NIST Special Publication 1278

5G Hardware Supply Chain Security Through Physical Measurements

James C. Booth
Marla L. Dowell
Ari D. Feldman
Paul D. Hale
Melissa M. Midzor
Nathan D. Orloff
authors in alphabetical order

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.1278

National Institute of Standards and Technology
U.S. Department of Commerce

NIST Special Publication 1278

5G Hardware Supply Chain Security Through Physical Measurements

James C. Booth
Marla L. Dowell
Ari D. Feldman
Paul D. Hale
Melissa M. Midzor
Nathan D. Orloff
authors in alphabetical order

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.1278

May 2022

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Undersecretary of Commerce for Standards and Technology

National Institute of Standards and Technology Special Publication 1278
Natl. Inst. Stand. Technol. Spec. Publ. 1278, 75 pages (May 2022)
CODEN: NSPUE2

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1278

Executive summary

"5G" is the collection of fifth-generation telecommunication specifications as detailed by the 3rd generation partnership project (3GPP). 5G is different from previous communications technologies because it enables higher data rates and lower latency while increasing reliability. In some cases, these improvements are more than an order of magnitude better than previous generations of cellular technology. This leap in technology will have transformative impacts on the U.S. economy by making artificial intelligence, augmented reality, industrial automation, massive device to device communications, and other unprecedented technologies commonplace in our everyday lives, in both personal and business applications.

This transformation also presents new vulnerabilities in our communications infrastructure through attacks on system hardware, including integrated circuits, passive components (resistors, capacitors, inductors), and printed circuit boards. Hardware vulnerabilities can include:

- insertion of malicious features during design,
- alteration of system behavior through illicit access points that exist due to hardware design weaknesses or architectural flaws,
- extraction of sensitive or secret information through unintended communications (side) channels,
- stolen intellectual property through reverse engineering,
- counterfeit, including recycled, cloned or remarked components or systems represented as genuine,
- modification to insert hidden functionality.

Hardware security has been known to be a problem for some time and many mitigation strategies are being developed. No single approach will solve the problem, but new methods could augment or improve upon existing methods.

In this report, we focus on quantifiable physical measurements to verify the authenticity of hardware and to detect modifications from the manufacturer's intended design that might change the functionality or reliability of the hardware. Maliciously modified hardware provides a means to bypass traditional software and cryptographic-based protections, allowing a malicious actor to control or manipulate system software, turn the system off, cause system failure, or allow access to sensitive information. Counterfeit devices, including recycled, cloned, and remarked devices, generally have unknown quality or long-term reliability and are thus less trustworthy[1]. Hardware compromises can be difficult to detect and, when detected, are often only corrected by expensive equipment replacement.

We intend that this report complement other security efforts and inform the development of standardized physical measurement and data-driven approaches for electronics hardware security, particularly hardware for 5G communications. In this report, we distill a series of interviews, a workshop[2], and literature review into four themes that arose repeatedly as barriers to further application of physical measurements to hardware security. Then, based on the

[1] Recycled components are parts that have been extracted from used or defective circuit boards. Cloned components are non-conforming, but functionally equivalent parts, manufactured illegally outside the original component manufacturer's (OCM's) supply chain, potentially through intellectual property (IP) theft. Remarked parts are often sold as a completely different component of the same form factor.
[2] "Securing the 5G Supply Chain through Measurement" virtual workshop, held May 18-19, 2021.

workshop input, interviews, and literature reviews we make actionable recommendations to overcome these barriers. These themes and related recommendations are summarized in Table 1 and described in detail in Section 3.

Table 1. Summary of themes and recommendations for implementing a measurement-based hardware security strategy. The section number refers to the report section where this information is described in more detail.

Section	Primary theme	Recommendation
3.1	Securing a complex, dynamic 5G supply chain requires multiple approaches agreed upon by stakeholders at each link in the supply chain.	Coordinate industry-led international consensus building activities through international industry standards and national metrology institutes.
3.2	Physical measurements could inform security risk assessments, but they are difficult to quantitatively evaluate.	Develop standard test articles for evaluating and benchmarking measurement performance. Standardize test methods and analysis practices to promote measurement reproducibility between different organizations.
3.3	Deployment of physical tests must address the needs of manufacturers and end-users for specific application spaces.	Evaluate deployment issues for specific manufacturing environments and use cases to enable user cost-benefit analysis of measurement-based and other hardware security approaches.
3.4	Industry needs a way to exchange and add measurement data to provenance while maintaining confidentiality.	Explore use or extension of data sharing frameworks being developed for other industry segments.

Keywords
5G; hardware security; measurement; microelectronics, supply chain; telecommunications.

Contents

List of Tables

List of Figures

1. Introduction

1.1 Background: Electronic hardware vulnerabilities

Information and data security have been of paramount importance since the beginning of electronic information and communications technologies (ICT), including network security, software security, and hardware security. While hardware might have been seen in the past as trusted, continuing trends in hardware design, hardware manufacturing, and the global supply chain have led to increased concern with hardware security. In the current environment, hardware vulnerabilities exist at all points in the system life cycle, including design, development, manufacturing, testing, acquisition, distribution, deployment, maintenance, and disposal [1–6]. Hardware vulnerabilities can include:

- Intentional and unintentional insertion of vulnerabilities during design[7, 8],
- alteration of system behavior through illicit access points that exist due to hardware design weaknesses or architectural flaws[9],
- extraction of sensitive or secret information through unintended communications (side) channels [10, 11],
- stolen intellectual property through reverse engineering [12],
- counterfeit, recycled, cloned or remarked components or systems represented as genuine [4],
- modification to insert hidden (trojan) functionality [6].

Hardware attacks can happen at the integrated circuit level, printed circuit level, or system level. Hardware compromises can be difficult to detect and, when suspected, are often only corrected by expensive equipment replacement [13]. In this report, we focus on quantifiable physical measurements to detect counterfeit devices and modifications from the manufacturer's intended design that might change the functionality or reliability of the hardware.

There are many different types of counterfeit devices. Recycled components are parts that have been extracted from used or defective circuit boards. Cloned components are non-conforming, but functionally equivalent parts, manufactured illegally outside the original component manufacturer's (OCM's) supply chain, potentially through intellectual property (IP) theft. Remarked parts are often sold as a completely different component of the same form factor. Counterfeit devices generally have unknown quality and long-term reliability and are thus less trustworthy [4]. As counterfeit devices affect many industrial sectors, including computers, communications, automotive electronics, and military systems, the consequences of system failure due to low-quality components can impact safety, reliability of infrastructure, and national security.

The existence of counterfeit electronic components at all levels, from simple capacitors, diodes, and transistors to integrated circuits, assemblies [14], and fully assembled equipment, such as network interface modules [15], network routers, automotive control assemblies [16, 17], cell phones [18, 19], is well documented. According to [1], legitimate electronics manufacturers lose about $100B/yr globally because of counterfeiting. Counterfeiters are well financed, and their tools and techniques are constantly becoming more sophisticated [20]. In turn, new, more sophisticated methods for counterfeit detection may be called for.

Hardware that has been modified with a hidden functionality, unknown to the user (sometimes called a hardware trojan) can provide a means to bypass traditional software and cryptographic-based defenses, allowing a malicious actor to control or manipulate system software, turn the system off, cause system failure, or allow access to sensitive information [21]. Hidden functionality can also be introduced unintentionally in the design process and then exploited by a malicious actor.

Hidden functionality can take on many forms and can happen anywhere in the value chain. In the design stage, "back door" or "kill switch" capability might be included in microcircuits, as alleged in [21], so that an unknown antagonist might disrupt the circuit's function. Trojans might be inserted in printed circuit boards, and many academic demonstrations, as well as alleged real-world examples are listed in [6]. ICT equipment can be intercepted and modified in transit between the manufacturer and the end user. As an example, Soviet Russia intercepted electric typewriters shipped to the U.S. embassy in Moscow in the early 1980s. The Soviets added the capability to log and transmit keystrokes, allowing them to copy every document typed on the altered typewriters [22].

Although it is difficult to find specific and unclassified examples of maliciously modified hardware in the defense or private sectors, Table 1 in [5] presents a non-exhaustive list of ten reports between 2010 and 2017 documenting examples of counterfeits and malicious insertions in the U.S. supply chain, to which we add three more between 2005 and 2018 [2, 22, 23]. In that same time, the U.S. government has spent enormously on programs such as the DoD trusted foundry program [24], the Joint Federated Assurance Center (JFAC) [25], and numerous DARPA programs, to protect national defense systems from adversaries who seek to exploit vulnerabilities due to intentionally implanted logic in hardware and software or unintentional vulnerabilities that are maliciously exploited [26, 27].

1.2 The need for 5G hardware security

5G communications network hardware, cell phones, and IoT devices pose a new set of attack surfaces [28]. The 5G communications standard has been considered "transformational" [29]

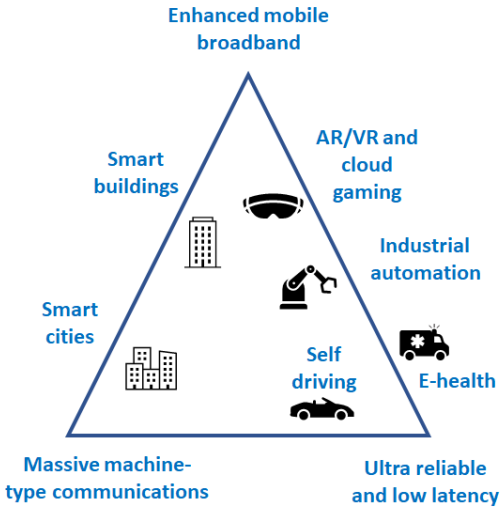

Figure 1. Visualization of the proposed application spaces of 5G communication systems.

because it enables fast, reliable, secure, and ubiquitous connections in ways that previous communications technologies could not. As an example, 5G enables the network provider to create multiple "slices" [30], each optimized to carry a wide range of use cases (see Fig. 1), trading off high data rates, large numbers of devices in ultra-dense environments, high mobility, high reliability, and low latency [31–33]. This new flexibility has led to and will continue to lead to, an interconnected network of devices dependent on 5G technology that was simply not possible before. Examples include self-driving vehicles, wireless video gaming with 3D graphics, robotic telemedicine, smart manufacturing with wireless coordination between robots, and smart buildings and cities with massive numbers and types of wirelessly connected sensors and other IoT devices. These new and diverse applications of 5G and technologies beyond 5G (5G+) in the commercial, defense, public infrastructure, and public safety sectors could make 5G+ communications networks, and their constituent components a desirable target for malicious actors [34].

The need for 5G security has been known since the beginning of its development [35, 36]. In response, government agencies have been developing strategic initiatives [37] and guidelines for secure 5G deployment [38, 39]. To the best of our knowledge, public programs targeted specifically at counterfeit or maliciously modified 5G hardware are focusing on prevention, rather than detection, see Section 1.6.5.

1.3 Purpose of this report

This special report summarizes the "Securing the 5G Supply Chain Workshop" held by the National Institute of Standards and Technology (NIST) from May 18th to May 19th in 2021, and the interviews and literature review, conducted by the authors, before and after the workshop. The purpose of the research was to:

- Understand what physical measurements are already being used by the electronics industry, especially for 5G+ hardware, to detect malicious and counterfeit hardware.
- Capture different stakeholder perspectives on how measurement-based countermeasures might mitigate threats, vulnerabilities, and risks inherent in complex 5G+ hardware, and how measurement-based security procedures might complement or enhance a provenance-based security strategy.
- Provide a broad overview of state-of-the-art (SOTA) methods for, and research on, measurements for validating the authenticity of 5G+ hardware.
- Explore barriers and stakeholder attitudes around development and adoption of measurements and measurements-based standards targeted at validating authenticity and detecting counterfeit or modified 5G+ hardware.

1.4 Intended audience

The intended audiences for this report are:

1) Technical researchers' who wish to align their research programs to government and industry needs.

2) Industry leaders and stakeholders who need to ensure 5G hardware security and want to understand the problem space.

3) Technical science advisors needing to inform science and technology policy in the United States.

Each audience has a unique point of view, and a need to understand how measurements can inform their decision-making.

The first group includes government researchers, academics, and industrial measurements scientists seeking new measurement opportunities. NIST researchers were an important part of this target audience and sought to help identify what, if any, critical measurement solutions and/or standards could help facilitate economic security and fair commerce.

While first group is the primary source for the development of measurement science solutions, the second group must make security decisions that can impact their business or their ability to do business. The second group includes leaders in research and development, security professionals, and manufacturers. Industry leaders strive to understand the problem space of 5G hardware security, how vulnerabilities in this space might impact commerce, and how best to support the needs of the first group. This second group is a critical NIST stakeholder.

The third group includes science advisors that could benefit from a high-level summary of the 5G security field to advise both public and private policy. It is one of NIST's roles to gather data and build information products to support policy and decision-makers.

NIST has a unique responsibility to define measurement methodologies and standards to compare different measurement modalities. This role is technology agnostic and helps to establish a neutral source of data for decision making. We intend that the findings and suggestions in this report augment other hardware supply chain security efforts, such as [38, 40–43] and those referenced in the next sections.

1.5 Traditional hardware security strategies

Traditional hardware security strategies start with a risk assessment, such as that described in [40]. Risks are addressed with a quality control system such as ISO/IEC9001 [44], which documents a counterfeit part control plan, including processes used for procurement, risk identification, mitigation, detection, avoidance, disposition, and reporting of suspected counterfeit parts [45–49]. The plan starts with avoidance of counterfeit and malicious devices by procurement through authorized sources, including the OCM, their authorized suppliers, and suppliers that obtain parts exclusively from the OCM or their authorized suppliers [45, 50]. Some industries call for a bill of materials (BoM) [51] or materials traceability [52]. Manufacturers that are subject to DFARS 252.246-7007 [46] are required to screen potential component vendors through the Government-industry data exchange program (GIDEP) [53] and also report suspected counterfeit electronic parts. Similar databases, such as ERAI [54], are available internationally.

If authorized sources are not available, or if higher level quality is required, established industry standards and processes for counterfeit prevention (including inspection, testing, and authentication) are employed. Inspection, often through an SAE or IDEA accredited laboratory, can include visual inspection of shipping packaging and electronic package [55, 56], imaging of the electronic package through scanning electron microscopy [55, 56], delid/ decapsulation followed by visual inspection of the inside of the electronic package through high magnification [56, 57], and imaging of the x-ray radiographic imaging of the part [56, 58]. These standard practices are focused on integrated circuits and do not extend to printed circuit boards or systems (although an assembly standard is in development [59]).

Decapsulation and delidding are destructive practices, as can be x-ray radiography [60] and are therefore only suitable for assessing small (random) samples of the incoming parts.

Testing can include electrical functional and parametric test [61], chemical analysis [62–65], and scanning acoustic microscopy [66]. Testing for resurfaced packaging might also be conducted [55]. This destructive test entails checking the resistance of part markings to solvents and/or abrasion, followed by visual reexamination with magnification.

Destructive integrated circuit (IC) delayering methods are the most accurate, time consuming, and costly inspection methods, but yield the highest level of assurance that the device is authentic [67]. Scanning electron microscopy (SEM) images, alternated with delayering, reveal the device's physical layout at each level, including vias and metal layers that form the physical structure of the IC. The practices related to this type of analysis are highly complex and often require significant specialized experience to yield meaningful results [68–70].

Some organizations question the effectiveness of the above inspection methods [60] "…SIA member companies have numerous examples where third-party laboratories reportedly using these standards have made incorrect authenticity determinations. Moreover, these standards are generally ineffective for identifying the latest forms of counterfeiting. For example, counterfeits where used, low-grade, or second-source die are assembled in new packages and are marked as higher-grade components would likely escape detection." The document goes on to argue that even "authentic" parts that are not supplied through an authorized distributor may be improperly handled or stored[3], possibly degrading the device. Many of the standard procedures cited above have been updated since the publication of [60] and it is unknown to us if these newer standards adequately address the charges outlined there. Furthermore, the above methods are specifically targeted at remarked and cloned counterfeit ICs and are not designed to detect counterfeit or modified assemblies, printed circuit boards, or assembled systems.

1.6 Emerging counterfeit detection and avoidance methods

Because of the continued prevalence of counterfeit devices in the supply chain [14], methods for detection and avoidance of counterfeit and modified hardware continue to be proposed in academia, industry, and the government. This work is too numerous and is evolving too quickly for all the different methods to be described here. The interested reader should consult the proceedings of the several conferences in this area (*e.g.*, [72–76]) and the textbook [77] for further technical information. Here, we summarize some emerging physical inspection and measurement techniques and a counterfeit avoidance method (physical unclonable functions, (PUFs)) used in the electronics industry. This summary will serve as background and motivation for the themes of Section 3.

It should be pointed out that the specific inspections and measurements performed by any manufacturer are closely held secrets. The DFARS regulations [46, 50] cited in the previous section only apply to certain government procurements requiring heightened levels of quality and do not apply when procuring commercial products and services using part 12 [78, 79]. It

[3] It is unknown to the authors if the revised standard [71] on procedures for long-term storage was released as a response to this concern.

is unknown to the authors if any of the methods outlined in sections 1.5 and 1.6 are utilized by the communications industry.

1.6.1 Machine vision and x-ray tomography

Visual inspection can be enhanced by machine vision systems [80, 81], although issues with lighting remain. Simple visual inspection is inadequate for modern multi-layer printed circuit boards and 3D integration. X-ray tomography [80, 82, 83] or terahertz imaging [84] may offer a solution.

1.6.2 Fingerprints, identifiers, and classifiers

Fingerprint features, more technically known as identifiers and classifiers, are repeatable unit-to-unit imperfections in the behavior of electrical circuits or systems. These imperfections are typically small and arise from circuit nonlinearities and random manufacturing variations and are intrinsic to the device and the manufacturing process. Fingerprint features may also be referred to as second order effects, signatures, or analog physically unclonable features.

Fingerprint features might be the variations in the intentional function of a circuit, such as small variations in the conducted electrical signal in the circuit or in the in-band radiated signal from a radio transmitter. The unintentional or side channel behaviors of a device might also be used as a fingerprint, and might include variations in the circuit's bias current, emitted sound, or electromagnetic radiation in the RF, visible, or infrared regions of the spectrum.

In some cases, measurements of fingerprint features, along with a decision rule, can, be used to identify different devices, or detect packaging modifications or device degradation due to age, wear, and damage. To be precise, measurements quantify variations of some physical property $\mathscr{P}$ of a device. There are some very fundamental criteria that $\mathscr{P}$ must meet to be useful for classification of the device into two groups, *e.g.*, modified and unmodified, or defective and meeting specifications [85]:

1. *Universality*: Every circuit under consideration must have the property $\mathscr{P}$ that is used for classification.
2. *Collectability*: The value of $\mathscr{P}$ can be measured quantitatively and non-destructively.
3. *Permanence*: The value of $\mathscr{P}$ is either invariant or has a known dependence over time and environmental conditions.

For $\mathscr{P}$ to be useful to uniquely identify an individual device, the additional criterion is needed:

4. *Uniqueness*: No two devices have the same value of $\mathscr{P}$.

To be practical, the measurement process and decision rule must meet further criteria:

5. *Distinguishability:* Measurement uncertainty in the value of $\mathscr{P}$ from systematic effects and noise must be small enough to draw statistically significant conclusions.
6. *Reproducibility:* The measurement conditions, procedure, and analysis must be sufficiently specified such that the identifier or classifier results can be reproduced at different laboratories.

There are many different types of identifiers and classifiers of circuits and systems reported in the literature. As mentioned above, many different physical phenomena can be measured, with or without stimulus, and a wide range of statistical and machine learning tools can be employed for the decision rule.

