Facilitating Assurance and Collaboration through Digital Threads in Microelectronics Experiments

Edward Carlisle IV, Scott Harper, Jonathan Graf
Graf Research Corporation
Blacksburg, Virginia, USA
benches@grafresearch.com

***Abstract*—Laboratory experimentation with circuits and systems can be a complex process. Exact repetition of processes such as radiation testing, second-party verification of conclusions drawn from side channel analysis, and preservation of experimental processes all require the full detail of an experiment to be captured when it is run. Capturing a digital thread of an experiment provides this capability but can be a complex process that is prone to human error if not fully automated. This paper presents an automated microelectronics lab experimentation platform called Benches. We describe how Benches automates the capture of the digital thread of a microelectronics experiment and how these digital threads facilitate assurance and collaboration.**

Keywords—Digital Thread, Reproducibility, Second-Party Verification, Automation, Microelectronics, Lab Bench

I. Introduction

Researchers typically design and perform experiments to verify or refute their hypotheses. The ability to repeat these experiments and obtain consistent results is vital to ensuring the results are valid and can be trusted. In many fields, these experiments require complex orchestration between many disparate pieces of laboratory equipment. This is particularly true in the Microelectronics domain. Manually running experiments introduces many opportunities for human errors. These errors may occur during configuration or execution of the experiment and may affect the current or future iterations of the experiment. For example, a researcher may easily forget to capture a last-minute adjustment to a piece of equipment in the experimental setup. Due to this omission, anyone attempting to repeat this experiment in the future may now obtain invalid results and potentially discredit the body of research. An automated platform that is capable of capturing the digital thread of an experiment can help reduce the opportunity for these human errors to be introduced in microelectronics experimentation. Furthermore, a platform that defines a portable format for the digital thread of a microelectronics experiment can facilitate collaboration between multiple parties by allowing them to easily share all information required to reproduce an experiment and independently verify the results. This paper presents such an automated platform, called Benches™, and describes how it can be used in this way.

II. Background

Experiments are commonly performed at various stages throughout the microelectronics device lifecycle, including at the initial design stage to prove out concepts and during verification and validation to ensure proper operation. Experimentation is especially important when investigating new concepts to determine if they are even feasible in the first place. One example of performing an experiment to demonstrate the feasibility of a concept was presented in [1], where a ring-oscillator based circuit was demonstrated as a functional trigger mechanism for a Hardware Trojan Horse.

Digital threads serve as the authoritative source of truth about a system [2] [3] and can help establish trust by providing evidence that claims are being met. These properties are especially useful in the assurance domain where a digital thread can be used to provide evidence that the requirements of a certification process are being met. Digital threads also have the potential to improve historical integrity of information by packaging all information related to an experiment together so that it can be retrieved later without being fragmented or lost. Ideally, a digital thread could also be used to automatically evaluate its physical counterpart to ensure the data captured in the digital thread matches the physical realization of the system.

III. Digital Threads in Microelectronics Labs

Digital threads in microelectronics labs are particularly well suited to fulfilling the ideal property of reproducibility while also facilitating collaboration among researchers. Experiments performed in microelectronics labs often involve many pieces of equipment that must power, stimulate, and observe a device under test. These pieces of equipment often provide interfaces that allow them to be controlled remotely and even automated. The communication that takes place over these interfaces during an experiment can be captured in a digital thread to store a record of the experiment. The data captured from this communication contains a wealth of information, including equipment configuration parameters, experiment procedures, and experimental measurements. Sharing a digital thread containing all these types of information, as illustrated in Figure 1, can facilitate collaboration by not only providing the raw measurements collected during an experiment, but also by including additional context about how the experiment was performed via the configuration parameters and experiment procedures. Additionally, the configuration parameters and experiment procedures captured from the equipment interfaces can enable experiments to be reproduced.

