RY20-9

DAGSI Research Topic

1) **Research Title:** Adaptable Protection for Embedded Systems Resilience

2) **Individual Sponsor:**

Dr. Tem Kebede, AFLR/RYWA
2241 Avionics Circle, Blg 620
Wright-Patterson AFB OH 45433
temesgen.kebede.1@us.af,mil

3) **Academia Field/Education Level**

Electrical Engineering, Computer Science, Computer Engineering and Systems Engineering (MS or PhD level).

4) **Objectives**: Software and/or hardware embedded systems play an integral role in performing mission specific tasks. However, current defense techniques for Unmanned Aerial Systems (UAS) or Intelligence Surveillance Reconnaissance (ISR) systems are inadequate to rapidly adapt and respond to unforeseen events - threats or unpredicted changes of conditions in a software and hardware environment. Such events could include malware attacks or unexpected malfunctions of one or more of the system components. System resilience at all levels, software and hardware, i.e., the ability to withstand such events, by adapting and responding (i.e., self-repairing) efficiently and effectively in order to assure successful mission execution is highly critical. Therefore, the proposed research project should develop a game-changing resilient framework that can detect, adapt and respond to "zero-day" attacks and/or malfunctions. To this end, the objectives of this project are (1) to develop an approach for embedded systems that includes systematic techniques to allocate available resources in anticipation of adaptability, (2) to develop a self-checking mechanism so as to easily detect any form of unintended modification/behavior (e.g., malware attacks or malfunctions), and (3) to develop the capability to self-repair/heal so as to retain the original functionality of the system as a whole, thereby assuring successful mission completion.

5) **Description:** Applications that are critical to mission related tasks require software and/or hardware resiliency, most importantly, the ability to properly self-repair from damages in order to ensure mission accomplishment. Although some work has been done in detecting malware attacks, or system malfunctions, there is little or no research in recovering from the detected threat or malfunction in a critical time-interval. Today's conventional software and/or hardware implementations are highly geared towards *independent* and *interchangeable* modules/units that attend to separate aspect of the desired mission-oriented functionality. Hence, a damaged module could be detrimental to mission execution, i.e., software and/or hardware modules remain

vulnerable during mission operation. To enable resilience, the architecture of the protection system supporting functional redundancy will be useful. This raises questions on *minimal* redundancy supportive of *maximum* resilience, including mechanisms to self-check the overall functionality of the system. Moreover, if one or more units are damaged, evolutionary approaches used in conjunction with the protection architecture must ensure that the entire system can re-self-assembled or rapidly repaired.

6) **Research Classification and Restrictions:** Basic Fundamental research, no restrictions anticipated.

7) **Eligible Research Institutions:** University of Cincinnati, University of Dayton, Wright-State or other state universities with a suitable research background.

PA clearance for DAGSI TOPIC "Adaptable Protection for Embedded Systems Resilience": 88ABW-2019-3944