RF fingerprints, the small variation in intended RF emissions in a communications system, have been researched for more than two decades to distinguish authorized users from unauthorized users (spoof attacks) in wireless networks [86–94] and were recently the topic of the first phase in the DARPA Radio Frequency Machine Learning Systems (RFMLS) program [95]. There are many analog imperfections in RF transmitters that can be leveraged, individually or together, as identifiers, including phase noise, digital to analog converters (DACs), bandpass filters, frequency mixers, and power amplifiers [93]. The dynamic over-the-air behavior of 5G+ transmitters with multi-element antenna arrays might be leveraged as identifiers, such as beam pattern, signal to noise ratio, and waveform distortion as a function of beam sweep azimuth [96]. In some applications, fingerprint features might be intentionally enhanced, see *e.g.* [97, 98]. While much research has focused on the effects of both wireless channel and co-channel interference on the effectiveness of RF fingerprints for mitigating spoof attacks on wireless networks [91, 92, 99, 100], it is plausible that in a hardware security application these effects could be greatly reduced by measuring the electromagnetic emissions in an anechoic chamber [101, 102].

Other features that might be leveraged for fingerprinting electronic devices are numerous. Cell phones have embedded hardware, beyond the wireless devices, that also have nonlinearity and manufacturing imperfections that might be leveraged as identifiers, including the audio system digital to analog converter (DAC) and the analog to digital converter (ADC) and the camera sensor array [85]. Other possible fingerprint features include IoT network behavior [103], power supply current in both integrated circuits and fully integrated IoT devices [104–106], and thermal behavior [107].

1.6.2.1 Fingerprints for supply chain security

Fingerprints might be leveraged for authenticating various electronic components and systems as being the supplier's intended system, no more, no less. For example, the radiated emissions of user equipment (UE) might be measured at the system integrator's facility by use of a standardized method (ensuring reproducibility). The results of the measurement could be uploaded to a database. The device is then delivered to an end user who makes the same standardized measurements and compares the results with the database to identify the device as the same one produced by the integrator [108, 109]. In less demanding applications, the measurements at the end user could be used to categorize the incoming component as being the same as intended by the manufacturer or just the same as other components in a received batch. In the latter case, a reference measurement at the manufacturer would not be needed.

1.6.2.2 Fingerprints: state of the art

It was pointed out in [110] that at least 10 different systems leveraging fingerprints/second order effects are under commercial development. These systems make use of a varied set of

collected signals, stimulus, data analysis, and decision rules. However, in a recent study [111–113] the U. S. Air Force Research Lab (AFRL) tested the performance of five of these pre-commercial systems when detecting modifications of an in-house designed 128 bit AES core, fabricated in Global Foundry's 8HP SiGe BiCMOS process. A baseline design with five variants were tested, with the variants designed to be detectable with the specific second order modalities used by the measurement systems. Experiments were conducted to characterize the variability of the systems and blind measurements of the six different designs were made. In short, the measurements from all five systems failed to detect the different circuit variants at a statistically significant level.

The principal report [111] summarized the state of the industry by stating (approved for public release, APRS-RY-22-0197) "The analysis shows an overall trend of maturing hardware without equally mature calibration techniques, demonstrated repeatable measurements, utility in relevant environments, and analysis algorithms. Vendors have moved from the breadboard and prototype stage toward production level hardware but have not adequately demonstrated functionality for use in an operational environment." Although the results of the study were generally negative, the authors felt that the study was useful, "The lessons learned… will serve to help guide future research directions and test strategies" with the goal to "utilize multiple modalities to non-destructively screen devices, with each … modality covering gaps of the others, enabling a comprehensive screening routine, ending in a risk-based device disposition."

The AFRL report goes on to list three research milestones that are echoed in the themes of this report (approved for public release, APRS-RY-22-0197):

1. "...on the hardware side, either measurement equipment may be required to be enhanced to measure subtle changes at the device level, or the magnitude of change required to stand out from the noise of the measurement uncertainty sources needs to be better understood. …the beginning step requires establishing calibration approaches, or the ability to de-embed the measurement device from the fixtures used in the measurement. Having these improvements in place not only improves data quality, but also enables a systematic test strategy that can characterize absolute differences in devices, not just relative differences based on potentially time dependent measurements (impact of drift)."
2. "…on the analytics side, the emphasis needs to fall on understanding the impact of uncertainty on final classification and/or clustering results. Machine learning techniques are excellent in identifying patterns or subtle differences in data sets, but we must understand the data well enough to know whether those patterns stem form uncertainty or a meaningful result. Furthermore, in developing this understanding, measured features that are known to be driven by uncertainty sources can be minimized in the decision process, placing more emphasis on those features directly connected to the measured difference. In establishing these practices, it enhances dataset quality used in the risk-based decisions associated with aggregating results across a multimodal measurement space for either legacy devices or devices with designed in features."

3. "…there needs to be an emphasis on the incorporation and improvement of modeling and simulation techniques. This imperative allows for a more strongly correlated connection between known differences in measured devices and the changes in measured responses. Furthermore, being able to model device changes and accurately predict responses enables more informed machine learning practices, and a design feedback loop where [second order effect] features can be enhanced."

1.6.3 Advanced inspection and testing methods

Further inspection-based standards continue to be developed and the SAE is a leader in this area. Standards listed at the SAE web site on Feb. 8, 2022, as "work in progress" include:

- "Techniques for suspect/counterfeit EEE parts detection of capacitors by acoustic microscopy (AM) test methods"[114],
- "Technique for suspect/counterfeit EEE parts detection by secondary ion mass spectrometry (SIMS) test method" [115],
- "Techniques for suspect/counterfeit EEE parts detection by radiated electromagnetic emission (REME) analysis test methods" [116],
- "Techniques for suspect/counterfeit EEE parts detection by netlist assurance test methods" [117],
- "Technique for suspect/counterfeit EEE parts detection by laser scanning microscopy and confocal laser scanning microscopy (CLSM) test methods" [118],
- "Techniques for suspect/counterfeit EEE parts detection by thermomechanical analysis (TMA) test methods" [119],
- "Techniques for suspect counterfeit EEE parts detection by Auger electron spectroscopy (AES) test method" [120],
- "Techniques for suspect/counterfeit EEE parts detection by x-ray photoelectron spectroscopy (XPS) test method" [121],
- "Techniques for suspect/counterfeit EEE parts detection by gas chromatography/mass spectrometry (GC/MS) test methods" [122],
- "Technique for suspect/counterfeit EEE parts detection by scanning electron microscopy (SEM) including energy dispersive x-ray spectroscopy test methods" [123],
- "Techniques for suspect/counterfeit EEE assembly detection by various test methods" [59]
- "Counterfeit and substandard battery risk mitigation" [124]

1.6.4 Physically unclonable functions

Physically unclonable functions or features (PUFs) leverage random manufacturing variations and nonlinearities to derive an immutable device identifier [125–129] and can be used for detecting and avoiding counterfeits. We distinguish PUFs from fingerprints in that PUFs are intentionally added to a circuit to leverage the randomness in a manufacturing process to engineer a random, but repeatable, behavior. Fingerprints are unintentional and based on intrinsic variation away from a nominal behavior.

Generically, PUFs can be used in two different ways. In the first, the PUF is used as a marker that is difficult to replicate (clone), examples of which include Deoxyribonucleic acid (DNA), or a large quantity of nanoparticles scattered on the marked device [127, 128]. The

general strategy here is like that used for identifiers in the above section. The markers are scattered onto the device and a measurement is taken. The measurement is uploaded to a database. At the next link in the supply chain, a similar measurement is performed and compared with the database to confirm the identity of the device. Different methods have differing advantages and disadvantages, some of which are reviewed in [127].

The second type of PUFs use digital circuits. Implementations, applications, and potential weaknesses of digital PUFs are reviewed in [125, 126, 129]. One standard use of a digital PUF is to authenticate the chip through a challenge-response approach. PUFs can also be used to generate encryption keys. As pointed out in [129, 130], some PUFs are vulnerable to machine learning attacks through repeatedly providing challenges to the PUF and using the obtained set of challenge-response pairs to train a machine learning algorithm. Finding PUF implementations that are less vulnerable to this kind of attack is an ongoing area of research [131]. One advantage of a digital PUF is that it can be integrated within a chip that needs to be authenticated, and thus cannot be separated from the chip.

As PUFs are more of an identification tag, rather than a physical measurement-based approach to security, further discussion PUFs is beyond the scope of this document.

1.6.5 5G hardware security standards

Here we list various efforts for related to 5G hardware security, with descriptions from their standard documents or web sites.

NCCoE: The National Cyber Security Center of Excellence (NCCoE) brings together experts from industry, government, and academia to develop example implementations addressing specific security needs of complex IT systems and the nation's critical infrastructure [132], including mobile computing [38], 5G [39, 133], and supply chain assurance [41–43].

GSMA: The objective of the GSMA Network Equipment Security Assurance Scheme (NESAS) standards [134–137] is to provide an industry-wide baseline security assurance framework to facilitate improvements in security levels across the whole industry. NESAS defines security requirements and an assessment framework for secure product development and product lifecycle processes, as well as security test cases (from [138, 139]) for the security evaluation of network equipment. One of the motivations for developing NESAS is that the scheme will help vendors and operators avert fragmented regulatory security requirements (from [134]). GSMA hosts the Coordinated Vulnerability Disclosure (CVD) program, which gives security researchers a route to disclose a vulnerability impacting the mobile ecosystem, meaning that the impact can be mitigated before it enters the public domain [140].

ATIS: The ATIS 5G Supply Chain Working Group was launched at the request of the Department of Defense (DoD) in consultation with other government agencies. The goal is to extend the development of 5G best practices and guidelines for the purpose of creating supply chain standards that can be operationalized in the public and private sectors.

Among other things, the 5G Supply Chain Working Group is working to establish a common assurance framework for trusted 5G networks; develop or identify standards to be applied to 5G systems; and evaluate audit/certification options for ICT solution providers, infrastructure

and endpoint device original equipment manufacturers. These objectives are intended to address end-to-end ICT supply chain visibility, coordination of existing supply chain management best practices, industry alignment with federal guidelines, improved threat monitoring tools and a method to influence national/international standards development (from [51]). As of April 19, 2022, the document "ATIS standard for a 5G Network Assured Supply Chain" was still in draft form.

CTIA Certification™: CTIA develops test procedures for verifying wireless standards compliance and certifies testing laboratories to conduct those tests. Topic areas include [141]:

- battery compliance to IEEE 1725 and IEEE1625
- battery life
- device hardware reliability
- interoperability
- over-the-air performance
- speech performance.

CTIA Certification also maintains a reverse logistics and service quality (RLSQ) program to establish standards for non-consumer-facing aftercare of wireless devices for the repair, refurbishment, and remanufacturing of wireless devices.

TIA: SCS 9001 provides guidance for key components of supply chain security [142]:

- Secure software development
- Validation methods for ensuring software identification and source traceability
- Product security
- Governmental requirements on source of origin and transparency of internal controls

1.7 Need for measurements

Current hardware security approaches across the supply chain generally use provenance-based approaches or post-exploit diagnostics to harden hardware security from future attacks. Other forms of hardware security include documentary standards or advanced labeling. Measurement-based approaches can augment current approaches to hardware security by attaching measurement data to a product, as either a unique stand-alone measurement-based profile or a common thread or identifier throughout a supply chain. Measurement data offers some unique advantages over conventional approaches to hardware security:

- offer parallel or independent methods for identification that cannot be separated from the product (example: provenance records can be lost, misdirected, or tampered with),
- providing additional methods to identify counterfeit or altered units (unique physical qualities)
- enabling quantification of risk linked to measured elements rather than relying on qualitative methods.

In addition to the potential value of improving 5G hardware security, measurement-based approaches could also enable innovation, for example, by connecting measurement data

Table 2. NIST 5G+ hardware supply chain working group

Name	Expertise/contribution
Paul D. Hale	Waveform metrology
Melissa Midzor	Spectrum sharing & coexistence
James C. Booth	Radio frequency electronics
Ari Feldman	High-speed measurements, materials
Jason Coder	Spectrum sharing and wireless test
Nathan D. Orloff	Microwave materials
Dylan Williams	High-speed electronics
Kate Remley	Wireless systems test
Joseph Kopanski	Nanoscale characterization
Yaw Obeng	Semiconductor manufacturing
Theodore Heilweil	Terahertz measurements
Chris Carson	Meeting planning
Alexandra Esquibel	Outreach and video conference support
Melissa Johnson	Meeting planning and conference support
Anne Lane	Communications support

throughout the supply chain, helping to track effects due to aging or reliability, or tracking performance indicators.

Measurements should be viewed as part of a comprehensive hardware security strategy that builds trust across the supply chain. That strategy might include research programs to assess measurement technologies, periodic industry-wide economic studies to assess the effect of current security strategies, and industrial consortia that engage in test procedure development and round-robin testing. Standards are an important part of any strategy or benchmarking effort because they enable the use of a common measurement scale, even when measurements are performed at different locations and by different techniques.

2 Workshop on physical measurements for supply chain security

2.1 Supply chain security working group

In 2020, the NIST Communications Technology Laboratory (CTL) launched a working group to explore industry needs for, and use of, physical measurements for 5G Supply Chain Security (see Table 2). The group hosted the NIST-sponsored virtual workshop "Securing the 5G Supply Chain through Measurement", held May 18-19, 2021, to focus on the goals described in Section 1.3.

2.2 Methods

This report is the product of interviews, the workshop, and literature review.

The methodology for scoping the workshop began with a series of stakeholder interviews. A subset of the working group conducted the bulk of the interviews; these were led by Paul Hale, Melissa Midzor, Ari Feldman, and Nathan Orloff.

After the interviews, the steering group reached out to industry, academic, and government leaders to identify potential speakers to support the workshop. The working group assembled a list of speakers based on participation at recent conferences and recommendations from

leaders in the field. Often recommended multiple times, NIST discussed each potential speaker and many of the participants at length before recruiting them to the workshop. Speakers were chosen based on their technical background and ability to provide complementary contributions to the discussion.

Acting on behalf of the group, Paul Hale invited each speaker to the workshop, reviewing the workshop structure together with speaker to align each talk with the goals of the workshop. The working group also generated a list of potential attendees who were notified and encouraged to invite other potential interested parties. The speakers and participants represented industry leaders, technical fellows, program managers, chief executive officers, executives, and other technical professionals in 5G and supply chain security.

2.2.1 Workshop participation

Participant input was an important source of data for this report. After speaking with industry and academic leaders, NIST requested each interviewee to provide a list of potential invitees. NIST sent an electronic invitation to all suggested participants and opened the workshop to any attendee through an online registration form. Each day of the workshop registrants joined the workshop virtually/electronically. The electronic workshop software recorded which attendees joined the workshop and for how long.

As part of registration, participants were asked to identify their affiliation as government-defense, government-other, test and instrumentation, electronics component manufacturer, communications equipment manufacturer, academia, other (fill in the blank)[4]. Table 3 shows the response of workshop attendees[5].

Registrants were also asked to choose, from a list, all the ways (one or more) in which they planned contribute to the workshop. The responses to this question are shown in Table 4. While many opted to just observe, there were a variety of expertise and interests represented in the workshop.

2.2.2 Workshop data

After the workshop, NIST had four datasets, including digital attendance records generated by the virtual conference software, notes from each note-taker during the breakout sessions, a web-based comment app that attendees could access any time during the workshop, and the speaker's slides.

[4] There was a total of 109 technical attendees. Removing the NIST technical and helper attendees, most of the workshop attendees had industry affiliations, representing approximately 53 % of the external participants. The remainder of the attendees had either government (27 %) or academic affiliations (20 %). Thus, the information gathered in the workshop could have an industry bias, compared to other workshops with a more significant representation of a different population.

[5] "Semiconductor capital equipment" and "Transportation" were entered under "other" by registrants who did not attend.

Table 3. Business sector to which the attendees belonged

Response	Count
NIST (non-helper)	28
NIST (workshop helper)	17
Academia	16
Government Defense	14
Government Other (non-NIST)	8
Industry consortium	8
Communications Equipment Manufacturer	7
Test and Instrumentation	6
5G Industry	5
Electronics Component Manufacturer	4
Telecommunications	4
Law and Tech Policy	3
Consulting	2
Cyber Security	2
NIST MEP participant	1
Software	1
Semiconductor capital equipment	0
Transportation	0

Table 4. Ways in which registrants planned to contribute to workshop

Response	Count
Just an Observer	69
Supply chain management	33
Standards development	20
Counterfeit detection	19
Machine learning	18
Digital/analog signal measurements	17
Government Policy	15
Other	15
RF fingerprints	12
Manufacturing quality assurance	12
Electronic design tools	10
Circuit and multi-physics modeling	9
Physical Unclonable Features	8
Microelectronics	2

3 Measurements for 5G hardware security

The four themes discussed in this section were expressed repeatedly as concerns during the workshop, in interviews, and in the literature. The subsections 3.*x*.*y*, again based on comments at the workshop, interviews, and literature review, explore recommendations for further work that might address these concerns, with the goal of further industry and government application and adoption of physical measurement methods for electronic (particularly 5G) hardware security. This work might be conducted by some combination of industry consortia and various national metrology institutes (NMIs), including NIST, as appropriate.

3.1 Theme #1: Securing the complicated 5G supply chain and wide range of use cases will require multiple approaches, agreed upon by stakeholders at each link in the supply chain, and will include authentication through hardware inspection and characterization that is traceable to the International System of Units

The supply chain for electronics hardware is complex, dynamic, and global, as exemplified by the illustration of a smartphone supply chain in Fig. 2 (from [143]). Because of the many different components in a 5G network, and the many different use cases, there are many 5G hardware supply chains. The supply chain consists of "suppliers", "acquirers", and "system integrators" [40, 144], as well as transportation between supplier and acquirer. Each link in the chain has potential vulnerabilities for the insertion of counterfeit or malicious materials,

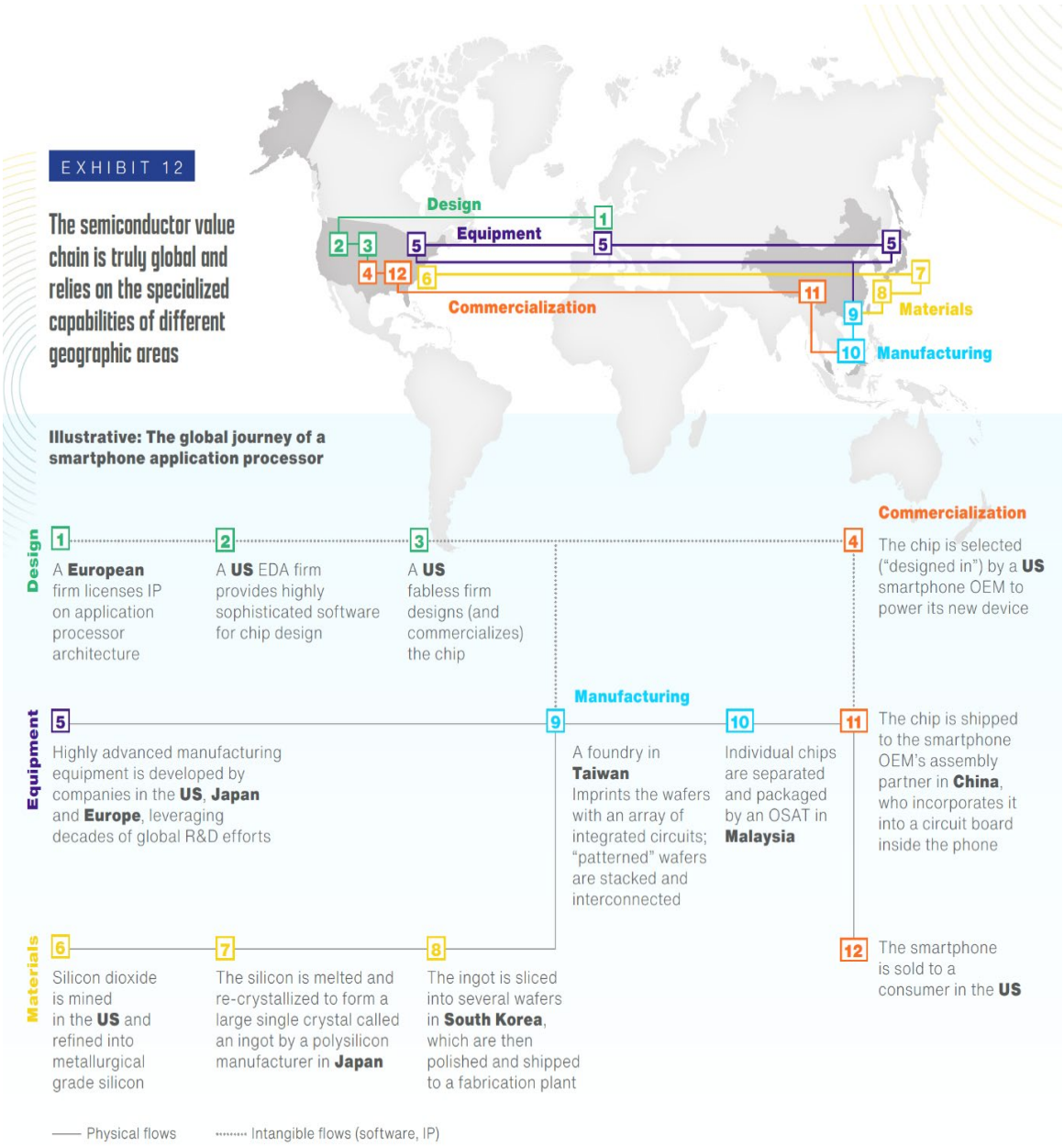

Figure 2. Complex global nature supply chain for a smart phone (from [143]).

designs, or devices, examples of which are shown in Fig. 3 (adapted from [145]). For more details see [4, 6, 146].