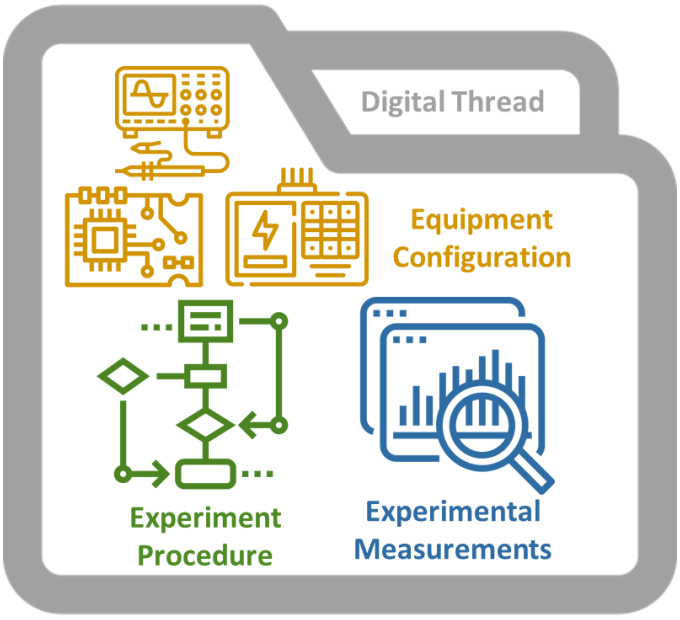

Figure 1. Contents of a digital thread for a microelectronics lab experiment (figure contains images from Flaticon.com)

A. Capturing Equipment Configuration

Each piece of equipment involved in an experiment requires its own precise configuration that should be applied and verified before the experiment proceeds. For example, the voltage output of a power supply should be specified to match the nominal input voltage of the device under test. Another configuration example may include the operating modes (e.g., frequency or pulse width) of all configured data acquisition instrument ports and a record of their physical connections to the device(s) under test. This information is vital to the proper operation of the experiment and must be included in the digital thread. Not only will this information ensure the proper operation of the experiment, but it will also assist users who wish to repeat experiments by documenting each piece of physical equipment used in a lab station, including the device under test, and the connections between them, which will be required when reconstructing the physical lab station.

B. Capturing Experiment Procedure

The experiment procedure describes the sequence of steps required to perform an experiment and details the complex interactions between each piece of equipment. The procedure should document any initialization steps (e.g., power sequences, bitstream programming, etc.), device stimuli steps (e.g., output waveform generator pattern), and device measurement steps (e.g., begin JTAG readback). This information defines the experiment and therefore must be included in the digital thread. Experiments become more complex when measurement and stimuli steps become intertwined, for example an experiment may require programming *bitstream A* when the operating temperature of the device under test drops below 80°C and programming *bitstream B* when the operating temperature exceeds this threshold. These types of feedback loops are also well suited for automated experiments.

C. Enabling Reproducible Results

Since a digital thread captures the configuration of all equipment in an experimental setup and the procedure of the experiment, it includes all the information necessary to repeat the experiment. Therefore, a digital thread for a well-defined experiment enables the experiment to be repeated and results to be reproduced. Of course, the caveat of a well-defined experiment is necessary since any reliance on any uncontrollable environmental conditions may hamper the ability of an experiment to provide reproducible results, with or without a digital thread.

D. Facilitating Collaboration

Storing the digital thread data in a portable format that can be easily shared between parties can facilitate collaboration. Not only can the information captured in a digital thread be used to repeat experiments, but also to provide additional context about procedure of an experiment for any researchers who are interested in analyzing the results without independently repeating the experiment.

IV. Benches™

We have developed a fully automated, web-based lab bench platform called Benches [1]. This platform enables engineers distributed across the country to interact with lab equipment hosted at one or more facilities and perform experiments. While OEM (original equipment manufacturer) solutions exist to interact with and automate the operation of individual pieces of equipment, experiments often require the use of multiple pieces of equipment. Using OEM solutions requires users to run a standalone vendor tool to interact with each piece of equipment, or alternatively, write a patchwork of scripts that each automate the operation of a single piece of equipment in isolation. Similarly, the data captured from equipment using the OEM tools is not consistent between tools and may be stored in proprietary formats. Conversely, Benches provides a unifying framework, including a graphical user interface, scripting support, and integrated interfaces for many types of equipment, that enables users to easily run complex experiments where multiple pieces of equipment are operating in unison.

