device : The device to prevent reverse engineering," p. 5.

[12] D. M. J. Atallah, E. D. Bryant, and D. M. R. Stytz, "A Survey of Anti-Tamper Technologies," p. 5, 2004.

[13] C. Rossi, "Nano-Engineering of Al/CuO Multilayers: Bridging the Gap Between Research and Applications," p. 2.

[14] S. Patnaik, N. Rangarajan, J. Knechtel, O. Sinanoglu, and S. Rakheja, "Advancing hardware security using polymorphic and stochastic spin-hall effect devices," in *2018 Design, Automation Test in Europe Conference Exhibition (DATE)*, Mar. 2018, pp. 97–102. doi: 10.23919/DATE.2018.8341986.

[15] O. Koemmerling and M. G. Kuhn, "Design Principles for Tamper-Resistant Smartcard Processors," p. 13.

[16] A. Nicollet, L. Salvagnac, V. Baijot, A. Estève, and C. Rossi, "Fast circuit breaker based on integration of Al/CuO nanothermites," *Sensors and Actuators A: Physical*, vol. 273, pp. 249–255, Apr. 2018, doi: 10.1016/j.sna.2018.02.044.

[17] P. Pennarun, C. Rossi, D. Estève, and D. Bourrier, "Design, fabrication and characterization of a MEMS safe pyrotechnical igniter integrating arming, disarming and sterilization functions," *J. Micromech. Microeng.*, vol. 16, no. 1, pp. 92–100, Dec. 2005, doi: 10.1088/0960-1317/16/1/013.

[18] T. J. Fleck *et al.*, "Controlled Substrate Destruction Using Nanothermite," *Propellants, Explosives, Pyrotechnics*, vol. 42, no. 6, pp. 579–584, 2017, doi: https://doi.org/10.1002/prep.201700008.

[19] E. R. Westphal *et al.*, "The Effects of Confinement on the Fracturing Performance of Printed Nanothermites," *Propellants, Explosives, Pyrotechnics*, vol. 44, no. 1, pp. 47–54, 2019, doi: 10.1002/prep.201800188.

[20] V. Brailovski, F. Trochu, and G. Daigneault, "Temporal characteristics of shape memory linear actuators and their application to circuit breakers," *Materials & Design*, vol. 17, no. 3, pp. 151–158, Jan. 1996, doi: 10.1016/S0261-3069(96)00049-0.

[21] J. Song *et al.*, "A comparative study of thermal kinetics and combustion performance of Al/CuO, Al/Fe2O3 and Al/MnO2 nanothermites," *Vacuum*, vol. 176, p. 109339, Jun. 2020, doi: 10.1016/j.vacuum.2020.109339.

[22] T. Wu, F. Sevely, S. Pelloquin, S. Assie-Souleille, A. Esteve, and C. Rossi, "Enhanced Reactivity of Copper Complex-Based Reactive Materials via Mechanical Milling," *Combust Flame In Review*, 2021.

[23] T. Wu *et al.*, "Unexpected Enhanced Reactivity of Aluminized Nanothermites by Accelerated Aging," *Chemical Engineering Journal*, p. 129432, Mar. 2021, doi: 10.1016/j.cej.2021.129432.

[24] J.-L. Pouchairet and C. Rossi, "PyroMEMS as Future Technological Building Blocks for Advanced Microenergetic Systems," *Micromachines*, vol. 12, no. 2, Art. no. 2, Feb. 2021, doi: 10.3390/mi12020118.

[25] D. A. de Koninck, D. Briand, and N. F. de Rooij, "A shadow-mask evaporated pyroMEMS igniter," *J. Micromech. Microeng.*, vol. 21, no. 10, p. 104013, Sep. 2011, doi: 10.1088/0960-1317/21/10/104013.

[26] L. Salvagnac, S. Assie-Souleille, and C. Rossi, "Layered Al/CuO Thin Films for Tunable Ignition and Actuations," *Nanomaterials*, vol. 10, no. 10, Art. no. 10, Oct. 2020, doi: 10.3390/nano10102009.

[27] J. Zapata, A. Nicollet, B. Julien, G. Lahiner, A. Esteve, and C. Rossi, "Self-propagating combustion of sputter-deposited Al/CuO nanolaminates," *Combustion and Flame*, vol. 205, pp. 389–396, Jul. 2019, doi: 10.1016/j.combustflame.2019.04.031.

[28] G. Taton, D. Lagrange, V. Conedera, L. Renaud, and C. Rossi, "Micro-chip initiator realized by integrating Al/CuO multilayer nanothermite on polymeric membrane," *J. Micromech. Microeng.*, vol. 23, no. 10, p. 105009, Sep. 2013, doi: 10.1088/0960-1317/23/10/105009.

[29] A. Nicollet *et al.*, "Investigation of Al/CuO multilayered thermite ignition," *Journal of Applied Physics*, vol. 121, no. 3, p. 034503, Jan. 2017, doi: 10.1063/1.4974288.

[30] T. Wu *et al.*, "New coordination complexes-based gas-generating energetic composites," *Combustion and Flame*, vol. 219, pp. 478–487, Sep. 2020, doi: 10.1016/j.combustflame.2020.05.022.

[31] F. Sevely *et al.*, "Effect of Process Parameters on the Properties of Direct Written Gas-Generating Reactive Layers," *ACS Applied Polymer Materials*, Jul. 2021, doi: 10.1021/acsapm.1c00513.