3.1.1 Industry consortia should engage to identify suitable use cases, agree upon suitable measurands, and benchmark and standardize test procedures

Acquirers and system integrators need the providers to share provenance and measurement information with them to reduce risk by assuring the quality and security of the materials they purchase. Data sharing should be done in a way that does not disclose proprietary technical or business information. Furthermore, at each successive link in the chain, an acquirer becomes a supplier for the next link until the hardware has been safely and securely disposed of. For example, an IC manufacturer and a printed circuit board (PCB) manufacturer are suppliers for

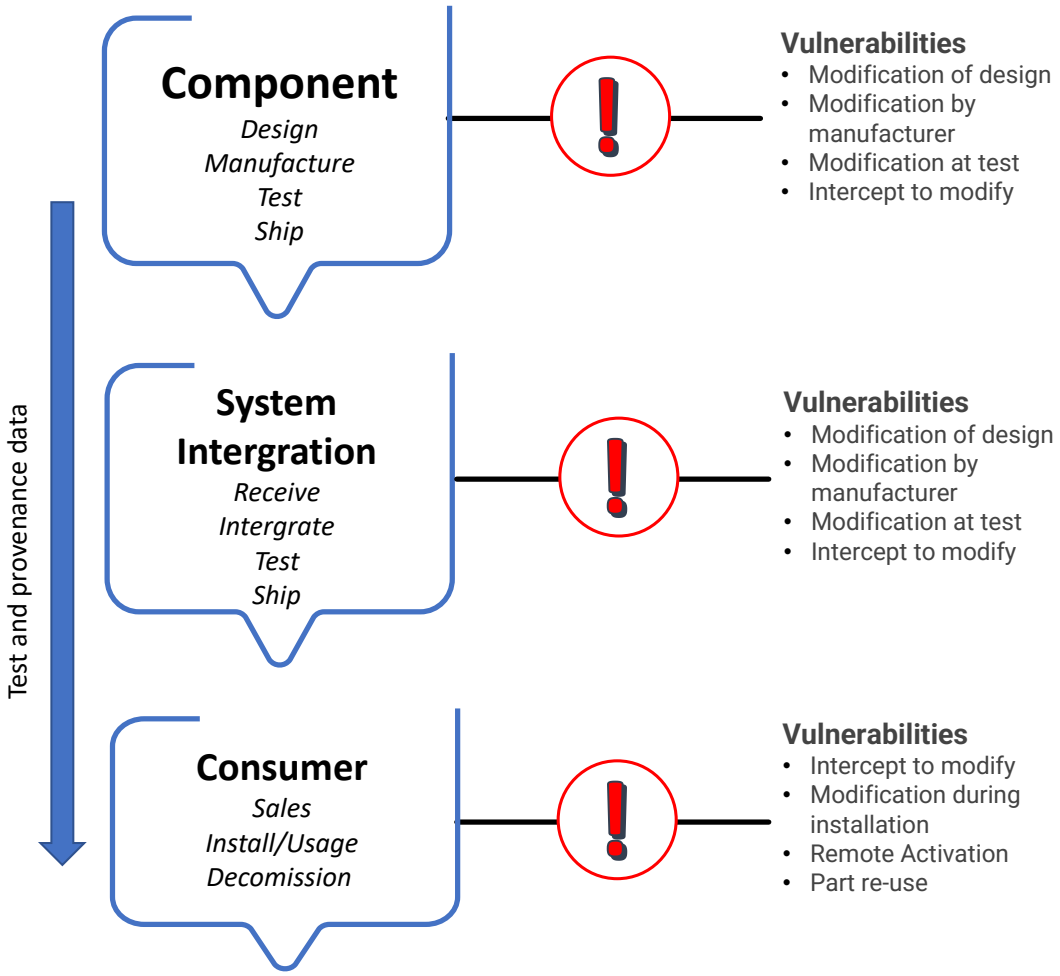

Figure 3. A high-level view of some hardware security vulnerabilities in the supply chain of a completed system, such as a cell phone, gNB, or 5G enabled vehicle. Each step in the supply chain has unique vulnerabilities. A comprehensive security strategy needs to address the unique aspects of each step in the chain and consider the use case, risk, and cost of mitigation actions (adapted from [145]).

a PCB assembler (the acquirer), which in turn might become the supplier to a system integrator. The system integrator will need to be assured of the security and integrity of the PCB and components that are on the PCB, as well as the same for other PCBs that are integrated into the end system. There is therefore a need to share end-to-end information across the supply chain.

The vulnerabilities at each link in the supply chain are different and must be mitigated in a way that is appropriate for that place in the supply chain and for the use case of that hardware at later steps in the supply chain. For example, the mitigation strategies for various IC vulnerabilities will be different from the strategies used to secure vulnerabilities when manufacturing the PCB that the IC will be used with. Mitigation strategies used with a 5G base station (gNB) used in a public network may be different than those used for the same equipment deployed in a network used by the DoD. One mitigation procedure might address certain known vulnerabilities while other procedures might be needed to mitigate other vulnerabilities. Information from multiple security approaches should be transmitted through the supply chain. See Section 3.3 for more discussion of this point.

The measurands associated with inspections and measurements are chosen to reduce risk. By necessity, the measurands will be different at different links in the supply chain. Which measurands are needed will depend on the form of the hardware and its security threats and vulnerabilities, which will be specific to any particular location in the supply chain [4, 147].

Measurands and the associated measurement procedures should be agreed upon by the supplier and acquirer. The acquirer should agree that measurements performed by the supplier are useful and should agree that the measurement procedures give an acceptable level of accuracy and uncertainty for the intended application or use case. Likewise, the supplier should agree that acceptance tests performed by the acquirer give a meaningful result. When measurement procedures differ between supplier and acquirer, disagreements can arise.

In some cases, the acquirer might authenticate the hardware by making inspections and measurements that they then compare to the inspections and measurements performed by the supplier. Making measurement techniques traceable to the SI is an important step towards measurements that are reproducible at different laboratories. The goal of these measurements is to increase the likelihood of detecting a modified or counterfeit device (true positive) while managing the cost of erroneously labeling a piece of hardware as being modified or counterfeit (false positive) [148], as will be described further in Section 3.2.

To use measurement and inspection results for authenticating hardware, data exchange formats should be agreed upon by each party in the supply chain. Data exchange formats should remain the same throughout the supply chain, as system integrators may want measurement information from suppliers from which they are separated by several chain links (see Section 3.4).

3.2 Theme #2: Physical measurements could inform security risks assessments, but must be quantitatively evaluated

As described in section 1.6 there are many different emerging methods for validating hardware through physical measurement. However, recurring themes, both at the workshop at in the literature, are that methods are needed to benchmark the performance of these test methods (see for example [111, 149] and Appendix A under "General topics"). In the case of a classifier, this means having a good understanding of the expected results when testing a good component or a modified component, and understanding the true positive, false positive, and false negative detection rates. Similar, multidimensional metrics exist for identifiers.

3.2.1 Standard test articles

Workshop attendees said that common standard test articles for quantitatively comparing different measurement techniques or standardized methodologies would be useful, but do not currently exist. (After the workshop the authors of this report did find some research examples, including [83, 111, 150]). Standard test articles would also be useful to demonstrate and maintain reproducible measurement systems at different times and at different facilities. A lack of standards also makes it difficult to provide quantitative hardware security specifications. Our suggestion includes both standard test articles and standard measurement procedures.

Our vision for a standard test article includes at least two populations of electronics and lends itself to the classification approach described in Section 1.6.2. The first population consists of pristine devices that meet the manufacturer's specifications and do not have any additional or missing functionalities. The second population of electronics includes a modification, such as a maliciously modified or counterfeit component or some other substantive defect. A measurement of some physical property $\mathcal{P}$ of the circuit is then performed to classify each circuit as a member of one of the populations: 'with modification' or 'without modification'. Examples of the physical property might include, but are not limited to, the output high and low voltage levels of a digital circuit, the distorted output waveform when the circuit is stimulated by a calibrated reference signal at its input terminals, or the power supply waveform when the circuit is stimulated by a calibrated reference signal at its input terminals and the output terminals are terminated in a standard configuration.

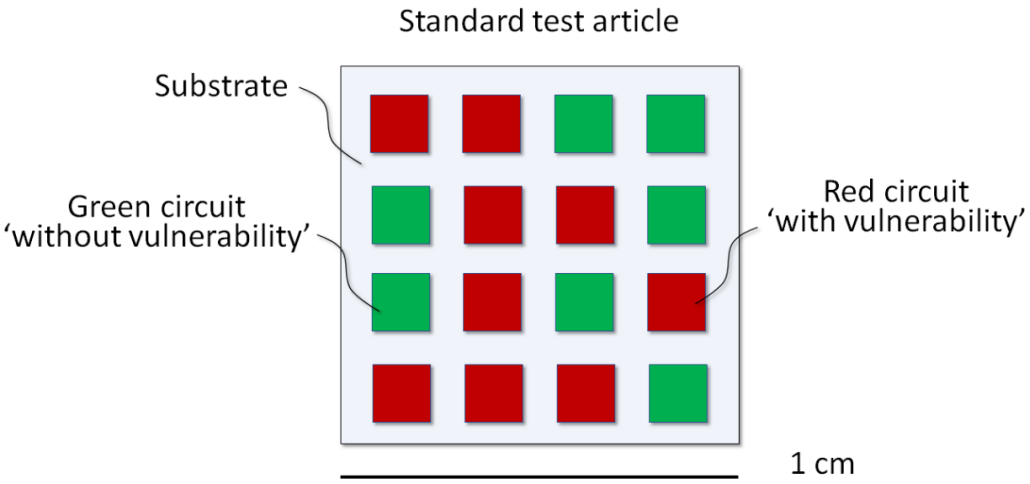

Figure 4. Example of a standard test article for quantifying a measurement techniques' ability to measure specific vulnerabilities. This standard test article allows comparisons across disparate measurement modalities that otherwise produce measurements that cannot be compared directly.

As an example, Fig. 4, depicts a hypothetical standard test article with several integrated circuits instantiated on a single substrate. The unmodified circuits are depicted as green squares and the modified circuits are depicted as red squares. This hypothetical standard test article has an unequal number of green and red circuits that are randomly distributed over the test substrate. In this example, the hypothetical standard test article is 1 cm on an edge.

Any measurement produces data that includes a value and uncertainty under a given measurement condition. As depicted in Fig. 5(a) not all the measurements have the same value because of random and systematic errors in the measurement. This is also true for our hypothetical standard test article. Fig. 5(b) shows the results of a hypothetical measurement technique applied to the standard test article. Here, the two distribution functions correspond to measurements of the 'red' and 'green' populations in Fig. 6. In this example, a user applies a threshold on the value $\mathscr{P}$ to classify each circuit. Measurements of circuits that fall below the threshold are classified as green and those falling above as red. If the distribution functions overlap, then some fraction of green circuits might be misidentified as red and *vice versa*.

Fig. 6 shows an example of how our classifier might be used to sort the devices on our hypothetical test article. In this example, our measurement and threshold value classified two circuits incorrectly. Comparing the measured classification to the known classification (sometimes called "ground truth") allows one to estimate the probability of correctly classifying green circuits as green, red circuits as red, and incorrectly classifying green circuits as red or red circuits as green [148]. Because the distributions in Fig. 5(b) are generally unknown, it is necessary to estimate the above probabilities for different thresholds. Once this is done, the appropriate threshold can be chosen based on a risk assessment (see Appendix C).

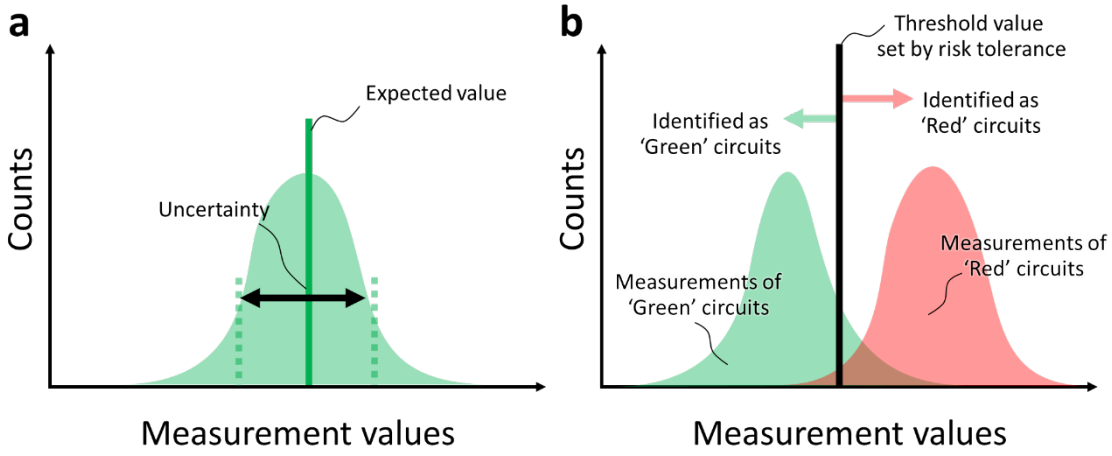

Figure 5. (a) Example of a distribution of measurement values. (b) Example of two distributions of measurements of a hypothetical standard test article that includes 'green' circuits without a vulnerability and 'red' circuits with a vulnerability. In this case, a threshold value is a hard cutoff used to identify both the 'red' and 'green' circuits.

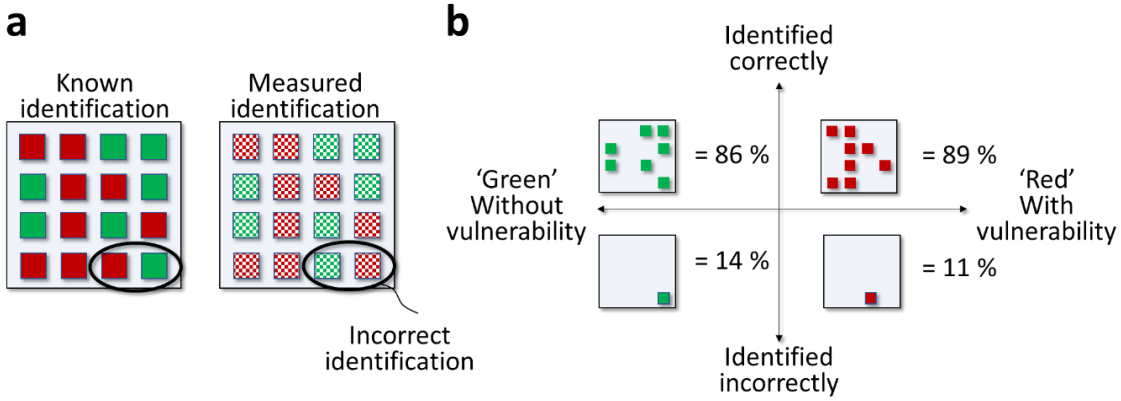

Figure 6. (a) Example of a map of known identification and a map of measured identification. We deliberately chose unequal totals for the number of red and green circuits. The example includes 2 incorrectly identified devices. (b) A quadrant chart showing the correct and incorrect identifications for the red and green devices.

There are a few key points in Fig. 6. One must have the known identification to estimate the probabilities in Fig. 6(b). As an example, Fig. 6(a). has 7 known green circuits and one was incorrectly identified. The probability of correctly identifying a circuit as green is 86 % (6 out of 7) and the false negative is 14 % (1 out of 7); thus, the total is 100 %. Likewise, the measurement identified 8 red circuits correctly (89 %), and one incorrectly (11 %), which also sums to 100 %.

As a practical example, Fig. 7 goes step-by-step through the standard test article process. In this example, a user obtains a known standard test article from a national metrology institute or an industry consortium. The user measures physical property $\mathcal{P}$ of each device, and then uses the measurement values as inputs to identify each device. Next a classification step labels each device in the population from the measured values, generating a map of the measured classification. Finally, the user (or other entity, see next paragraph) compares the measured classification against the known class of each device. This comparison step quantifies the ability of the measurement technique to classify devices with this specific modification. The resulting comparison data can be used to inform a risk control process or to compare different measurement techniques.

Some subtleties may be necessary. The known values of the individual components of the standard test article should be kept secret from the measurement lab and the general public. In the former case, secrecy is needed to avoid possible test bias, while in the latter case, counterfeiters might use the added understanding of the refence artifact to subvert the test process. Actual values of the reference circuits might be obfuscated through the use of a web-based process for submitting and benchmarking results, limiting the number of submissions for a given test artifact, and release of only aggregated results.

The above example with only red and green devices is an oversimplification. Firstly, if only one type of modification were sampled, there may be a risk of not sampling the full space of possible threats. Secondly, there must be a way of checking the resolution of the measurement approach. Some trojans or other modifications might manifest themselves at varying degrees. Without some varying magnitude of the modification, it may be difficult to quantify what can and cannot be detected.

Standard test articles could lead to a false sense of security, in that one might deem a technique capable of identifying a real circuit defect when in practice it cannot. This situation could arise if the measurement distribution of the property $\mathcal{P}$ for the test article is significantly different than the measured distribution for real defects. While as one attendee put it, a “flawed solution

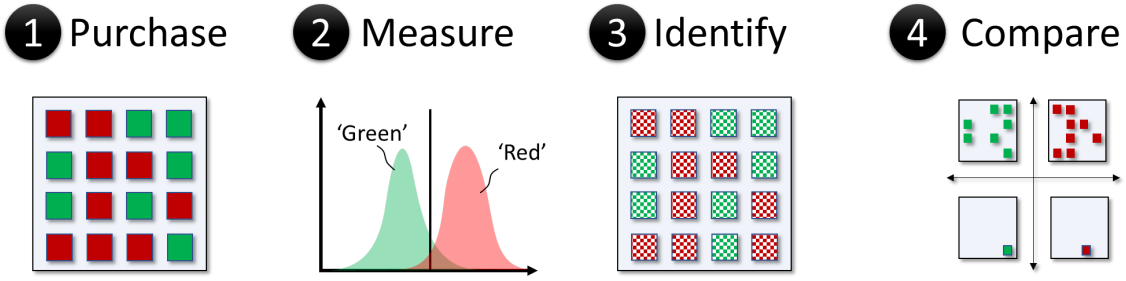

Figure 7. Measurement verification process. A user obtains a standard test article that they measure with one or more measurement techniques. Then, a classification step groups circuits into ‘red’ and ‘green’ classes. The next step compares the measured identification to the known identification, which produces metrics that can quantify the performance of the measurement technique against alternative measurement-based approaches.

is better than no solution", we must consider weaknesses in the standard test article and ways that the article can be improved.