A. Equipment Interfaces & Management

Benches includes a flexible interface architecture that enables interactions with a disparate collection of lab equipment. These user-definable equipment interfaces provide a means to operate equipment and collect and store data captured during an experiment. The Benches web user interface allows users to specify the available lab equipment (e.g., power supplies, data acquisition instruments, etc.) as well as devices under test. To run an experiment, a lab station is defined as a collection of equipment and a device under test. This provides two important characteristics. First, any experiment run on a lab station will be associated with a specific device under test, allowing users to analyze the behavior of a device across experiments. Second, it provides for a resource lock on the lab station to ensure experiments do not interfere with each other.

Figure 2 shows the lab station configuration dialog in Benches that allows a user to specify the device under test and collection of instrumentation equipment that belongs to a particular lab bench. When a user wants to run an experiment, they select an appropriate lab bench and are presented with the form shown in Figure 3. The lab station device under test is automatically associated with the experiment and the user can then provide a description for the experiment along with python code that is executed during the initialization of the lab station, a script for an automated experiment, and files to be used during the experiment. The files associated with an experiment could include FPGA bitstreams to configure the device under test, data to be fed to a device, or any other files that should be transferred to the device under test.

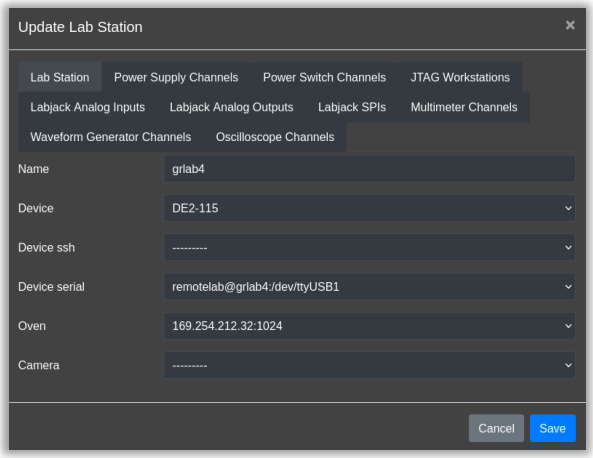

Figure 2. Lab station configuration dialog

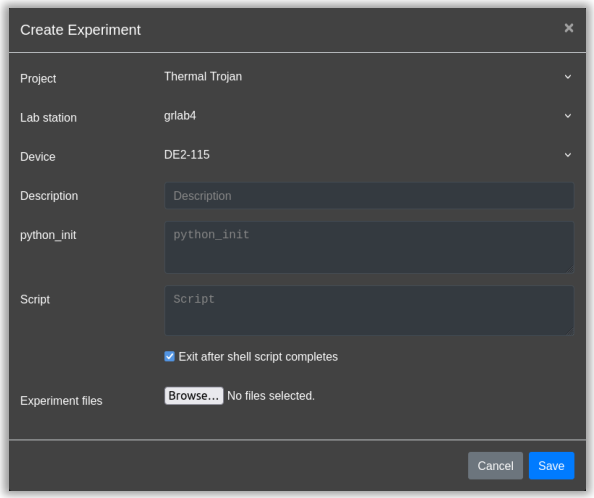

Figure 3. Experiment creation form

The Benches web user interface provides a shell interface, shown in the upper left quadrant of Figure 4, that can be used to run both interactive and scripted experiments. This shell interface includes commands to invoke functionality from the equipment interfaces. Python integration is included to enable advanced scripting capabilities, allowing users to define dynamic experiments that can perform operations in reaction to experimental data captured in real time.

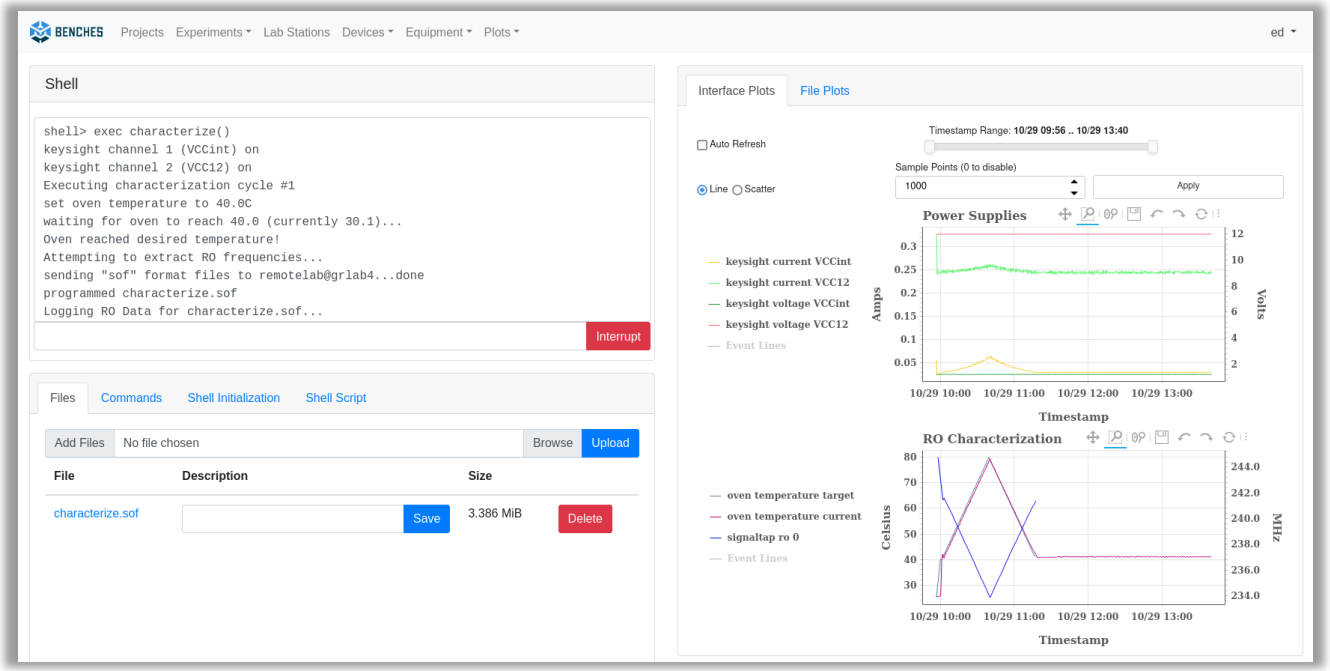

Figure 4. Experiment shell interface

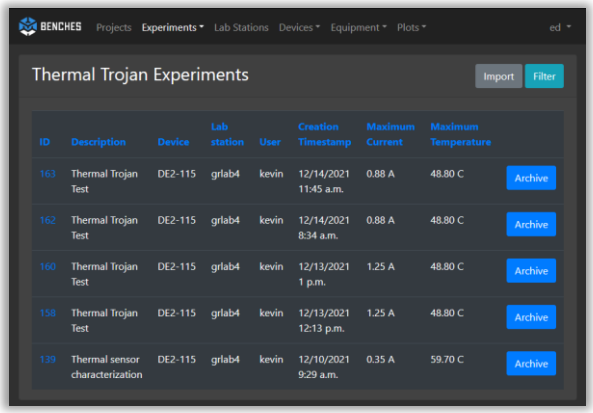

Figure 5. Experiment list

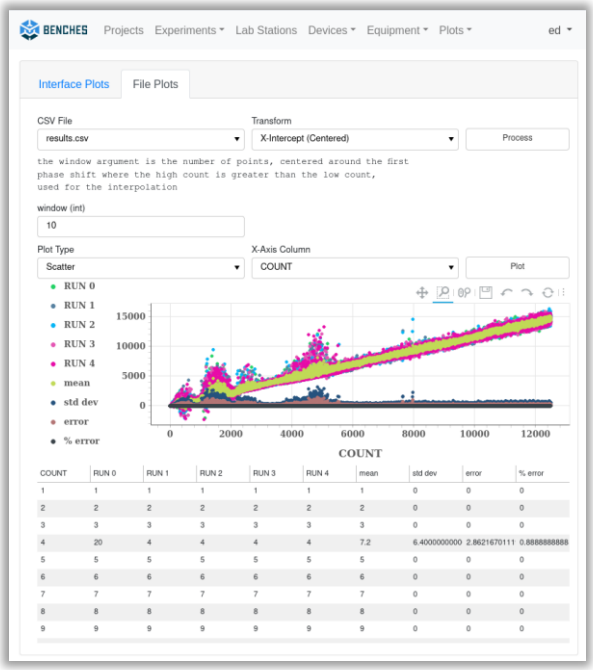

Figure 6. Data transformation interface

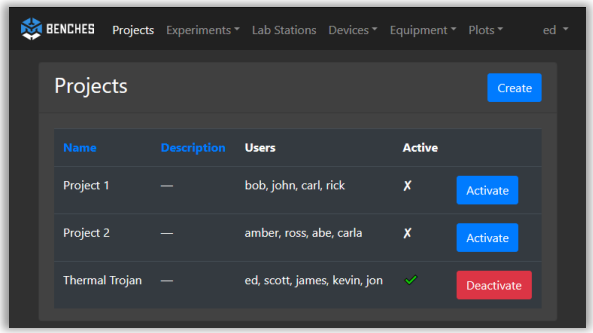

Figure 7. Project management interface

B. *Data Storage & Analysis*

Benches serves as a central data repository containing all the data captured during experiments, enabling engineers to perform analysis and draw conclusions about their experiments. The web user interface enables collaboration among distributed team members by allowing engineers to easily share results. Additionally, experiment results can be exported as an archive for further external analysis. An archive of an experiment contains the entire digital thread and includes the shell output, all the files associated with the experiment, all the data events (commands issued, measurements taken, etc.), the python initialization script, the shell script, and an html file that includes plots produced during the experiment.

Experiments within the Benches system are grouped together into "projects" for both organization of information and access control. Figure 5 shows a list of experiments performed in Benches for a particular research project. This interface provides various statistics to summarize experiments and allows users to view, modify, archive, or delete experiments. Only a user who created an experiment has permission to modify or delete it, otherwise users who have been assigned to the project can view, create, and archive experiments within the project.

Integrated analysis capabilities enable data visualization and analysis. Access to the data captured is not only available after an experiment has concluded, but also in real time during interactive experiments. Plots can be defined by users to include the data of interest. For example, a power plot can be defined to contain various voltage and current measurements captured by power supplies and other instrumentation. Python integration is included to enable advanced data transformation capabilities, as shown in Figure 6.

C. *Authentication and Authorization*

Benches provides security by default, requiring connections to the web interface to use HTTPS. Of course, security does not stop at traffic encryption, therefore Benches also enforces authentication and authorization principles. The web interface requires users to authenticate themselves and includes Lightweight Directory Access Protocol (LDAP) integration. Once logged in, a user must acquire permissions to access individual projects. This facilitates restricted access to experimental data by ensuring users can only view, create, modify, or delete experiments to which they have been assigned permission.

Figure 7 shows the project management interface in Benches, which allows an administrator to create projects and assign users to projects. An experiment in Benches is always associated with a project and only users assigned to a specific project are allowed to view or create experiments associated with that project. Additionally, equipment and devices under test can be associated with a project to ensure that only the users assigned to that project will have access to them.