Another inherent danger is that standard test articles might quickly become outdated. This might be addressed by a dedicated team of engineers working with an industry consortium to maintain and support standard test articles. Indeed, partnerships with industry, government, and academic research might help clarify other dangers and identify new ways to solve them, as discussed in more detail in Section 4.

3.2.2 Best practices for measurements, methods for classification and identification, and comparisons and the case for industry standards

As mentioned above, there are many different measurement methods that are in development for supply chain security applications. Some measurement techniques compare unknown devices to an internal standard used for benchmarking, sometimes called a 'golden reference' or 'golden standard'. These internal standards and the measurements techniques applied to them can vary from lab-to-lab, which makes it challenging to assess supply chain security across each link. Traceable standard reference materials, instruments, and data are important for developing industry standards precisely because they have known variability that is not lab dependent.

Even without a traceable standard test article, standard practices set by industry consensus could help address this problem by establishing best practices or standard procedures for measurements and classification or identification methods. An industry-government partnership is one way to develop industry standards. These efforts should focus initially on a handful of the most common techniques, and once a measurement method and use case is selected, participants could perform round-robin benchmarking activities to document variability between participants and measurement techniques and establish best practices. The output of a such activities could provide essential inputs for physical and documentary standards and might help determine minimal requirements for standard test articles or industry documentary standards.

In addition to different measurement methods, there are also different analysis tools for using the measurement data to classify authentic and modified hardware or identify specific devices. These tools range in complexity from simple single variable statistical tests, such as those outlined in Section 3.2.1, to multi-variate statistical tests and machine-learning algorithms [151, 152]

Machine learning and principal component analysis are some examples of more sophisticated tests to identify authentic hardware or hardware with and without defects. Examples provided in the workshop took raw data and then used a 'golden reference' to learn how to measure the difference between hardware with and without defects. Such tests rely on training data to render a classification or identification.

Answering some open questions could improve application of the sophisticated tests to hardware security. How to quantitatively compare two different sophisticated tests and benchmark them against simple tests? How to evaluate the accuracy, precision, and uncertainty

of sophisticated tests and their training data? What do we need to do to quantify a test's behavior when measurements fall outside or near the extremes of the training data? How do we ensure the security of the testing algorithms and the training data themselves? Can the machine learning algorithms be explainable and physics based? While not comprehensive, these questions might help start a broader conversation about how to integrate sophisticated classification and identification tests into supply chain security.

There are examples of national metrology institutes (NMIs) generating and providing standard reference data sets. Developing a standard reference dataset requires industry input and guidance and a framework for getting feedback as quickly as possible. A standard reference dataset suffers the similar inherent dangers as the standard test article. Namely, it can produce a false sense of security or become outdated and irrelevant.

The type of effort required to support standard test articles and datasets differs from documentary standards developments in a few important ways. Both argue for large research efforts and consistent government/industry engagement, often through consortia. However, standard test articles require infrastructure to build the articles, characterize the articles, and maintain the stock of articles as dictated by customer demand. Development of a one-off test article, without maintenance of the hardware used to provide the standard or continued stakeholder support, will not be successful. Periodic review, to sunset obsolete standards, will be necessary because a growing standard artifact portfolio would become unsustainably large.

3.2.3 Measurement coverage

As there are many different vulnerabilities, there are many tests that might detect these vulnerabilities with different levels of effectiveness. The physics behind the tests and how they detect the vulnerability needs to be well understood, both to understand better how vulnerabilities might escape detection and to understand the range of tests and analysis algorithms required to detect the anticipated vulnerabilities (*cf.*, [153]). Standard test articles might be used to gain this understanding.

Furthermore, physical tests do not need to mitigate all risks. For example, the end user may have considered mitigation options in the system design. Analysis of the measurement coverage may allow the user to test less or use a less expensive test campaign that only screens for vulnerabilities that are not mitigated by the overall system design.

3.3 Theme #3: Deployment of physical tests must address the needs of manufacturers and end-users for specific application spaces

To provide the widest possible benefits to the hardware security community, physical tests for hardware security should provide value to end-users, who usually bear the risk posed by hardware security threats. Successful deployment and adoption of physical tests will depend critically on balancing the benefits of this approach to hardware security against the costs of implementation. This section explores different potential approaches to deployment of physical tests for industry and end-user adoption, identifies some barriers to adoption, including cost and scalability, and explores ways in which benefits of physical tests can be quantified and positive impacts identified. We conclude with a suggestion for establishing concrete use cases that can enable meaningful cost-benefit analyses and address impacts for

specific 5G and microelectronic application spaces, including aerospace and defense, autonomous vehicles, medical and health, mobile communications, industrial internet of things (IIoT) devices, and high-performance computing.

3.3.1 Deployment Approaches

There are in general a wide variety of options for deploying physical tests for hardware security depending on the specific application. These can include labeling and readout, measurement-based identification or fingerprinting, challenge-and-response testing, and multimodal device profiling, to name a few.

The question arises about how to address the efficient deployment of physical tests for hardware security in industrial settings covering a wide range of application spaces. The answer depends somewhat on the application space being addressed. For example, for some aerospace and defense applications where extremely low false negative rates (*i.e.*, the probability of a malicious or counterfeit part being classified as "good") are required, more extensive testing can be accommodated despite requiring longer test times, higher cost, and more specialized equipment and operators. The same is true for applications where life-threatening risks can result from hardware security threats, such as autonomous vehicles and medical/health applications. On the other hand, for some IIoT applications, the number of parts that require testing can be extremely large, favoring rapid tests with high throughputs that may allow much higher false negative rates. It is essential to keep in mind that no one approach to deployment of physical tests for hardware security will be appropriate for all applications where some level of hardware security is desired. For some end-users, a type of security certification based on the physical test measurements employed could provide additional value for a component, potentially justifying a higher cost.

3.3.2 Barriers to Adoption

Workshop participants raised several important concerns regarding deployment of physical test for hardware security in a manner that would enable widespread adoption. Barriers included: (i) the added cost of hardware tests, and who would pay for them; (ii) the ease of use of hardware tests for manufacturers or assembly facilities with limited test equipment and staff expertise; (iii) concerns about organization and responsibility for measurement data and test results; (iv) data formats, management, and security; (v) the speed of physical tests and throughput limitations for a large volume and variety of potential devices; and others. Given the large range of potential different physical tests and application spaces, these important barriers are likely best addressed within the context of specific applications.

3.3.3 Impacts and Cost/Benefit Considerations

To evaluate impact and pursue an efficient deployment strategy, it is necessary to evaluate the cost of testing and impact of false positives for manufacturers (how many good parts need to be thrown away or re-tested) for different application spaces. The cost for manufacturers includes not only the cost of implementing the needed test(s) for a given application space, but also includes the impact of the false positive rate for a manufacturer. It may be possible to lower the cost of a specific physical test, but the lower cost test might result in a higher false positive rate, which requires a larger number of parts to be either discarded or retested, consuming time, money, and resources that might be better used elsewhere.

The impacts of physical tests for hardware security also need to be considered from an end-user perspective. While these impacts will likely depend on the specific application space, end-users will have requirements related to the false negative rates of physical tests for hardware security, as this is a valuable metric to quantify risk via the percentage of potentially compromised devices that pass a given physical security test. In general, the need for lower false negative rates will result in higher false positive rates, driving up testing costs and time for manufacturers.

3.3.4 Development of Use-Cases to Quantify Impacts in Specific Application Spaces

Next Steps: Engage with specific industry segments/application areas (via consortia**,** workshops, industry groups, etc.) to evaluate deployment issues for specific manufacturing environments and establish the relative importance of hardware security for end-users. These engagements should have as a goal the development of concrete use-cases for the deployment of physical tests against specific hardware security threats for a given application space. In this manner the specific costs and requirements of hardware testing on manufacturers can be weighed against the benefits of reducing security risks for end-users.

3.4 Theme #4 Acquirers and system integrators need secure methods to exchange provenance and measurement information with suppliers

Component or integrated circuit manufactures typically characterize their products to internally validate performance, both for quality assurance and process verification. For integrated circuits and printed circuit boards a “traveler document” or “digital twin”, often tracks the device through the fabrication to record processing conditions and circuit performance. Combined, these data make up inputs for quality assurance documentation for compliance with various international standards, which may include ISO 9000 [154] requirements. Quality assurance measurement data is often proprietary information because the data contains intellectual property or trade secrets that could give insight into the manufacturing process. As a result, manufacturers provide specifications documents with nominal performance and confidence intervals based on manufacturing tolerances [155], holding back the “traveler document” data which may contain measurement data with uncertainties. This paradigm means that real measurement data that could be used to authenticate hardware never makes it to the component or system acquirer.

Importantly, traveler document data can differ from provenance data. While it can contain metadata or image data that could be used for provenance-based authentication, it also contains correlated measurement data corresponding to both the processing conditions and the performance of a component. In this section, we specifically discuss the direct measurements of component performance and how they are propagated through the supply chain.

Nominal performance is enough information to allow for inspection testing procedures and for circuit designers to predict the nominal performance of a circuit. A rectangular distribution on the nominal performance is typical for circuit components and is based on both the manufacturing tolerances and validation measurement uncertainty. However, this nominal performance does not provide enough information for circuit designers to predict a distribution of outcomes due to individual components. (For example, for RF components and systems, the

frequency response with uncertainties provides insight, into the true operation.) The situation is compounded when system integrators use component replacements (due to lack of supply, reduction in cost, etc.) that nominally perform the same as the original yet are likely to have a different distribution in their actual performance. Administratively these components are interchangeable, yet the minor differences can create unanticipated downstream effects on the system performance and distribution of measurement results when applied for security applications.

When considering supply chain integrity and verification, measurements of the specific waveforms generated by a component or system can be used to identify anomalous behavior by comparing to a known performance distribution. Without measurements made by both the supplier and the acquirer, it may be difficult to determine if the changes are due to unauthorized tampering, or due to authorized supply chain replacements. Furthermore, the distribution of expected component performance must be accurately communicated by the supplier to draw conclusions regarding the confidence in such a measurement program.

3.4.1 Explore framework for transferring measurement data and uncertainty from vendor to vendor

A paradigm change is required around measurement data in the manufacturing process to enable efficient propagation of data throughout the supply chain (from manufacturer to integrator and beyond). A recommendation is to build measurement data with uncertainty into the product development workflow. From component manufacturing and integration, quality assurance, and then shipment through the supply chain, all data relevant to the product and end use should be considered for transfer with the product. Obviously proprietary information needs to be protected, but all other data that could be useful for modeling, simulation, and measurements should be considered.

There are many documentary standards that cover data exchange within manufacturing lines and between vendors. Within the factory, the Connected Factory Exchange [156] provides a protocol for all tooling and test equipment to provide metadata associated with the manufacturing process. As specified, this protocol is meant for IoT type operations of tools within a factory and only captures qualitative status messages. Standards such as IPC-1756 [157] specify metadata needed for packaging by other vendors including material properties, process sensitivities, and interface specifications. To these authors knowledge, none of these efforts explicitly include uncertainty in measurements.

Beyond necessary data for manufacturing, there has been a push for provenance-based traceability through documentary standards. IPC-1782 [52] outlines a series of risk-based metadata requirements for all electronic products to track through the supply chain. Traceability levels are based on risk analysis and define the type of information, data integrity, data collection automation, and data lifecycle. As defined in the standard, the highest traceability, Level 4, is to “Capture all available metrics: complete test results and process data” with a data integrity of 9 sigma. Even at this highest level, while pass/fail test results are included, the standard does not consider quantitative uncertainty on these measurements as essential for propagation down the supply chain.

Data transfer mechanisms need to enable both manufacturers and integrators to share data in a vendor agnostic and confidential way. When considering complex systems (*e.g.,* 5G+ systems) which are comprised of hundreds of components, the data from individual components needs to be easily findable and usable. The Digital Metrology Standards Consortium (DMSC) has supported the Quality Information Framework (QIF) which "enables the capture, use, and re-use of metrology-related information throughout the Product Lifecycle Management (PLM) and Product Data Management (PDM) domains" [158]. IPC-1782 also outlines an architecture for data exchange through a secure supply chain database to exchange tamper-evident data through a blockchain mechanism [159]. A framework that leverages these concepts, and includes measurement data with uncertainty, could be very beneficial to the 5G+ supply chain but must also protect confidential information that is identifiable. Through a change in operations, one could identify measurement-based approaches to validate the security of the supply chain through reduction of uncertainty on performance.

3.4.2 Build uncertainty propagation of individual components into circuit simulators and machine learning algorithms

Building on the suggestion of Section 3.3.1 while one could advocate for more measurements and the transfer data along the supply chain, how the data is used downstream is also a major consideration. Circuit designers already use software tools like SPICE which can allow for Type B component tolerances [160, 161] While some academic work has been done on uncertainty quantification [162, 163], no current SPICE simulators account for full frequency responses with correlated uncertainties. Building the uncertainty into the circuit design enables the *a priori* understanding of the distribution of outcomes for any given RF circuit.

To enable this change in paradigm, the data formats may need to accommodate large amounts of metadata and measurement data. Electronic Design and Automation (EDA) tools have used data formats, such as ODB++ [164], to transfer computer aided designs to computer aided manufacturers (CAD to CAM) since the 1990's. In 2004, IPC-2581 [165] was implemented to combine the best features of existing design formats and create a global standard for efficient data transfer between these entities. This format captures information related to tooling, manufacturing, assembly, and inspection, and designers can use the format for integration of subcomponents into assemblies. As noted in Section 3.4.1, none of these formats currently capture measurement uncertainty data, but that is only part of the usage chain. The EDA tools themselves need to be able to use and propagate the uncertainty data through to the simulation results. This change in data handling could require more intensive computational resources for approaches such as Monte Carlo simulations, so for broad adoption of these methods, EDA tools should carefully consider implementation tradeoffs between performance and data usability.

Machine learning algorithms are increasingly used to assess anomalous behavior for communication systems [166]. To develop machine learning algorithms, knowledge of the system of systems is necessary to predict the distribution of outcomes that are allowed. Utilizing a data framework, propagation of the measurement uncertainty of components through the system to the machine learning decision point, could give better confidence in the machine learning classification of the system behavior. Discerning the difference between nominal performance with uncertainties (that include process variations and manufacturing

tolerances) and malicious behavior of tampered parts is critical to the success of these machine learning approaches.

4 Next steps for securing 5G hardware

Physical tests for security provide an extremely wide range of new test methods to help reduce risk of hardware-based threats for 5G applications. Potential benefits of measurement-based approaches include:

- Physical measurements can be applied to detect and identify hardware security threats and quantify risks for multiple device domain levels and can be implemented at multiple points in the supply chain.
- Physical tests create opportunities for innovation to develop new technology-based solutions to the ever-evolving hardware threats to 5G applications.
- Physical tests have the potential to complement existing provenance and documentary standards-based approaches to improve the hardware security posture for the myriad of 5G applications.
- Physical tests can *add value* for manufacturers and end-users, beyond security, by providing critical information on performance and reliability of hardware components.

Given the significant potential of physical testing to reduce hardware security threats, and the broad themes identified by this document, what are the necessary next steps for developing physical tests to secure 5G hardware? In what follows we address the characteristics that a comprehensive strategy to develop physical testing might include, provide guidelines for developing application-specific use cases to demonstrate the value of physical tests, and discuss opportunities for creating the collaborations and cross-disciplinary communities that will be needed to rapidly develop and implement new approaches to physical test for hardware security.

4.1 Features of a comprehensive approach

Given the wide range of potential hardware threats and a correspondingly large number of potential measurement-based countermeasures, is there a basis for a cohesive approach to developing and implementing measurement-based approaches to hardware security? What is required for success? Despite the wide range of potential threats and widely differing levels of risk tolerance of different application spaces, measurement-based approaches to hardware security all tend to follow similar trajectories. Requirements include the identification of potential test points, the need to document details of relevant threats and existing countermeasures, followed by the development of potential measurement approaches for physical test(s). Any developed physical tests must be validated, and subsequently deployed in manufacturing or other non-laboratory environments. The impact of the developed tests needs to be described in the context of the security requirements of the proposed end-users, and the impact of the costs considered from a manufacturing perspective.

These considerations describe a need to develop a threat response framework that is based on the specific application space, and that considers both the benefits and costs for manufacturers, integrators, and end-users. The development of application- or industry-specific use cases that articulate this common trajectory could be a valuable approach to developing a comprehensive approach to 5G+ hardware security across the wide range of current and future 5G+ application spaces. While the details of such use cases may be quite

different, the common goal would be to evaluate the potential added benefits of different hardware testing approaches to reduce the risk of hardware vulnerabilities in 5G+ applications.

4.2 Developing use cases for physical tests in hardware security

The above considerations are presented below in Fig. 8, which describes an approach to developing a research pathway for enabling efficient new physical tests for hardware security. The pathway can be applied to create a wide range of application-specific use cases, to evaluate potential benefits of implementing physical tests against the cost of test development and deployment. This approach fosters innovation by connecting the fundamental U.S. research infrastructure with application-specific needs for different 5G+ application spaces, while engaging with the manufacturers, end-users, and government stakeholders to strengthen hardware security approaches across the U.S. economy.

Following Fig. 8 for a specific use case, the potential test point(s) for implementing physical test need to be identified in the context of complex global supply chains for an application space of interest. This identifies where one is looking for the vulnerability, such as the component level, the board level, the system level, *etc.*, and determines where in the supply chain testing may be viable. The Common Weakness Enumeration (CWE) web site can help with this process [146]. Then specific threat(s) must then be identified and characterized. The Common Attack Pattern Enumeration and Classification (CAPEC) [167], ATT&CK [168] and Trust-hub [169] web sites might prove useful for understanding potential threats[6]. Once the test points are established and the hardware threat(s) identified, the benefits of existing mitigation strategies can be considered to evaluate if there is a significant risk that physical test can effectively mitigate. If physical tests can help, then physical hardware tests can be proposed or developed based on one or more physical measurement approaches, often including sophisticated machine-learning algorithms. The efficacy of the measurement-based tests must then be validated against relevant threat models, exploiting known-good populations or strict

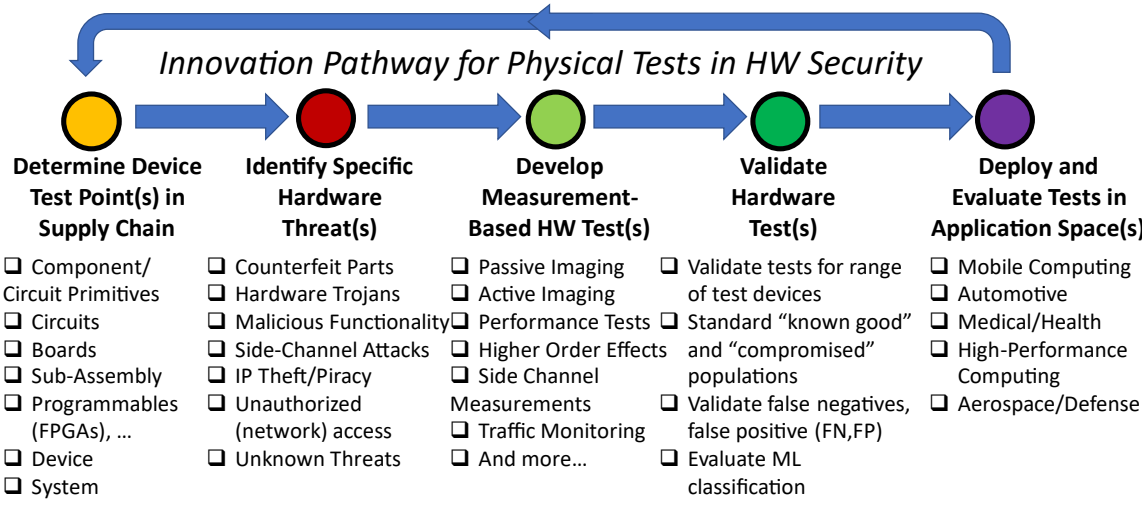

Figure 8. Innovation pathway for developing physical tests for hardware security.