V. Collaborating with Digital Threads in Benches™

Benches natively provides many features that enable digital threads to be automatically captured as experiments are performed. Since Benches provides interfaces to all the equipment involved in an experiment, all the equipment configuration and experiment procedure flows through Benches and is captured in real-time during both scripted and interactive experiments. This removes the possibility of any human errors preventing the experimental procedure from being properly captured.

Before users can run an experiment in Benches, they must first define a lab station. This definition captures the equipment configuration of a physical lab station and is included in the experiment digital thread. To define a lab station, users first describe the device under test including identifying information such as the device manufacturer, family, and serial number. Then users configure the equipment interfaces for each piece of equipment that exists at the physical lab station. These configurations may include power supply channel parameters, JTAG programming parameters, data acquisition instrument port parameters, etc. as well as labels that help identify both physical connections between equipment and the device under test as well as data measurements captured during experiments. Once an experiment begins, the configuration of the corresponding lab station will be used to initialize its digital thread with the equipment configuration. Since lab station configuration is already a part of the normal Benches workflow, users do not have to perform any additional steps to capture equipment configuration in the digital threads of their experiments.

Once users select an available lab station, they can begin running an experiment and Benches will automatically capture the experiment procedure in the digital thread without any additional action required by the user. For scripted experiments, the experiment procedure will consist of the experiment script and any input artifacts (such as FPGA bitstreams) that the user specified at experiment creation. For interactive experiments, the experiment procedure will consist of the commands entered by the user and will also include any required input files (such as FPGA bitstreams) that the user uploaded while running the experiment. If any actions in the experiment procedure include acquiring measurements, this data will also be automatically stored in the digital thread.

Experiments performed with Benches are reproducible since the digital threads captured for both scripted and interactive experiments contain the necessary equipment configuration and experiment procedure. Reproducing a scripted experiment in Benches from its digital thread simply requires importing the digital thread archive and re-executing the script (assuming a lab station exists that matches the configuration contained in the digital thread). Interactive experiments can be reproduced by assembling a script from the instructions that were previously issued by the user. However, it should be noted that, due to the nature of interactive experiments, they may not be reproduced to the same level of fidelity of scripted experiments since a user may have interactively issued commands due to some condition that was manually observed rather than programmatically handled (e.g., with an *if* statement).

While the digital thread of an experiment exists within the Benches central data repository, it can also be exported as an archive for portability. These digital thread archives include the equipment configuration, experiment procedure, and previously obtained experimental results. Benches facilitates collaboration by allowing users to import digital thread archives into other instances of Benches and either browse the included results or automatically re-run the experiment to reproduce the results and enable an independent verification. To further facilitate collaboration, the digital thread archives use non-proprietary file formats (e.g., tar, csv, and json) so that users receiving Benches digital thread archives do not require access to an instance of Benches to view the thread contents.

VI. Applications of Digital Threads in Benches™

The digital threads captured by Benches enable many real-world applications, this section will provide some examples of these applications. Benches can enable multidisciplinary teams from multiple institutions to collaborate on experiments. Using the web-based Benches user interface, users can remotely perform experiments from any of the team members' facilities or even when working from home. Similarly, the equipment used to perform the experiments can be located at one or more of the team members' facilities. This highly collaborative environment allows each team to contribute their unique expertise and advance the overall goals of the experiment. Consider an experiment focused on studying the effects of aging in FPGA devices where a team of FPGA firmware experts in one location collaborates with a team of physicists in another location to develop and analyze methods for artificially aging FPGA devices. Using Benches, the FPGA firmware experts can ensure their bitstreams operate as expected on the device under test and the physicists can use the bitstreams to run automated experiments that measure the effects of aging using various pieces of lab equipment orchestrated with Benches. This begins a feedback cycle, where the FPGA firmware experts have visibility into the practical usage of the bitstreams by the physicists and can either implement improvements in the bitstream based on their observations or provide suggestions to the physicists to improve their experiment. Similarly, the physicists have visibility into the FPGA firmware experts' bitstream tests and can provide feedback on the bitstream operation.