[6] The cited web pages were originally designed for cataloging software vulnerabilities and have recently included hardware vulnerabilities. The application of the sites is explained in [170] along with suggested improvements.

provenance controls for validation. Once the test(s) have been validated, then the tests and protocols must be deployed in manufacturing or other non-laboratory settings for use by non-specialists. The specifics of this deployment will depend strongly on the potential application space and the desired insertion point in the supply-chain. The collection of successful and unsuccessful use cases can then be used to inform future development of physical tests to mitigate hardware security risks for other threats and application spaces, including for newly identified threats.

4.3 Opportunities for collaboration and community-building

The above pathways for the development of physical tests for hardware security, and the broad themes identified in Section 3 together reveal potential new opportunities for collaboration and cross-disciplinary team building that will be needed to enable successful development of measurement-based countermeasures to security threats for 5G+ hardware. Such collaborative activities are a critical part of an overall strategy for implementing physical tests for 5G+ hardware security, and can include focused efforts such as conference sessions, workshops, industrial consortia, and standards activities. The timely development of cohesive communities dedicated to 5G+ hardware security is critical, particularly considering the rapid pace of the development and deployment of new 5G+ applications across the US economy. Without the close collaboration of different R&D and manufacturing communities, it will be difficult to respond to existing and emerging hardware threats for 5G+ applications in a timely and effective manner.

The complexity of the global supply chain for many microelectronic and 5G+ components and devices were discussed extensively in theme #1 in Section 3.1 above. Given the dynamic and complex nature of these supply chains, what opportunities exist for coordination among seemingly disparate elements? One possible approach is to convene workshops or industry groups to draft use cases for specific applications, such as for example addressing counterfeit RF components for 5G+ base stations. This would allow for concrete discussions around specific problems in 5G+ hardware security, drawing on current industry efforts (*e.g.*, see Section 1.6.5), with an achievable outcome in the form of a detailed draft use case.

The challenges surrounding physical test development and validation summarized in theme #2 in Section 3.2 above suggest opportunities for developing collaborations between cybersecurity and hardware security experts to help define threat characteristics and models and the researcher community developing and validating physical tests to detect and identify such threats. Targeted conference sessions focused on these issues for specific hardware threats, in addition to government-convened working groups, are potential avenues to enable the needed collaborations in this area.

Coordination among researchers developing and validating physical tests with manufacturers, integrators, and end-users was addressed under theme #3 in Section 3.3 above. To facilitate collaborations in this area, the development of industry working groups for specific application spaces of interest to manufacturers may provide new opportunities. Industry groups such as the International Electronics Manufacturing Initiative (iNEMI), IPC, or CTIA [171–173] could provide valuable insight from the perspective of manufacturers and potentially contribute to the development of draft use cases focused on 5G+ hardware security issues relevant for electronics manufacturing.

Coordination among manufacturers along different parts of the supply chain regarding test deployment and validation efforts, as well as for the purposes of measurement and data sharing, was addressed under theme #4 in Section 3.4 above. Exploration of frameworks for sharing data and test implementations would be facilitated by the development of draft use cases to explore specific issues related to data sharing, uncertainty propagation through simulations, and development of efficient machine learning algorithms.

5 Conclusions

Advances in the communications technology drive innovations in computing, artificial intelligence, advanced manufacturing, augmented reality, and telemedicine. Each of these promising technologies is driven by any combination of high data rate, low latency, or massive connectivity enabled by 5G+ deployments. Compromises in the safety and security of these technologies will stifle economic growth, endanger human lives, loss of privacy, and could impact national security.

To add to this conversation, NIST reviewed the literature, interviewed key industry participants, and held a two-day workshop. These information gathering exercises served as the source material for this report. This report attempted to capture and bin the ideas into four themes and makes associated suggestions for each theme. It must be emphasized that this report is not a comprehensive representation of the available sources. The themes and suggestions are the beginning of a conversation and should be considered with other work in this area to develop a comprehensive hardware security strategy.

The first theme recognizes that the 5G hardware supply chain is dynamic and complex. Any effort to enact solutions will need to coordinate activities and build consensus between multiple and globally dispersed stakeholders throughout the supply chain. NIST suggests a coordinated industry-government partnership specifically focused on developing piloted solutions and tailored test cases for supply chain security vulnerability assessments. While making demonstrable headway, these efforts would also serve as templates for future activities to counter new vulnerabilities.

The second theme recognizes that measurements could positively impact risk assessments, but without common standard test vehicles, artifacts, or methods it is difficult to evaluate which measurement technique is best suited for each vulnerability. Security oriented measurements are not generally a part of the industry's 5G+ supply chain security portfolio. NIST suggests that an industry-government partnership could define and develop standard test vehicles and methods to facilitate quantitative measurements that focus on specific vulnerabilities. These standard test vehicles and methods enable measurements that can help quantify risk. However, continued development will be required to ensure that the standards are relevant to evolving threats.

The third theme recognizes the need for different approaches to deployment of physical tests for industry and end user adoption. It also identifies barriers to adoption, including cost and scalability, and explores ways in which benefits of physical measurement can be quantified and positive impacts identified. NIST suggests establishment of tailored use cases to enable meaningful cost benefit analyses and address impacts for specific hardware applications.

The fourth and final theme recognizes that the exchange of measurement data at multiple points across the supply chain could create a layered series of security checks. It also recognizes that industry generates and stores comprehensive measurement data of each component, but often this data is deemed proprietary. Consequently, much of this measurement data often remains in house. Transmitted data often lacks the specificity to enable meaningful risk assessment. NIST suggests exploring secure data management and transfer frameworks that enable companies to securely and economically transmit measurement data, uncertainty, and data measurement methodology.

In conclusion, measurements can add significant value to a 5G+ hardware security strategy, adding complementary security information and increasing supply chain resilience.

Appendix A. Workshop structure

The agenda for May 18th is shown in Table 5. The first day began with opening remarks by Marla Dowell, followed by an open conversation by Lisa Friedersdorf of the White House Office of Science and Technology Policy. The next speaker was Paul Hale, who introduced NIST, the workshop, and the breakout session ground rules. The goal of these first talks was to listen to representatives from the current administration about federal goals and upcoming priorities and to set the stage for the workshop and the talks that followed.

The second session was "Current measurements and gaps for 5G hardware". This session discussed industrial techniques to produce provenance data, unclonable tags, and pre-life-cycle data (sometimes called a traveler) that accompanies each product before it changes hands between vendors. There were four talks in this session. Ophir Gaathon from DUST Identity gave the first talk on "Anchoring TRUST". This talk introduced the idea of the asset-centric supply chain, where integrity is often assigned to a physical object with provenance data. Maintaining hardware security requires maintaining provenance data, which has its own associated costs and vulnerabilities. One potential solution is to make identity a physical attribute associated with an object. This solution is the argument for physically unclonable functions. The second talk, by Yousef Iskander, discussed examples of hardware security threats as described in the popular media, and how they impact a company's market capitalization, shareholders, and the public. Turning an eye towards efforts at Microsoft, the talk showed how counterfeits evolved and are almost indistinguishable from genuine hardware. The talk advocated for a CAD (computer-aided design)-based security paradigm where centralized tools and resources could be used to standardize hardware at the circuit level. Stergios Papadakis's talk on "An RF side-channel reverse engineering tool" discussed Johns Hopkins Applied Physics Lab's effort to use RF side channels to monitor software installed on a processor. Finally, the session concluded with Kabir Kasargod's talk on "Quantifiable assurance performed by Qualcomm". This talk discussed the hardware supply chain and how Qualcomm implements trust in an industrial setting and uses that data to help produce products. After the talks concluded, attendees joined one of ten breakout sessions on "Threats, Vulnerabilities, and How to mitigate them" Discussion prompts for this session are listed in Appendix B.

The agenda for May 19th is given in Table 6. The second day began with opening remarks by Marla Dowell. These remarks reintroduced the workshop and the breakout session ground rules. The third session was "Innovation in measurement strategies to secure the 5G supply chain". This session's four technical talks discussed the need for measurements and what new measurement techniques are on the horizon for hardware supply chain security.

The first talk by Ian Oliver at Nokia Bell Labs discussed "Experiences in System Integrity Measurement from Remote Attestation and TPM". This talk discussed the root of trust in hardware systems and introduced the concepts of "measure, attest, verify, decide". The second talk by Mark Tehranipoor addressed "Hardware Security: A Physical Inspection Perspective". This talk introduced the taxonomy of hardware threats and classifications, placing them in context with the hardware supply chain. The talk then progressed through specific examples of supply chain vulnerabilities and work at University of Florida to understand and mitigate those risks. The talk advocated for a measurement-based inspection

approach to hardware security. The third talk by Kaushik Chowdhury entitled “Trusting the fingerprint: Challenges and advances in RF fingerprinting for device identification” focused on using the physical layer to fingerprint hardware in a network. The talk described research on machine learning to identify individual UEs in a communication network. The talk demonstrated the feasibility of hardware fingerprinting with real hardware “in the wild” with 99% accuracy and highlighted the need to understand channel effects. The final talk of the session, “Supply chain security insights” by Keith Rebello (DARPA), recognized the complexity of the problem and the vast number of attack surfaces. The talk discussed current programs on detection methods and hardware safeguards in communications and computing technology. The talk concluded by calling out the need for tools to compare different methods for detecting trojans. A major theme throughout the talks was the need to develop standards (physical, data-based, and procedural) to compare different methodologies. Section 3.2 discusses this theme further. After the talks concluded, attendees joined one of five breakout sessions on “Overlapping metrologies, New opportunities”. Discussion prompts for the session are listed in Appendix B.

The fourth session continued the theme of developing measurement techniques where Richard Ott of the Air Force Research Lab (AFRL) talked about second order effects for classifying authentic and counterfeit devices. The theme then changed to standardization and industry adoption. Urmi Ray described how iNEMI has worked through collaborative industry engagement to develop measurement best practices for characterizing materials properties at microwave and millimeter wave frequencies for 5G applications. Michael Schuldenfrei and Marc Vanden Bossche talked about efforts at NI to develop an assurance network for the entire supply chain. The system will use multiple attributes at each manufacturing stage to authenticate parts, ensure quality and reliability and identify potential tampering or counterfeits. The system will allow participants to create unique authentication methods, including ID tracking, physically unclonable features, fingerprints (such as RF fingerprints), data check sums, image comparisons, and generic anomaly detection. Several workshop participants expressed concerns about storing and exchanging measurement data that might be used to extract proprietary information about circuits or business health. Sylvere Krima of NIST closed the session by presenting NIST work on trusted exchange of digital manufacturing data, such as computer assisted design (CAD) files and dimensional measurements of mechanical parts.

Table 5. Workshop agenda, May 18th

Session #1: Role of measurements in securing the nation's 5G supply chain
"Welcome" –Marla Dowell, NIST
"A conversation with the Office of Science and Technology Policy" –Lisa Friedersdorf, White House Office of Science and Technology Policy
"NIST workshop on measurement-based approaches to 5G supply chain security" –Paul Hale, NIST
Session #2: Current measurements and gaps for 5G hardware
"Anchoring TRUST" –Ophir Gaathon, DUST Identity
"Building your security house on a foundation of (virtual) Silicon" –Yousef Iskander, Microsoft
"An RF side-channel reverse engineering tool" –Stergios Papadakis, Johns Hopkins Applied Physics Laboratory
"Quantifiable assurance performed by Qualcomm" –Kabir Kasargod, Qualcomm
Breakout discussion on "Threats, Vulnerabilities, and How to Mitigate Risks"
Regroup and Report

Prior to the workshop, the steering group recruited facilitators and note-takers for the breakout sessions. Both the facilitators and the note-takers received a list of questions to guide the breakout sessions. The role of the facilitator was to stimulate the conversation and, if possible, obtain direct answers to the questions below. The role of the note-taker was to record the conversation and, if possible, identify key points for the facilitator to reflect to the group and build consensus. In addition, each attendee received a link with an online form to the questions.

On Day 1, there were 10 groups of approximately 6 people per group. Because of the relatively low number of non-NIST attendees in each session on Day 1, the working group decided to merge pairs of groups on Day 2 to give 5 groups with approximately 10 non-NIST attendees each. Discussion prompts for each of the breakout sessions are listed in Appendix B.

After each breakout session, the facilitator and note-taker reviewed the notes and generated a list of key points. At each 30-minute "Regroup and Report" the facilitator read the key points back to the moderator and attendees.

Notes from the note-takers and the steering group were condensed manually, to remove speaker's names and redundant comments. These condensed notes are recorded in Appendix C. These condensed notes, along with input from additional interviews and literature review were used to identify the themes presented in Sections 3.1 - 3.4.

Table 6. Workshop agenda, May 19th

Session #3: Innovation in measurement strategies to secure the 5G supply chain
"Welcome to day two" –Marla Dowell, NIST
"Experiences in system integrity measurement from remote attestation and TPM" –Ian Oliver, Nokia
"Hardware security: A physical inspection perspective" –Mark Tehranipoor, University of Florida
"Trusting the fingerprint: Challenges and advances in RF fingerprinting for device identification" –Kaushik Chowdhury, Northeastern University
"Supply chain security insights" –Keith Rebello, Defense Advanced Research Projects Agency
Breakout discussion on "Overlapping metrologies, New opportunities"
Regroup and Report
Session #4: Potential adoption paths for measurements in 5G hardware security
"Excerpts from IEEE PAINE 2020 and GOMAC2021" –Richard Ott, Air Force Research Laboratory
"5G/high frequency materials test challenges: Closing the gaps via E2E supply chain collaborative innovation" –Urmi Ray, International Electronics Manufacturing Initiative (iNEMI)
"RF fingerprinting via an assurance hub and new OTA characterization techniques" –Michael Schuldenfrei and Marc Vanden Bossche, NI
"Reducing the digital threat in smart manufacturing" –Sylvere Krima, NIST
Breakout discussion on "Barriers, Common ground, Shared Visions"
Regroup and Report
"Closing remarks", Paul Hale, NIST

Appendix B Discussion prompts in each of the breakout sessions

B.1 Breakout session #1: Threats, Vulnerabilities, and How to Mitigate Risks

This breakout followed the session, "**Current measurements and gaps for 5G hardware."** Each facilitator and note-taker received the following questions before breakout session #1. The note-taker posted these questions in the chat during the breakout session along with a link to a web-based form for attendees who could not participate in the live discussion.

a) What current measurements are you using in your sector? What vulnerabilities do these measurements address? How can the measurements be improved?
b) What "measurement outputs" do you want to add to improve your security posture?
c) What are the vulnerabilities that we haven't addressed today? How can they be mitigated with new or existing measurements?
d) What are the use cases where measurements could be beneficial?
e) What did we miss today?
f) Why do commercial companies care about integrity assurance? How are commercial teams different in their workflow from Defense Contractors?

B.2 Breakout session #2: Overlapping metrologies, New opportunities

This breakout followed the session, "I**nnovation in measurement strategies to secure the 5G supply chain**." Each facilitator and note-taker received the following questions before breakout session #2. The note-taker posted these questions in the chat during the breakout session along with a link to a web-based form for attendees who could not participate in the live discussion.

g) What are the intrinsic properties of 5G devices? Can we use these properties to authenticate devices in the supply chain, *e.g.*, counterfeit, and malicious hardware detection? Do they have enough variation (*e.g.*, entropy) and stability to serve as a fingerprint?
h) Are there other security applications for intrinsic properties of 5G hardware?
i) Do intrinsic properties provide a 'root-of-trust'? Where in the supply chain do we start? Can measurements in one segment be relayed to another segment? Is root-of-trust the right way to think about this?
j) At what points in the supply chain do we need to revalidate security? If at all?
k) What are some of the practical challenges of RF Fingerprinting that impair widespread industry adoption today?
l) Developing measurement techniques in a controlled lab is idealistic, but unrealistic for broad implementation. What are some approaches that might be used to manage the extra noise in production environments?
m) Related to the new Over-The-Air characterization techniques: How important is the accuracy of the electromagnetic field measurements? Are mainly magnetic fields used for RF fingerprinting in close vicinity?
n) What are the barriers (besides cost-see Q3) for implementing security measures (general)? Barriers to measurement-based security?

B.3 Breakout session #3: Barriers, Common ground, Shared visions

This breakout followed the session, "**Potential adoption paths for measurements in 5G hardware security**." Each facilitator and note-taker received the following questions before breakout session #3. The note-taker posted these questions in the chat during the breakout session along with a link to a web-based form for attendees who could not participate in the live discussion.

a) Why is Supply Chain Security important to you?
b) Who will pay for the cost of the added security? What is the incentive for industry to think about security measures? How does increasing supply chain security impact your business model?
c) Are there physical measurements, calibration methods, and artifacts, and related industry standards that could make measurement-based supply chain security practices implemented widely?
d) Are there knowledge gaps in particular measurement areas that need to be filled to make measurement-based supply chain security practices implemented widely?
e) If NIST were to champion an industry consortium that worked on measurement-based hardware security and validation strategies, what should be the key deliverables the first year? The first 3 years? Would your organization be interested in participating?

Appendix C. Discussion points from workshop

Points of discussion were captured by notetakers at the workshop[7] breakout sessions. A summary of these discussion points is captured below. Discussion points are grouped by topic rather than by breakout session.

1) **Threats, vulnerabilities, and mitigating risks to 5G hardware**
   a) **Threats**
      i) Counterfeits and malicious attacks may be very advanced and could include post-production modifications to integrated circuits and printed circuit boards
      i) We need to consider the threat model for 5G devices and create an appropriate response that can change over time.
      ii) Emerging free, open-source IP for chip making can hide or be contaminated with malicious bad code at the design stage
      iii) The blurred lines between virtualized hardware and software makes a complex landscape for security and measurements
      iv) 5G is being deployed now. What about other wireless standards, including next generation 3GPP standards and 6G?
   b) **Vulnerabilities**
      i) Insertion of design aspects that weaken system or network security
      ii) Insertion, during production, of components/aspects that weaken system or network security
      iii) Post-production insertion of components/aspects that weaken system or network security
      iv) Hardware trojans that are dormant for some period of time or trojans that are hard to detect
      v) Design theft
      vi) Flawed cryptography
      vii) Default and/or hard-coded passwords/keys
      viii) Firmware editing
      ix) Materials and components that do not support specifications
      x) 5G IoT devices are under intense pressure to reduce cost and go first to market. Replacing higher-priced OEM parts with lower-cost equivalents opens the door for security vulnerabilities.
      xi) Design manipulation
   c) **Risks**
      i) 5G, because of its many new use cases is more risky than previous generations of wireless
         1) The proliferation and connectedness of 5G+ devices make hardware security issues more complex and difficult
         2) There are so many different implementations/device types that it will be difficult to implement a uniform solution
         3) Use cases will dictate security posture; [there is a] big difference between the smart water sensor in your home vs. nuclear site vs. F-15.

[4] "Securing the 5G Supply Chain through Measurement" virtual workshop, held May 18-19, 2021.

ii) The 5G supply chain is very international and complex. No one measurement solution can be used to secure the whole chain, different measurements will be useful at various points in the supply chain
iii) What is the residual risk that industry and government must accept when balancing security with manufacturability and cost
iv) Blockchain or public ledger technologies could expose business identifiable information (how much of each component are ordered from which vendors, etc.)
v) ML algorithms can only learn from trojans already identified and in a library
vi) For FPGA's, the software on the FPGA becomes the hardware, allowing for malicious code to be hidden in the hardware

2) Measurement-based countermeasures to 5G+ hardware security

a) **Need: Why are measurements useful? How do they go beyond or complement other mitigation strategies?**
i) Commercial companies care a great deal about integrity assurance as counterfeits can cause their products to fail in the field, costing the commercial company a great deal of money
ii) Speaker said that their company only followed up on hacks if they offered something novel, implying that the volume of modified equipment was too large for them to follow up on. How many of these hacks were malicious compared with curiosity driven or do-it-yourself projects?
iii) "Can't manage what we can't measure"

b) **State-of-the-art (SOTA) and gaps: Broad overview of SOTA methods/research for validating authenticity of equipment**
i) Current security practices: focus on procurement through authorized dealers, bill of materials (BoM), and a quality control system that describes how parts are procured. What to do if parts are not acquired through authorized channels?
ii) Cryptographic hashes of software address software integrity but are limited in scope and structure.
iii) Leveraging existing techniques for counterfeit detection is important. Get current test houses involved.
iv) Multi-spectral imaging, including optical, infrared, x-ray and terahertz imaging, combined with data fusion and machine learning may be required to detect some malicious modifications
v) A digital thread of data that follows a piece of equipment from design to decommissioning could be useful
vi) How do we get the digital thread for small- to medium-sized manufacturers? How can it be made cost effective and manageable, not overwhelming?
vii) A taxonomy of vulnerabilities paired with insertion point and measurement type will be useful. This might be a starting point for standards development.
viii) Security considerations or measurements might be included in JTAG IEEE Std 1149.1.
ix) Differential power analysis/power monitoring is a "broadband"/radiation free way to monitor for compromises. Has highest SNR. Can be used for chip/circuit/PCB.

x) For chip authentication some [identification] solutions already exist, including PUFs (such as DUST), chip ID's, etc., but nothing exists for passive components
xi) RF Side-channel monitoring: Very academic currently, uses ML.

c) **Adoption and barriers: Explore how measurements can be adopted by industry & government to validate authenticity of equipment.**
i) Cost and ease of use – who pays for it, needs to be accessible to small, medium, and large suppliers
ii) Volume and variety of 5G and IoT equipment that might need to be inspected
iii) Technical issues that will need to be addressed
iv) Even if we have the how (measurements), can we still trust? To what extent do we need to quantify the risk, uncertainties, probabilities?
v) Tests may be highly technical, and staff will need to be trained

3) General topics
i) Who is responsible for which measurements?
ii) Where in the supply chain should there be measurements (key points? sampling?)
iii) How is measurement data managed in the chain of trust (between entities)
1) A secure, tamperproof mechanism to transfer test and measurement data across vendors for historical provenance
2) It is very important to collect data along the supply chain. Probably want to expand the way you look at the data to look at automated approaches to look at the supply chain.
3) Common data format would be useful
iv) Cost and time. Some customers may demand the added security and be willing to pay for it
v) Some sort of security certification (*e.g.*, EnergyStar), perhaps at certain levels, would be useful for consumers
vi) User education needed
vii) RF Fingerprinting
1) Holy Grail: RF signature that can be easily scanned and confirmed. This is a complex problem that varies on a case-by-case basis and includes consideration of risk tolerance.
2) Stability of the fingerprints with respect to aging, temperature cycling, etc.
3) Amount of data required to fingerprint may be difficult to manage
4) Measurements are much more statistical, and this makes it difficult for a certifying authority to deal with, rather than hashes of digital data
5) Fingerprinting devices is difficult due to the amount of data necessary, but manufacturers may require simple/easy deployment
6) EMI based measurements, impedance measurements, thermal measurements. We must look at all modalities and correlate them to other effects
viii) Standard Trojans
1) How can we be confident that measurements are working properly?
2) Would trojans be engineered to evade standard tests?
3) How would test capability be benchmarked? – standard trojans?
4) Does trojan need to be "On" to be detected?

4) **Machine Learning**
    i) Tracking uncertainty in measurement through to ML decision point is difficult
    ii) Could "train away" differences in performance
    iii) Need data sets, but how do we determine that they are "good" vs. having corrupted data in them?
    iv) Even if a change is detected, by *e.g.*, a scattering measurement, considerable amount of work still needed to find cause of change
    v) Data-based features vs. physics-based features
5) **Possible NIST facilitated consortium.**
    i) The consortium would need to differentiate itself from other industry efforts, such as ATIS, and a measurement focus might be the way to do this
    ii) There are existing efforts by ATIS/DOD/NSA/Homeland security
    iii) The first line of business of the group would be to agree on deliverables and a roadmap
    iv) Another goal would be to understand tools that are already being used and work with those
    v) Partner with JFAC efforts?
    vi) Partner with iNEMI? Small group to focus on a couple of use cases to create a reference implementation or baseline
    vii) There is a need for a framework/architecture/roadmap to focus efforts
    viii) Topic areas might include
        1) Standard test methods for over-the-air testing tailored to side channel diagnostics
        2) Standard reference integrated circuits and trojans for cross comparison between different measurement modalities

Appendix D. Risk assessment

A risk assessment identifies a vulnerability, the approximate likelihood that the vulnerability would be exploited by different threats, and severity of the impact of an exploit. One risk assessment method structures the assessment in the form of a risk matrix. The columns of the matrix increase from left to right in severity and have a numeric value for each column. The rows of the matrix increase from top to bottom in likelihood and have a numeric value. The values start at 1 and increase linearly to the number of rows or columns. Each vulnerability receives a score, which is the product of the severity of the impact and the approximate likelihood. Finally, the user chooses a risk tolerance value, with which to prioritize the vulnerabilities based on the score.

The first step in assessing risk in a supply chain is to identify known vulnerabilities in the supply chain. As an example, consider a collection of vulnerabilities shown abstractly in Fig. D.1a. These can include components that are susceptible to side-channel attacks, critical electronics that could include trojan integrated circuits, and more. The next step is to define the granularity of the risk matrix. In this case (Fig. D.1b), we chose three levels of severity of impact (low, medium, and high) and three levels of likelihood (low, medium, and high). In our example, all risk scores greater than 5 have an intolerable level of risk (colored red in Fig. D.1b). All risk scores more than 2 and less than 5 have a moderate level of risk (colored yellow in Fig. D.1b). All risk scores less than 2 have a tolerable level of risk (colored green in Fig. D.1b). Finally, we assigned each vulnerability a position in the risk assessment matrix (Fig. D.1c).

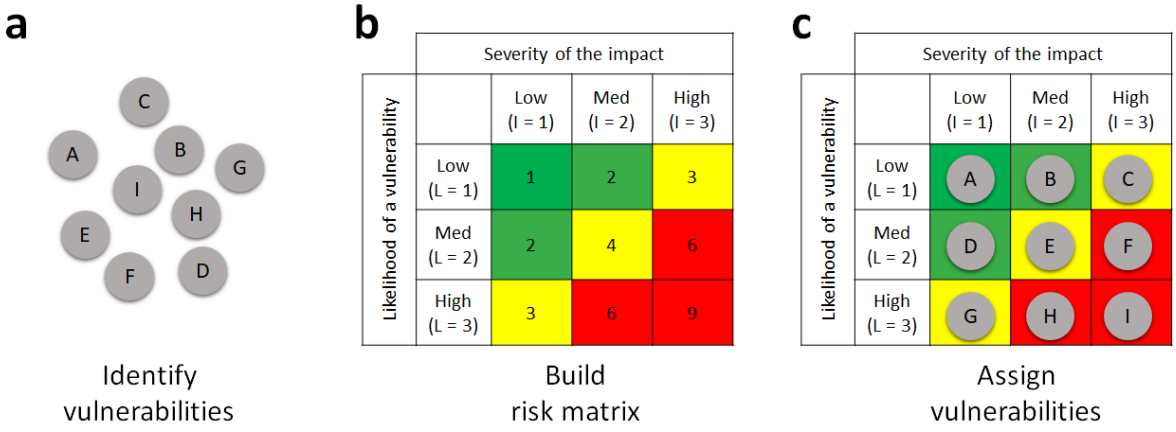

Figure D.1. Process for building a risk assessment matrix, including (a) vulnerability identification, (b) definition of risk matrix granularity, and (c) assignment of each vulnerability to a position in the risk matrix.

Measurements could reduce the likelihood that a piece of hardware with a known vulnerability would be deployed, moving the position of the vulnerability up on the risk matrix. Measurements can also create a common thread of data that connects each step in the supply chain, which may also make it more difficult for a vulnerability to go undetected. Fig. D.2 illustrates that claim that measurements change the likelihood of vulnerability and therefore decrease the total risk in the hardware supply chain.

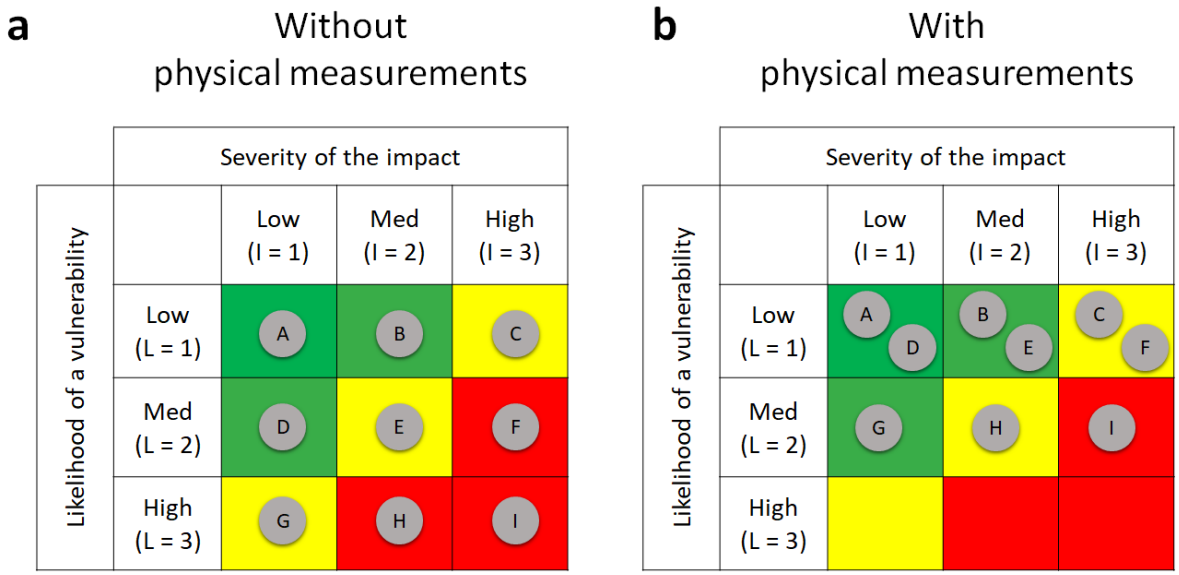

Figure D.2. Hypothetical risk matrix (a) without and (b) with measurement-based mitigation strategies.

If the measurements indeed decrease the risks, as in Fig. D.2, then adding those measurements to the hardware supply chain may be beneficial to the overall security strategy.

Appendix E. List of Acronyms

3GPP	3rd Generation Partnership Project
5G	Set of 5G specifications from 3GPP, starting with release 15
5G+	Communications using 5G and later specifications, 5G and beyond
ADC	Analog to digital converter
AES	Advanced Encryption Standard
AES	Auger Electron Spectroscopy
AFRL	Air Force Research Laboratory
ATIS	Alliance of Telecommunications Industry Solutions
AM	Acoustic Microscopy
BiCMOS	Bipolar Complimentary Metal-Oxide Semiconductor, Bipolar CMOS
BoM	Bill of Materials
CAD	Computer Assisted Design
CAM	Computer Assisted Manufacturing
CAPEC	Common Attack Pattern Enumeration and Classification
CISA	Cybersecurity and Infrastructure Security Agency
CLSM	Confocal Laser Scanning Microscopy
CNSS	Committee on National Security Systems
CTIA	Formerly the Cellular Telecommunications Industry Association
CTL	Communications Technology Laboratory
CWE	Common Weakness Enumeration
DAC	Digital to Analog Converter
DARPA	Defense Advanced Research Projects Agency
DFARS	Defense Federal Acquisition Regulation Supplement
DNA	Deoxyribonucleic acid
DoD	Department of Defense
DMSC	Digital Metrology Standards Consortium
EDA	Electronic Design and Automation
EEE	Electrical, Electronic, and Electromechanical
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Standards
GC/MS	Gas Chromatography/ Mass Spectroscopy
gNB	Next Generation NodeB, 5G base station
GSMA	GSM Association,
HOST	IEEE International Symposium on Hardware Oriented Security and Trust
IC	Integrated Circuit
ICT	Information and Communications Technology
IDEA	Independent Distributors of Electronics Association
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of Things
IIoT	Industrial Internet of Things
iNEMI	International Electronics Manufacturing Initiative
IP	intellectual property
IPC	formerly the Institute of Printed Circuits
ISO	International Organization for Standardization

ITU	International Telecommunication Union
JFAC	Joint Federated Assurance Center [25]
ML	Machine Learning
NCCoE	National Cybersecurity Center of Excellence
NESAS	Network Equipment Security Assurance Scheme
NIST	National Institute of Standards and Technology
NMI	National Metrology Institute
NSA	National Security Agency
OCM	Original component manufacturer
PAINE	IEEE International Conference on Physical Assurance and Inspection of Electronics
PCB	Printed Circuit Board
PDM	Product Data Management
PLM	Product Lifecycle Management
PUF	Physically Unclonable Function/Feature
QIF	Quality Information Framework
REME	Radiated Electromagnetic Emissions
RF	Radio Frequency
RFMLS	RF Machine Learning Systems
SAE	Society of Automotive Engineers
SEM	Scanning Electron Microscope
SI	International System of Units
SIA	Semiconductor Industry of America
SiGe	Silicon Germanium
SIMS	Secondary Ion Mass Spectroscopy
SOTA	State of the Art
SPICE	Simulation Program with Integrated Circuit Emphasis
TIA	Telecommunications Industry Association
TMA	Thermomechanical Analysis
TPM	Trusted Platform Module
UE	User Equipment
VIM	International Vocabulary of Metrology
XML	Extensible Markup Language
XPS	X-ray Photoelectron Spectroscopy

Appendix F. Glossary

acquirers	stakeholders that acquire or procure a product or service.	[40, 144]
authorized supplier	a supplier, distributor, or an aftermarket manufacturer with a contractual arrangement with, or the express written authority of, the original manufacturer or current design activity to buy, stock, repackage, sell, or distribute the part..	[50]
component	Active or passive electronic part or mechanical part intended for assembly into a circuit or system	
counterfeit	Unlawful or unauthorized reproduction, substitution, or alteration that has been knowingly mismarked, misidentified, or otherwise misrepresented to be an authentic, unmodified electronic part from the original manufacturer, or a source with the express written authority of the original manufacturer or current design activity, including an authorized aftermarket manufacturer. Unlawful or unauthorized substitution includes used electronic parts represented as new, or the false identification of grade, serial number, lot number, date code, or performance characteristics.	[46]
Fifth generation standard, 5G	Communications systems following the set of 3GPP standards, starting with Release 15.	[174]
industry	the 5G telecommunication industry suppliers, component manufacturers, component acquirers, and system integrators.	
integrator	an organization that customizes (*e.g.*, combines, adds, optimizes) elements, processes, and systems. The integrator function can be performed by acquirer, integrator, or supplier	[175]
measurand	Quantity intended to be measured	[176]
measurement	Process of experimentally obtaining one or more quantity values that can reasonably be attributed to a quantity	[176]

	NOTE 1 Measurement does not apply to nominal properties. NOTE 2 Measurement implies comparison of quantities and includes counting of entities. NOTE 3 Measurement presupposes a description of the quantity commensurate with the intended use of a measurement result, a measurement procedure, and a calibrated measuring system operating according to the specified measurement procedure, including the measurement conditions.	
measurement procedure	A detailed description of a measurement according to one or more measurement principles and to a given measurement method, based on a measurement model and including any calculation to obtain a measurement result NOTE 1 A measurement procedure is usually documented in sufficient detail to enable an operator to perform a measurement. NOTE 2 A measurement procedure can include a statement concerning a target measurement uncertainty. NOTE 3 A measurement procedure is sometimes called a standard operating procedure, abbreviated SOP.	[176]
millimeter-wave, mmWave	Formally, the definition of millimeter-wave (or mmWave) is frequencies above 30 GHz. For this document, we include all bands in Frequency range 2 of the 3GPP Specification 38.101-2. These bands are n258 (center frequency = 26 GHz), n257 (center frequency = 28 GHz), n261 (center frequency = 28 GHz), n260 (center frequency = 39 GHz), n259 (center frequency = 41 GHz)	
Provenance	The chronology of the origin, development, ownership, location, and changes to a system or system component and associated data. It may also include personnel and	[177]

	processes used to interact with or make modifications to the system, component, or associated data.	
risk	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.	[178]
risk analysis, risk assessment	The process of identifying, estimating, and prioritizing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place.	[179]
supplier	Organization or individual that enters into an agreement with the acquirer or integrator for the supply of a product or service. This includes all suppliers in the supply chain, developers or manufacturers of systems, system components, or system services; systems integrators; suppliers; product resellers; and third-party partners.	[40, 144]
threat	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability.	[179, 180]
traceability	In measurements, the ability to trace measured quantities back to the international system of units through primary or transfer standards	[176]
trust	The confidence one element has in another, that the second element will behave as expected.	[40]

trustworthiness	The interdependent combination of attributes of a person, system, or enterprise that provides confidence to others of the qualifications, capabilities, and reliability of that entity to perform specific tasks and fulfill assigned responsibilities. The degree to which a system (including the technology components that are used to build the system) can be expected to preserve the confidentiality, integrity, and availability of the information being processed, stored, or transmitted by the system across the full range of threats.	[177]
validation	confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled, the requirements were met	[181]
verification	confirmation, through the provision of objective evidence, that specified requirements have been fulfilled, the intended output is correct.	[179, 181] (adapted)
vulnerability	Weakness in a system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat.	[177]
vulnerability assessment	Systematic examination of a system or product or supply chain element to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.	[177] (adapted)

References

[1] Pecht M, Tiku S (2006) Bogus: electronic manufacturing and consumers confront a rising tide of counterfeit electronics. *IEEE Spectrum* 43(5):37–46. https://doi.org/10.1109/MSPEC.2006.1628506

[2] Crawford M, Telesco T, Nelson C, Bolton J, Bagin K, Botwin B (2010) Defense industrial base assessment: Counterfeit electronics. (U.S. Department of Commerce, Bureau of Industry and Security). Available at https://bis.doc.gov/index.php/documents/technology-evaluation/37-defense-industrial-base-assessment-of-counterfeit-electronics-2010/file

[3] Goertzel KM (2013) Integrated Circuit Security Threats and Hardware Assurance Countermeasures. *Crosstalk*:6.