Another related application for the digital threads in Benches is a contract deliverable. Including the digital thread as a component of the deliverable can provide assurance that the deliverable functions as intended. Continuing the scenario described above, consider the FPGA firmware experts were contracted by the physicists to deliver an experiment that induced aging effects in an FPGA. If a Benches digital thread is a component of the deliverable it will include all the artifacts required to induce the aging effects (e.g., FPGA bitstream) and Benches can be used by the customer to automatically verify that the entire experiment operates as intended upon delivery by orchestrating the same equipment in their lab.

Commercial vendors can also use the digital threads in Benches to distribute reference procedures to their customers to demonstrate the capabilities of their platforms. Consider the ChipWhisperer platform, an open-source platform aimed at

performing side-channel power analysis and fault injection attacks. The vendor provides an application note [4] that describes how to perform a power analysis attack on an AES core implemented in an FPGA using one of their platforms. The document provides links to the required software and firmware, describes how to configure the hardware testbed, and walks users through the process of performing power analysis to recover the encryption key used in the FPGA testbed. Distributing these artifacts along with a scripted procedure for performing power analysis as a Benches digital thread could expedite the process of running the demo by increasing the level of automation and provide a more user-friendly experience.

A potentially broadly impactful application of Benches digital threads is in the area of research reproducibility. A recent IEEE Spectrum article highlighted that 60% of IEEE publications have no practices in place to ensure reproducibility [5]. The article highlighted the importance of understanding the processes used to generate scientific results as well as the ability to independently reproduce results, both key features of Benches digital threads. The digital threads produced by Benches, consisting of equipment configuration, experiment procedure, and experimental measurements, also align with the recommendations outlined by the National Academies of Sciences, Engineering, and Medicine in [6] to support reproducibility in scientific and engineering research. To help others reproduce their work and confirm their findings, researchers could distribute the Benches digital threads of their experiments alongside their research publications in open repositories as suggested in [6].

VII. Conclusion

We have demonstrated how Benches can facilitate collaboration through digital threads via portable experiment archives and described how Benches automates both the creation of digital threads and the reproduction of experimental results. The benefits of capturing microelectronics experiment digital threads include increased confidence in using the results as part of trust and assurance claims. Namely that trust can be established by leveraging a digital thread as an authoritative source of truth since it contains all the information necessary to reproduce an experiment. Reproducibility is also important for establishing assurance because it enables the independent analysis necessary for second-party verification.

References

[1] E. Carlisle, S. Harper, J. Koiner, K. Paar, M. Capone, J. Graf, "Automated Analysis of a Thermally Triggered FPGA Hardware Trojan," 2022 GOMACTech Conf., March 21-24, 2022.

[2] DOE Digital Innovation Center of Excellence, Digital Thread Pillar, https://dice.inl.gov/digital-thread [Accessed January 10, 2023]

[3] E. Kraft, "Digital Engineering Application to Developmental Test & Evaluation," NDIA Air Force Digital Thread/Digital Twin Workshop, December 13, 2016, https://www.ndia.org/-/media/sites/ndia/meetings-and-events/2016/december/air-force-workshop-december-13/ndia-saf-aq-oti-dt-workshop-dec-2016-for-website.pdf [Accessed January 10, 2023]

[4] A. Dewar, J. Thibault, C. O'Flynn, "NAEAN0010: Power Analysis on FPGA Implementation of AES Using CW305 & ChipWhisperer®," October 29, 2020, http://media.newae.com/appnotes/NAE0010_Whitepaper_CW305_AES_SCA_Attack.pdf [Accessed January 10, 2023]

[5] J. Goodrich, "Study Shows Ensuring Reproducibility in Research Is Needed," IEEE Spectrum, September 30, 2021, https://spectrum.ieee.org/study-shows-ensuring-reproducibility-in-research-is-needed [Accessed January 10, 2023]

[6] National Academies of Sciences, Engineering, and Medicine, "Reproducibility and Replicability in Science," 2019, http://nap.nationalacademies.org/25303 [Accessed January 10, 2023]