[4] Guin U, Huang K, DiMase D, Carulli JM, Tehranipoor M, Makris Y (2014) Counterfeit Integrated Circuits: A Rising Threat in the Global Semiconductor Supply Chain. *Proceedings of the IEEE* 102(8):1207–1228. https://doi.org/10.1109/JPROC.2014.2332291

[5] Committee on a Strategy for Acquiring Secure and Reliable Electronic Components for Air Force Weapon Systems, Air Force Studies Board, Intelligence Community Studies Board, Division on Engineering and Physical Sciences, National Academies of Sciences, Engineering, and Medicine (2019) *The Growing Threat to Air Force Mission-Critical Electronics: Lethality at Risk: Unclassified Summary* eds Darbes S, Fuller J (National Academies Press, Washington, D.C.). https://doi.org/10.17226/25475

[6] Harrison J, Asadizanjani N, Tehranipoor M (2021) On malicious implants in PCBs throughout the supply chain. *Integration* 79:12–22. https://doi.org/10.1016/j.vlsi.2021.03.002

[7] Roy JA, Koushanfar F, Markov IL (2008) Circuit CAD tools as a security threat. *2008 IEEE International Workshop on Hardware-Oriented Security and Trust* (IEEE, Anaheim, CA, USA), pp 65–66. https://doi.org/10.1109/HST.2008.4559052

[8] Alkabani Y, Koushanfar F (2008) Designer's hardware Trojan horse. *2008 IEEE International Workshop on Hardware-Oriented Security and Trust* (IEEE, Anaheim, CA, USA), pp 82–83. https://doi.org/10.1109/HST.2008.4559059

[9] Contreras GK, Nahiyan A, Bhunia S, Forte D, Tehranipoor M (2017) Security vulnerability analysis of design-for-test exploits for asset protection in SoCs. *2017 22nd Asia and South Pacific Design Automation Conference (ASP-DAC)* (IEEE, Chiba, Japan), pp 617–622. https://doi.org/10.1109/ASPDAC.2017.7858392

[10] He J, Guo X, Tehranipoor M, Vassilev A, Jin Y (2021) EM Side Channels in Hardware Security: Attacks and Defenses. *IEEE Design & Test*:1–1. https://doi.org/10.1109/MDAT.2021.3135324

[11] Tsalis N, Vasilellis E, Mentzelioti D, Apostolopoulos T (2019) A Taxonomy of Side Channel Attacks on Critical Infrastructures and Relevant Systems. *Critical Infrastructure Security and Resilience*, Advanced Sciences and Technologies for Security Applications., eds Gritzalis D, Theocharidou M, Stergiopoulos G (Springer International Publishing, Cham), pp 79–96. https://doi.org/10.1007/978-3-030-00024-0_5

[12] Quadir SE, Chen J, Forte D, Asadizanjani N, Shahbazmohamadi S, Wang L, Chandy J, Tehranipoor M (2016) A Survey on Chip to System Reverse Engineering. *ACM Journal on Emerging Technologies in Computing Systems* 13(1):1–34. https://doi.org/10.1145/2755563

[13] Secure and trusted communications act of 2019-116publ124.pdf (2020) , Public Law 116-124, Chapter 116. Available at https://www.congress.gov/bill/116th-congress/house-bill/4998/text

[14] Schipp F (2021) Trends in Counterfeit Electronic Parts – A Data-Driven Analysis. *Conference on Counterfeit Parts and Materials* (Virtual Symposium).

[15] Ashoor EA (2010) Saudi citizen found guilty of selling counterfeit Cisco computer parts to the marine Corps in Iraq. Available at https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2012/03/15/ashoorGuilty.pdf

[16] Tehranipoor MM, Guin U, Bhunia S (2017) Invasion of the hardware snatchers. *IEEE Spectrum* 54(5):36–41. https://doi.org/10.1109/MSPEC.2017.7906898

[17] U.S. Department of Justice Florida Man Charged in Federal Counterfeit Case for Trafficking Bogus Automotive Devices 'Reverse Engineered' in China. Available at https://archives.fbi.gov/archives/losangeles/press-releases/2014/florida-man-charged-in-federal-counterfeit-case-for-trafficking-bogus-automotive-devices-reverse-engineered-in-china

[18] U.S. Department of Homeland Security (2012) HSI dismantles counterfeit cell phone operation, 3 arrested. Available at https://www.ice.gov/news/releases/hsi-dismantles-counterfeit-cell-phone-operation-3-arrested

[19] U.S. Customs and Border Patrol (2021) 542 Fake iPhones Seized by Cincinnati CBP. Available at https://www.cbp.gov/newsroom/local-media-release/542-fake-iphones-seized-cincinnati-cbp

[20] Bastia S (2002) Next generation technologies to combat counterfeiting of electronic components. *IEEE Transactions on Components and Packaging Technologies* 25(1):175–176. https://doi.org/10.1109/6144.991192

[21] Adee S (2008) The Hunt For The Kill Switch. *IEEE Spectrum* 45(5):34–39. https://doi.org/10.1109/MSPEC.2008.4505310

[22] Defense Science Board Task Force on High Performance Microchip Supply (2005) Available at https://apps.dtic.mil/sti/citations/ADA435563

[23] OECD (2018) *Governance Frameworks to Counter Illicit Trade* (OECD). https://doi.org/10.1787/9789264291652-en

[24] DMEA Trusted IC Program Available at https://www.dmea.osd.mil/TrustedIC.aspx

[25] Joint Federated Assurance Center (JFAC) Available at https://rt.cto.mil/stpe/rs/jfac/

[26] Gold RA (2016) Long-term strategy of DoD trusted foundry needs. Available at https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fwww.navsea.navy.mil%2FPortals%2F103%2FDocuments%2FNSWC_Crane%2FMIM%2FTrusted%2520Foundry%2520Long-Term%2520Strategy_Gold.pptx%3Fver%3D2016-08-08-144912-137&wdOrigin=BROWSELINK

[27] Casto M (2020) Trusted and Assured Microelectronics Program, Presentation to U. S. Government Inter-Agency Semiconductor Leadership Working Group.

[28] Fang D, Qian Y, Hu RQ (2018) Security for 5G Mobile Wireless Networks. *IEEE Access* 6:4850–4874. https://doi.org/10.1109/ACCESS.2017.2779146

[29] Government-University-Industry Research Roundtable, Policy and Global Affairs, National Academies of Sciences, Engineering, and Medicine (2019) *The Transformational Impact of 5G: Proceedings of a Workshop in Brief* ed Saunders J (National Academies Press, Washington, D.C.). https://doi.org/10.17226/25598

[30] Network slicing for 5G networks & services (2016) Available at https://www.5gamericas.org/wp-content/uploads/2019/07/5G_Americas_Network_Slicing_11.21_Final.pdf

[31] Ding AY, Janssen M (2018) Opportunities for applications using 5G networks: requirements, challenges, and outlook. *Proceedings of the Seventh International Conference on Telecommunications and Remote Sensing* (ACM, Barcelona Spain), pp 27–34. https://doi.org/10.1145/3278161.3278166

[32] 5G services & use cases (2017) Available at https://www.5gamericas.org/5g-services-use-cases/

[33] Campbell K, Diffley J, Flanagan B, Morelli B, O'Neil B (2017) The 5G economy: How 5G technology will contribute to the global economy. (IHS ECONOMICS & IHS TECHNOLOGY). Available at https://www.qualcomm.com/media/documents/files/ihs-5g-economic-impact-study.pdf

[34] Potential Threat Vectors to 5G Infrastructure, p 16. Available at https://www.cisa.gov/sites/default/files/publications/potential-threat-vectors-5G-infrastructure_508_v2_0%20%281%29.pdf

[35] Ahmad I, Kumar T, Liyanage M, Okwuibe J, Ylianttila M, Gurtov A (2018) Overview of 5G Security Challenges and Solutions. *IEEE Communications Standards Magazine* 2(1):36–43. https://doi.org/10.1109/MCOMSTD.2018.1700063

[36] CISA Overview of Risks Introduced by 5G Adoption in the United States. Critical Infrastructure Security and Resilience Note. (U.S. Department of Homeland Security), p 16. Available at https://www.cisa.gov/sites/default/files/publications/19_0731_cisa_5th-generation-mobile-networks-overview_0.pdf

[37] CISA 5G Strategy: Ensuring the security and resilience of 5G infrastructure in Our Nation (2020) (U.S. Department of Homeland Security, CISA).

[38] Franklin J, Bowler K, Brown C, Dog SE, Edwards S, McNab N, Steele M (2019) Mobile device security: cloud and hybrid builds. (National Institute of Standards and Technology, Gaithersburg, MD), NIST SP 1800-4, p NIST SP 1800-4. https://doi.org/10.6028/NIST.SP.1800-4

[39] Scarfone K, Cybersecurity S (2021) 5G Cybersecurity Volume A: Executive Summary Preliminary Draft. NIST Special Publication., 1800–33A, p 4. Available at https://www.nccoe.nist.gov/5g-cybersecurity

[40] Boyens J (2021) (Draft) Supply Chain Risk Management Practices for Federal Information Systems and Organizations: Revision 1. https://doi.org/10.6028/NIST.SP.800-161r1-draft

[41] Diamond T, Grayson N, Polk WT, Regenscheid A, Souppaya M, Scarfone K (2021) Validating the Integrity of Computing Devices Volume A: Executive Summary. NIST Special Publication., 1800–34A, p 4. Available at https://www.nccoe.nist.gov/sites/default/files/legacy-files/nist-sp1800-34a-tpm-sca-preliminary-draft.pdf

[42] Diamond T, Grayson N, Polk WT, Regenscheid A, Sou[[aya M, Scarfone K, Brown C (2021) Validating the Integrity of Computing Devices Volume B: Approach, Architecture, and Security Characteristics. NIST Special Publication., 1800–34B, p 61. Available at https://www.nccoe.nist.gov/sites/default/files/legacy-files/tpm-sca-nist-sp1800-34b-preliminary-draft.pdf

[43] Diamond T, Grayson N, Polk WT, Regenscheid A, Souppaya M, Brown C, Deane C, Scarfone K (2021) Validating the Integrity of Computing Devices Volume C: How-to Guides. NIST Special Publication., 1800–34C, p 125. Available at https://www.nccoe.nist.gov/sites/default/files/2021-11/sca-nist-sp-1800-34c-preliminary-draft.pdf

[44] ISO/TC 176/SC 2 (2015) ISO 9001:2015 Quality management systems — Requirements. Available at https://www.iso.org/standard/62085.html

[45] AS5553 Rev. C, Counterfeit electrical, electronic, and electromechanical (EEE) parts; Avoidance, detection, mitigation, and disposition (2019) Available at https://www.sae.org/standards/content/as5553c/

[46] DFARS 252.246-7007 Contractor Counterfeit Electronic Part Detection and Avoidance System. Available at https://www.acquisition.gov/dfars/252.246-7007-contractor-counterfeit-electronic-part-detection-and-avoidance-system.

[47] JESD243A, Counterfeit electronic parts: Non-proliferation for manufacturers (2021) Available at https://www.jedec.org/standards-documents/docs/jesd243

[48] ITU-T-REC-Q.5050 Combating counterfeiting and stolen ICT devices: Framework for solutions to combat counterfeit ICT devices (2019) Available at https://www.itu.int/rec/T-REC-Q.5050-201903-I/en

[49] G-19A Test Laboratory Standards Development Committee (2016) Test Methods Standard; General Requirements, Suspect/Counterfeit, Electrical, Electronic, and Electromechanical Parts: AS6171A.

[50] DFARS 252.246-7008 Sources of Electronic Parts. Available at https://www.acquisition.gov/dfars/252.246-7008-sources-electronic-parts.

[51] ATIS-I-0000087, ATIS 5G supply chain standard: Creating the foundation for assured 5G networks (2021) Available at https://access.atis.org/apps/group_public/download.php/61541/ATIS-I-0000087.pdf

[52] IPC-1782A, Standard for Manufacturing and Supply Chain Traceability of Electronic Products (2020) Available at https://shop.ipc.org/general-electronics/standards/1782-0-a-english

[53] Government-industry data exchange program (GIDEP) Available at https://www.gidep.org/data/cft/cft.htm

[54] ERAI Available at https://www.erai.com/

[55] G-19A Test Laboratory Standards Development Committee (2017) AS6171/2A Techniques for Suspect/Counterfeit EEE Parts Detection by External Visual Inspection, Remarking and Resurfacing, and Surface Texture Analysis Using SEM Test Methods. Available at https://saemobilus.sae.org/content/as6171/2a

[56] IDEA-STD-1010-B, Acceptability of electronic components distributed in the open market (2011) Available at https://idofea.org/idea-std-1010-inspection-standard.html

[57] G-19A Test Laboratory Standards Development Committee Techniques for Suspect/Counterfeit EEE Parts Detection by Delid/Decapsulation Physical Analysis Test Methods. (SAE International). https://doi.org/10.4271/AS6171/4

[58] G-19A Test Laboratory Standards Development Committee Techniques for Suspect/Counterfeit EEE Parts Detection by Radiological Test Methods. (SAE International). https://doi.org/10.4271/AS6171/5

[59] G-19a Test Laboratory Standards Development Committee (2017) Techniques for Suspect/Counterfeit EEE Assembly Detection by Various Test Methods AS6171/23. Available at https://www.sae.org/standards/content/as6171/23

[60] Winning the battle against counterfeit semiconductor products: A report of the SIA anti-counterfeiting task force (2013) Available at https://www.semiconductors.org/wp-content/uploads/2018/06/SIA-Anti-Counterfeiting-Whitepaper-1.pdf

[61] G-19A Test Laboratory Standards Development Committee Techniques for Suspect/Counterfeit EEE Parts Detection by Electrical Test Methods. (SAE International). https://doi.org/10.4271/AS6171/7

[62] G-19A Test Laboratory Standards Development Committee Techniques for Suspect/Counterfeit EEE Parts Detection by Fourier Transform Infrared Spectroscopy (FTIR) Test Methods. (SAE International). https://doi.org/10.4271/AS6171/9

[63] G-19A Test Laboratory Standards Development Committee Techniques for Suspect/Counterfeit EEE Parts Detection by Raman Spectroscopy Test Methods. (SAE International). https://doi.org/10.4271/AS6171/8

[64] G-19A Test Laboratory Standards Development Committee Techniques for Suspect/Counterfeit EEE Parts Detection by Thermogravimetric Analysis (TGA) Test Methods. (SAE International). https://doi.org/10.4271/AS6171/10

[65] G-19A Test Laboratory Standards Development Committee Techniques for Suspect/Counterfeit EEE Parts Detection by X-ray Fluorescence Test Methods. (SAE International). https://doi.org/10.4271/AS6171/3

[66] G-19A Test Laboratory Standards Development Committee Techniques for Suspect/Counterfeit EEE Parts Detection by Acoustic Microscopy (AM) Test Methods. (SAE International). https://doi.org/10.4271/AS6171/6

[67] G-19A Test Laboratory Standards Development Committee Techniques for Suspect/Counterfeit EEE Parts Detection by Design Recovery Test Methods. (SAE International). https://doi.org/10.4271/AS6171/11

[68] Principe EL, Asadizanjani N, Forte D, Tehranipoor M, Chivas R, DiBattista M, Silverman S, Marsh M, Piche N, Mastovich J (2017) Steps Toward Automated Deprocessing of Integrated Circuits. (Pasadena, California, USA), pp 285–298. https://doi.org/10.31399/asm.cp.istfa2017p0285

[69] Feng H, Tan PK, Yap HH, Low GR, He R, Zhao YZ, Liu B, Dawood MK, Zhu J, Huang YM, Wang DD, Tan H, Lam J, Mai ZH (2015) A sample preparation methodology to reduce sample edge unevenness and improve efficiency in delayering

the 20-nm node IC chips. *2015 IEEE 22nd International Symposium on the Physical and Failure Analysis of Integrated Circuits* (IEEE, Hsinchu), pp 459–464. https://doi.org/10.1109/IPFA.2015.7224432

[70] Goldstein J, et al. (2018) *Scanning Electron Microscopy and X-Ray Microanalysis* (Springer), 4th Ed.

[71] Long Term Storage of Electronic Devices GEIA-STD-0003A Available at https://www.sae.org/standards/content/geiastd0003a/

[72] *Proceedings of the IEEE Conference on Physical Assurance and Inspection of Electronics (PAINE)*. Available at https://ieeexplore.ieee.org/xpl/conhome/1840106/all-proceedings

[73] IEEE International Symposium on Hardware Oriented Security and Trust (HOST): Past, Present, and Future *Proceedings of the IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*. Available at https://ieeexplore.ieee.org/document/9000111

[74] Attacks and Solutions in Hardware Security (ASHES) *Attacks and Solutions in Hardware Security (ASHES)*. Available at http://ashesworkshop.org/

[75] Symposium on Counterfeit Parts and Materials *Symposium on Counterfeit Parts and Materials*. Available at https://smta.org/mpage/counterfeit/

[76] FICS Research Conference *FICS Research Conference*. Available at http://fics.institute.ufl.edu/index.php/outreach/conferences/

[77] Bhunia S, Tehranipoor M (2019) *Hardware security: A hands on learning approach* (Elsevier, Cambridge, Ma).

[78] Part 12 - Acquisition of Commercial Products and Commercial Services *Part 12 - Acquisition of Commercial Products and Commercial Services*. Available at https://www.acquisition.gov/far/part-12#FAR_Part_12

[79] FAR 46.317 Reporting nonconforming items *FAR 46317 Reporting nonconforming items*. Available at https://www.acquisition.gov/far/46.317#FAR_46_317

[80] Mehta D, Lu H, Paradis OP, M. S. MA, Rahman MT, Iskander Y, Chawla P, Woodard DL, Tehranipoor M, Asadizanjani N (2020) The Big Hack Explained: Detection and Prevention of PCB Supply Chain Implants. *ACM Journal on Emerging Technologies in Computing Systems* 16(4):1–25. https://doi.org/10.1145/3401980

[81] Menon N (2021) Machine learning and machine vision systems for microelectronic screening. *Conference on Counterfeit Parts and Materials* (Virtual Symposium).

[82] Holler M, Odstrcil M, Guizar-Sicairos M, Lebugle M, Müller E, Finizio S, Tinti G, David C, Zusman J, Unglaub W, Bunk O, Raabe J, Levi AFJ, Aeppli G (2019) Three-

dimensional imaging of integrated circuits with macro- to nanoscale zoom. *Nature Electronics* 2(10):464–470. https://doi.org/10.1038/s41928-019-0309-z

[83] Kim FH, Pintar A, Obaton A-F, Fox J, Tarr J, Donmez A (2021) Merging experiments and computer simulations in X-ray Computed Tomography probability of detection analysis of additive manufacturing flaws. *NDT & E International* 119:102416. https://doi.org/10.1016/j.ndteint.2021.102416

[84] Burford NM, El-Shenawee M, O'Neal CB, Olejniczak KJ (2014) Terahertz Imaging for Nondestructive Evaluation of Packaged Power Electronic Devices. *International Journal of Emerging Technology and Advanced Engineering* 4(1):395–401.

[85] Baldini G, Steri G (2017) A Survey of Techniques for the Identification of Mobile Phones Using the Physical Fingerprints of the Built-In Components. *IEEE Communications Surveys & Tutorials* 19(3):1761–1789. https://doi.org/10.1109/COMST.2017.2694487

[86] Kaplan D, Stanhope DM (1999) U.S. Patent 5 99 980 6A,Waveform collection for use in wireless telephone identification.

[87] Remley KA, Grosvenor CA, Johnk RT, Novotny DR, Hale PD, McKinley MD, Karygiannis A, Antonakakis E (2005) Electromagnetic signatures of WLAN cards and network security. *Proceedings of the Fifth IEEE International Symposium on Signal Processing and Information Technology, 2005.* (IEEE, Athens, Greece), pp 484–488. https://doi.org/10.1109/ISSPIT.2005.1577145

[88] Brik V, Banerjee S, Gruteser M, Oh S (2008) Wireless device identification with radiometric signatures. *Proceedings of the 14th ACM International Conference on Mobile Computing and Networking - MobiCom '08* (ACM Press, San Francisco, California, USA), p 116. https://doi.org/10.1145/1409944.1409959

[89] Suski II WC, Temple MA, Mendenhall MJ, Mills RF (2008) Using Spectral Fingerprints to Improve Wireless Network Security. *IEEE GLOBECOM 2008 - 2008 IEEE Global Telecommunications Conference* (IEEE, New Orleans, LA, USA), pp 1–5. https://doi.org/10.1109/GLOCOM.2008.ECP.421

[90] Xu Q, Zheng R, Saad W, Han Z (2016) Device Fingerprinting in Wireless Networks: Challenges and Opportunities. *IEEE Communications Surveys & Tutorials* 18(1):94–104. https://doi.org/10.1109/COMST.2015.2476338

[91] Ur Rehman S, Sowerby KW, Chong PHJ, Alam S (2017) Robustness of radiometric fingerprinting in the presence of an impersonator. *2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)* (IEEE, Montreal, QC), pp 1–5. https://doi.org/10.1109/PIMRC.2017.8292279

[92] Reus-Muns G, Jaisinghani D, Sankhe K, Chowdhury KR (2020) Trust in 5G Open RANs through Machine Learning: RF Fingerprinting on the POWDER PAWR

Platform. *GLOBECOM 2020 - 2020 IEEE Global Communications Conference* (IEEE, Taipei, Taiwan), pp 1–6. https://doi.org/10.1109/GLOBECOM42002.2020.9348261

[93] Soltanieh N, Norouzi Y, Yang Y, Karmakar NC (2020) A Review of Radio Frequency Fingerprinting Techniques. *IEEE Journal of Radio Frequency Identification* 4(3):222–233. https://doi.org/10.1109/JRFID.2020.2968369

[94] Jian T, Rendon BC, Ojuba E, Soltani N, Wang Z, Sankhe K, Gritsenko A, Dy J, Chowdhury K, Ioannidis S (2020) Deep Learning for RF Fingerprinting: A Massive Experimental Study. *IEEE Internet of Things Magazine* 3(1):50–57. https://doi.org/10.1109/IOTM.0001.1900065

[95] Davies J Radio fingerprinting machine learning systems (RFMLS). Available at https://www.darpa.mil/program/radio-frequency-machine-learning-systems

[96] Wang N, Li W, Wang P, Alipour-Fanid A, Jiao L, Zeng K (2020) Physical Layer Authentication for 5G Communications: Opportunities and Road Ahead. *IEEE Network* 34(6):198–204. https://doi.org/10.1109/MNET.011.2000122

[97] Sankhe K, Restuccia F, D'Oro S, Jian T, Wang Z, Al-Shawabka A, Dy J, Melodia T, Ioannidis S, Chowdhury K (2019) Impairment Shift Keying: Covert Signaling by Deep Learning of Controlled Radio Imperfections. *MILCOM 2019 - 2019 IEEE Military Communications Conference (MILCOM)* (IEEE, Norfolk, VA, USA), pp 598–603. https://doi.org/10.1109/MILCOM47813.2019.9021079

[98] Sankhe K, Belgiovine M, Zhou F, Riyaz S, Ioannidis S, Chowdhury K (2019) ORACLE: Optimized Radio classification through convolutional neuraL networks. *IEEE INFOCOM 2019 - IEEE Conference on Computer Communications* (IEEE, Paris, France), pp 370–378. https://doi.org/10.1109/INFOCOM.2019.8737463

[99] Al-Shawabka A, Restuccia F, D'Oro S, Jian T, Costa Rendon B, Soltani N, Dy J, Ioannidis S, Chowdhury K, Melodia T (2020) Exposing the Fingerprint: Dissecting the Impact of the Wireless Channel on Radio Fingerprinting. *IEEE INFOCOM 2020 - IEEE Conference on Computer Communications* (IEEE, Toronto, ON, Canada), pp 646–655. https://doi.org/10.1109/INFOCOM41043.2020.9155259

[100] Huang Y, Zheng H (2015) Theoretical performance analysis of radio frequency fingerprinting under receiver distortions: Radio frequency fingerprinting under receiver distortions. *Wireless Communications and Mobile Computing* 15(5):823–833. https://doi.org/10.1002/wcm.2386

[101] Accredited Standards Committee C63® (2014) ANSI C63.4-2014, American National Standard for Methods of Measurement of Radio-Noise Emissions from Low-Voltage Electrical and Electronic Equipment in the Range of 9 kHz to 40 GHz. Available at https://doi.org/10.1109/IEEESTD.2014.6840852

[102] Remley KA, Young WF (2013) Test methods for RF-based electronic safety equipment: Part 2 — Development of laboratory-based tests. *IEEE Electromagnetic Compatibility Magazine* 2(1):70–80. https://doi.org/10.1109/MEMC.2013.6512222

[103] Bezawada B, Bachani M, Peterson J, Shirazi H, Ray I, Ray I (2018) Behavioral Fingerprinting of IoT Devices. *Proceedings of the 2018 Workshop on Attacks and Solutions in Hardware Security* (ACM, Toronto Canada), pp 41–50. https://doi.org/10.1145/3266444.3266452

[104] Agrawal D, Baktir S, Karakoyunlu D, Rohatgi P, Sunar B (2007) Trojan Detection using IC Fingerprinting. *2007 IEEE Symposium on Security and Privacy (SP '07)* (IEEE, Berkeley, CA), pp 296–310. https://doi.org/10.1109/SP.2007.36

[105] Liu Y, Huang K, Makris Y Hardware Trojan Detection through Golden Chip-Free Statistical Side-Channel Fingerprinting. 6.

[106] Hasegawa K, Chikamatsu K, Togawa N (2019) Empirical Evaluation on Anomaly Behavior Detection for Low-Cost Micro-Controllers Utilizing Accurate Power Analysis. *2019 IEEE 25th International Symposium on On-Line Testing and Robust System Design (IOLTS)* (IEEE, Rhodes, Greece), pp 54–57. https://doi.org/10.1109/IOLTS.2019.8854456

[107] Tinsley L, Liu H, Addepalli S, Lam W, Zhao Y (2020) Inspection of electronic component using pulsed thermography. *Procedia Manufacturing* 49:132–138. https://doi.org/10.1016/j.promfg.2020.07.008

[108] Hale P (2021) NIST workshop on measurement-based approaches to 5G supply chain security. *Securing the 5G Supply Chain through Measurement* (NIST virtual workshop).

[109] Hale P (2021) SI traceability for 5G hardware authentication. *IEEE Physical Assurance and Inspection of Electronics (PAINE)* (Virtual Conference).

[110] Foran B (2021) Evaluating the effectiveness of 2OE methods to mitigate specific risks. *Symposium on Counterfeit Parts and Materials* (Virtual Symposium).

[111] Ott R, McCue J, Eakins C, Bohman C, Skouson M, Jennings A, Duncan L, DiSabato D, Tribble J, Lachey R, Hansen B, Stanley J, Summers J (2021) Evaluation of second order effect system performance based on standardized test articles and a common metric. (AFRL), AFRL-RY-WP-TR-2021-0065, p 326.

[112] Ott R (2020) Assurance-From integrated circuits to printed circuits. *IEEE Physical Assurance and Inspection of Electronics (PAINE)* (Virtual Conference).

[113] Ott R (2021) Excerpts from IEEE PAINE 2020 and GOMAC 2021. *Securing the 5G Supply Chain through Measurement* (NIST virtual workshop).

[114] G-19a Test Laboratory Standards Development Committee (2015) Techniques for suspect/counterfeit EEE parts detection of capacitors by acoustic microscopy (AM) test methods AS6171/12. Available at https://www.sae.org/standards/content/as6171/12/

[115] G-19a Test Laboratory Standards Development Committee (2015) Technique for Suspect/Counterfeit EEE Parts Detection by Secondary Ion Mass Spectrometry (SIMS) Test Methods AS6171/13. Available at https://www.sae.org/standards/content/as6171/13

[116] G-19a Test Laboratory Standards Development Committee (2016) Techniques for suspect/counterfeit EEE parts detection by radiated electromagnetic emission (REME) analysis test methods AS6171/14.

[117] G-19a Test Laboratory Standards Development Committee (2016) Techniques for Suspect/Counterfeit EEE Parts Detection by Netlist Assurance Test Methods AS6171/16. Available at https://www.sae.org/standards/content/as6171/16

[118] G-19a Test Laboratory Standards Development Committee (2015) Technique for Suspect/Counterfeit EEE Parts Detection by Laser Scanning Microscopy (LSM) and Confocal Laser Scanning Microscopy (CLSM) Test Methods AS6171/17. Available at https://www.sae.org/standards/content/as6171/17

[119] G-19a Test Laboratory Standards Development Committee (2016) Techniques for Suspect/Counterfeit EEE Parts Detection by Thermomechanical Analysis (TMA) Test Methods AS6171/18. Available at https://www.sae.org/standards/content/as6171/18

[120] G-19a Test Laboratory Standards Development Committee (2016) Techniques for Suspect/Counterfeit EEE Parts Detection by Auger Electron Spectroscopy (AES) Test Method AS6171/19. Available at https://www.sae.org/standards/content/as6171/19

[121] G-19a Test Laboratory Standards Development Committee (2016) Techniques for Suspect/Counterfeit EEE Parts Detection by X-Ray Photoelectron Spectroscopy (XPS) Test Method AS6171/20. Available at https://www.sae.org/standards/content/as6171/20

[122] Techniques for Suspect/Counterfeit EEE Parts Detection by Gas Chromatography/Mass Spectrometry (GC/MS) Test Methods AS6171/21 (2016) Available at https://www.sae.org/standards/content/as6171/21

[123] G-19a Test Laboratory Standards Development Committee (2017) Technique for Suspect/Counterfeit EEE Parts Detection by Scanning Electron Microscopy (SEM) including Energy Dispersive X-Ray Spectroscopy Test Methods AS6171/22. Available at https://www.sae.org/standards/content/as6171/22

[124] G-21b, Counterfeit And Substandard Battery Risk Mitigation (2018) Counterfeit and Substandard Battery Risk Mitigation AS7492. Available at https://www.sae.org/standards/content/as7492/#:~:text=Counterfeit%20and%20Substandard%20Battery%20Risk%20Mitigation%20AS7492%20The,significant%20risk%20presented%20by%20counterfeit%20and%20substandard%20batteries.

[125] Ruhrmair U, Holcomb DE (2014) PUFs at a glance. *Design, Automation & Test in Europe Conference & Exhibition (DATE), 2014* (IEEE Conference Publications, Dresden, Germany), pp 1–6. https://doi.org/10.7873/DATE.2014.360

[126] Bauer T, Hamlet J (2014) Physical Unclonable Functions: A Primer. *IEEE Security & Privacy* 12(6):97–101. https://doi.org/10.1109/MSP.2014.123

[127] Sharief SA, Chahal P, Alocilja E (2021) Application of DNA sequences in anti-counterfeiting: Current progress and challenges. *International Journal of Pharmaceutics* 602:120580. https://doi.org/10.1016/j.ijpharm.2021.120580

[128] Gaathon O, Hodges J (2020) U.S. Patent US 10 685 199 B2, Generating a unique code from orientation information.

[129] Dey K, Kule M, Rahaman H (2021) PUF Based Hardware Security: A Review. *2021 International Symposium on Devices, Circuits and Systems (ISDCS)* (IEEE, Higashihiroshima, Japan), pp 1–6. https://doi.org/10.1109/ISDCS52006.2021.9397896

[130] Awano H, Iizuka T, Ikeda M (2019) PUFNet: A Deep Neural Network Based Modeling Attack for Physically Unclonable Function. *2019 IEEE International Symposium on Circuits and Systems (ISCAS)* (IEEE, Sapporo, Japan), pp 1–4. https://doi.org/10.1109/ISCAS.2019.8702431

[131] Kuhn DR, Raunak MS, Prado C, Patil VC, Kacker RN (2022) Combination Frequency Differencing for Identifying Design Weaknesses in Physical Unclonable Functions. *IEEE Intl Conf on Software Testing, Verification and Validation Workshops (ICSTW)*, p 8.

[132] NCCoE, National Cybersecurity Center of Excellence Available at https://www.nccoe.nist.gov/

[133] NCCoE: 5G Cybersecurity Available at https://www.nccoe.nist.gov/5g-cybersecurity

[134] GSMA Association (2021) Network Equipment Security Assurance Scheme - Overview Version 2.0-Overview-v2.0. Available at https://www.gsma.com/security/wp-content/uploads/2021/02/FS.13-NESAS-Overview-v2.0.pdf

[135] GSMA Association (2021) Network Equipment Security Assurance Scheme Security Test Laboratory Accreditation Version 2.0. Available at https://www.gsma.com/security/wp-content/uploads/2021/02/FS.14-NESAS-Security-Test-Laboratory-Accreditation-v2.0.pdf

[136] GSMA Association (2021) Network Equipment Security Assurance Scheme Development and Lifecycle Security Requirements Version 2.0. Available at https://www.gsma.com/security/wp-content/uploads/2021/02/FS.16-NESAS-Development-and-Lifecycle-Security-Requirements-v2.0.pdf

[137] Network Equipment Security Assurance Scheme - Development and Lifecycle Assessment Methodology Version 2.0 (2021) Available at https://www.gsma.com/security/wp-content/uploads/2021/02/FS.15-NESAS-Development-and-Lifecycle-Assessment-Methodology-v2.0.pdf

[138] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Security Assurance Methodology (SCAS) for 3GPP network products (Release 16), 3GPP TR 33.916 V16.0.0 (2020-07) Available at https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2270

[139] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Catalogue of general security assurance requirements (Release 17), 3GPP TS 33.117 V17.0.0 (2021-06) Available at https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2928

[140] GSMA coordinated vulnerability disclosure programme Available at https://www.gsma.com/security/gsma-coordinated-vulnerability-disclosure-programme/

[141] CTIA Certification home page Available at https://ctiacertification.org/

[142] About SCS 9001: Supply chain security standard Available at https://tiaonline.org/what-we-do/scs-9001-supply-chain-security-standard/

[143] Veras A, Varadarajan R, Goodrich J, Yinug F (2021) Strengthening the global semiconductor supply chain in an uncertain era. Available at https://www.semiconductors.org/wp-content/uploads/2021/05/BCG-x-SIA-Strengthening-the-Global-Semiconductor-Value-Chain-April-2021_1.pdf

[144] ISO/IEC/IEEE 15288-2015 Systems and software engineering - System life cycle processes Available at https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7106435

[145] Rebello K (2019) Supply chain vulnerabilities. *FIOCS Research Annual Conference on Cybersecurity*

[146] Common weakness enumeration Available at https://cwe.mitre.org/

[147] Guin U, DiMase D, Tehranipoor M (2014) A Comprehensive Framework for Counterfeit Defect Coverage Analysis and Detection Assessment. *Journal of Electronic Testing* 30(1):25–40. https://doi.org/10.1007/s10836-013-5428-2

[148] Metz CE (1978) Basic principles of ROC analysis. *Seminars in Nuclear Medicine* 8(4):283–298. https://doi.org/10.1016/S0001-2998(78)80014-2

[149] Tehranipoor MM (2022) State of Hardware/Microelectronics Security.

[150] Shakya B, He T, Salmani H, Forte D, Bhunia S, Tehranipoor M (2017) Benchmarking of Hardware Trojans and Maliciously Affected Circuits. *Journal of Hardware and Systems Security* 1(1):85–102. https://doi.org/10.1007/s41635-017-0001-6

[151] Hastie T, Tibshirani R, Friedman J *The elements of statistical learning: Data mining, inference, and prediction* (Springer), 2nd Ed.

[152] Goodfellow I, Bengio Y, Courville A (2016) *Deep Learning* (MIT Press).

[153] G-19A Test Laboratory Standards Development Committee (2016) AS 6171/1 Suspect/Counterfeit Test Evaluation Method. Available at https://saemobilus.sae.org/content/AS6171/1/

[154] ISO 9001:2015(en) Quality management systems — Requirements (2015) Available at https://www.iso.org/standard/62085.html

[155] ISO 22514-2:2017 Statistical methods in process management — Capability and performance — Part 2: Process capability and performance of time-dependent process models (2017) Available at https://www.iso.org/standard/71617.html?browse=tc

[156] IPC-2591-Version 1.4, Connected Factory Exchange (CFX) (2022) Available at https://www.ipc.org/ipc-2591-connected-factory-exchange-cfx

[157] IPC-1756(D)F, Manufacturing Process Data Management (2010) Available at https://shop.ipc.org/document-numbers/ipc-1756

[158] Quality information framework (QIF): Unified XML framework standard for CAD quality measurement systems Available at https://qifstandards.org

[159] IPC-WP-026, IPC Technology Solutions White Paper on Blockchain and the Electronics Industry: A Review of the Current State of Blockchain Technology and Its Potential Applications in Electronics Manufacturing (2019) Available at https://shop.ipc.org/general-electronics/whitepapers/026-0-0-english

[160] Spencer J, Alonso G LTSpice: Worst-Case Circuit Analysis with Minimal Simulations Runs. Available at https://www.analog.com/en/technical-articles/ltspice-worst-case-circuit-analysis-with-minimal-simulations-runs.html

[161] de Mendizábal I (2020) Performing Worst-Case Circuit Analysis with LTspice. Available at https://www.allaboutcircuits.com/technical-articles/performing-worst-case-circuit-analysis-with-ltspice

[162] Qian Ying Tang (2011) Uncertainty propagation in transistor-level statistical dircuit analysis. thesis (University of California at Berkeley). Available at https://www2.eecs.berkeley.edu/Pubs/TechRpts/2011/EECS-2011-66.pdf

[163] Zheng Zhang (2015) Uncertainty Quantification for Integrated Circuits and Microelectromechanical Systems. thesis (Massachusetts institute of Technology). Available at https://web.ece.ucsb.edu/~zhengzhang/zheng_mit_thesis_UQ_for_IC_MEMS.pdf

[164] Translators and Processors for ODB++ Available at https://www.artwork.com/odb++/odb++_overview.htm

[165] IPC-2581C-English, Generic Requirements for Printed Board Assembly Products Manufacturing Description Data and Transfer Methodology (2020) Available at https://shop.ipc.org/general-electronics/standards/2581-0-c-english

[166] Stratigopoulos H-G, Makris Y (2008) Error Moderation in Low-Cost Machine-Learning-Based Analog/RF Testing. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* 27(2):339–351. https://doi.org/10.1109/TCAD.2007.907232

[167] Common attack pattern enumeration and classification Available at https://capec.mitre.org/index.html

[168] ATT&CK Available at https://attack.mitre.org/

[169] Trust-hub Available at https://www.trust-hub.org/#/home

[170] Bellay J, Forte D, Martin R, Taylor C (2021) Hardware vulnerability description, sharing and reporting: Challenges and opportunities. *GOMACTech 2021* Available at https://par.nsf.gov/servlets/purl/10237521

[171] iNEMI Available at https://www.inemi.org/

[172] IPC Available at https://www.ipc.org/

[173] CTIA Available at https://www.ctia.org/

[174] Release 15 Available at https://www.3gpp.org/release-15

[175] Boyens J, Paulsen C, Bartol N, Shankles SA, Moorthy R (2012) Notional Supply Chain Risk Management Practices for Federal Information Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST IR 7622, 0 Ed., p NIST IR 7622. https://doi.org/10.6028/NIST.IR.7622

[176] International vocabulary of metrology − Basic and general concepts and associated terms (VIM) (2008) Available at https://www.iso.org/sites/JCGM/VIM/JCGM_200e.html

[177] Joint Task Force Interagency Working Group (2020) Security and Privacy Controls for Information Systems and Organizations. (National Institute of Standards and Technology), Revision 5. https://doi.org/10.6028/NIST.SP.800-53r5

[178] Joint Task Force Transformation Initiative (2011) Managing information security risk :: organization, mission, and information system view. (National Institute of Standards and Technology, Gaithersburg, MD), NIST SP 800-39, 0 Ed., p NIST SP 800-39. https://doi.org/10.6028/NIST.SP.800-39

[179] Committee on national Security Systems (2010) National Information Assurance (IA) Glossary, CNSS Instruction 4009. Available at https://www.dni.gov/files/NCSC/documents/nittf/CNSSI-4009_National_Information_Assurance.pdf

[180] National Institute of Standards and Technology (2006) Minimum security requirements for federal information and information systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST FIPS 200, p NIST FIPS 200. https://doi.org/10.6028/NIST.FIPS.200

[181] ISO/TC 176/SC 1 ISO 9000:2015 Quality management systems — Fundamentals and vocabulary. Available at https://www.iso.org/standard/45481.html