2025 Most Important Hardware Weaknesses

August 2025

Introduction

The Most Important Hardware Weaknesses (MIHW) empowers organizations with the knowledge to proactively strengthen hardware security and reduce risks at the source. The 2025 CWE™ MIHW represents a refreshed and enhanced effort to identify and educate the cybersecurity community about critical hardware weaknesses. This update incorporates advancements in data collection and analysis, leveraging AI-assisted data collection alongside expert opinions from the Hardware CWE Special Interest Group (SIG), which includes subject matter experts from the hardware design, manufacturing, research, and security domains, as well as academia and government. This approach combines data-driven analysis with collaborative subject matter expertise, ensuring the 2025 MIHW brings relevant and actionable insight for addressing persistent and emerging hardware security challenges.

The 2025 CWE Most Important Hardware Weaknesses

Below is a listing of the weaknesses in the 2025 CWE Most Important Hardware Weaknesses. These entries are unranked, listed in numerical order by CWE identifier.

CWE-226	Sensitive Information in Resource Not Removed Before Reuse
CWE-1189	Improper Isolation of Shared Resources on System-on-a-Chip (SoC)
CWE-1191	On-Chip Debug and Test Interface With Improper Access Control
CWE-1234	Hardware Internal or Debug Modes Allow Override of Locks
CWE-1247	Improper Protection Against Voltage and Clock Glitches
CWE-1256	Improper Restriction of Software Interfaces to Hardware Features
CWE-1260	Improper Handling of Overlap Between Protected Memory Ranges
CWE-1262	Improper Access Control for Register Interface
CWE-1300	Improper Protection of Physical Side Channels
CWE-1421	Exposure of Sensitive Information in Shared Microarchitectural Structures during Transient Execution
CWE-1423	Exposure of Sensitive Information caused by Shared Microarchitectural Predictor State that Influences Transient Execution

Expert Insights: Weaknesses Beyond Data Trends

The following CWEs are not included in the main 2025 MIHW, but stand out as expert-driven selections. Each of these weaknesses received high scores from our panel of experts, reflecting strong consensus among those with deep domain knowledge. Although these CWEs were not represented in the vulnerability data set, they are important issues that warrant attention. These entries are unranked, listed in numerical order by CWE identifier.

CWE-1231	Improper Prevention of Lock Bit Modification
CWE-1233	Security-Sensitive Hardware Controls with Missing Lock Bit Protection
CWE-1244	Internal Asset Exposed to Unsafe Debug Access Level or State
CWE-1272	Sensitive Information Uncleared Before Debug/Power State Transition
CWE-1431	Driving Intermediate Cryptographic State/Results to Hardware Module Outputs

Key Insights

The 2025 Most Important Hardware Weaknesses highlight CWEs that encompass both longstanding challenges in hardware security and emerging areas of concern. During the review process, the team identified several noteworthy elements that merit special attention. In this section, we analyze the lists, compare them to previous findings, and explore potential factors that may explain the observed trends, recognizing that these interpretations are informed by the limited evidence and community input but may not capture all the underlying dynamics.

Comparison to the 2021 MIHW

Despite the change in methodology and the inclusion of CVE data in deriving the new MIHW, five entries from 2021 remain on the 2025 MIHW:

- CWE-1189: Improper Isolation of Shared Resources on System-on-a-Chip (SoC)
- CWE-1191: On-Chip Debug and Test Interface With Improper Access Control
- CWE-1256: Improper Restriction of Software Interfaces to Hardware Features
- CWE-1260: Improper Handling of Overlap Between Protected Memory Ranges
- CWE-1300: Improper Protection of Physical Side Channels

These entries represent persistent challenges in hardware security that are both theoretically significant and commonly observed in practice. Their continued inclusion, even with the shift to a hybrid expert and data-driven selection process, underscores their ongoing importance.

While the other seven entries from 2021 fell off the 2025 MIHW, four of them appear within our Expert Insights:

- CWE-1231: Improper Prevention of Lock Bit Modification
- CWE-1233: Security-Sensitive Hardware Controls with Missing Lock Bit Protection
- CWE-1244: Internal Asset Exposed to Unsafe Debug Access Level or State
- CWE-1272: Sensitive Information Uncleared Before Debug/Power State Transition

This may indicate that these are emerging weaknesses that are well understood by experts but are not yet widely reported. Alternatively, these weaknesses may be routinely identified and addressed early in the development cycle, preventing them from appearing in fielded products when public reporting typically occurs.

Three 2021 entries did not make the 2025 MIHW and Expert Insights:

- CWE-1240: Use of a Cryptographic Primitive with a Risky Implementation
- CWE-1274: Improper Access Control for Volatile Memory Containing Boot Code
- CWE-1277: Firmware Not Updateable

This may reflect evolving trends in CVE data, shifting expert perspectives, or the prioritization of more pressing hardware security concerns.

Six CWEs made the MIHW for the first time:
(Denotes entries that were added to CWE after the 2021 MIHW Release.)*

- CWE-226: Sensitive Information in Resource Not Removed Before Reuse
- CWE-1234: Hardware Internal or Debug Modes Allow Override of Locks
- CWE-1247: Improper Protection Against Voltage and Clock Glitches
- CWE-1262: Improper Access Control for Register Interface
- *CWE-1421: Exposure of Sensitive Information in Shared Microarchitectural Structures during Transient Execution
- *CWE-1423: Exposure of Sensitive Information caused by Shared Microarchitectural Predictor State that Influences Transient Execution

One CWE added to the corpus after the 2021 MIHW release is included in the 2025 Expert Insights:

- CWE-1431: Driving Intermediate Cryptographic State/Results to Hardware Module Outputs

New entries in the 2025 MIHW and Expert Insights may reflect increased focus on issues such as resource reuse, debug mode issues, fault injection, and register interfaces. The inclusion of transient execution weaknesses may suggest greater attention and concern over microarchitectural issues. While a cryptographic-related weakness fell off the MIHW, another appeared on Expert Insights, possibly indicating evolving priorities in cryptographic security.

Hardware View Categories

Table 1 below presents a mapping between the 2025 Most Important Hardware Weaknesses (MIHW), Expert Insights, and the Hardware View categories. The chart shows which hardware security weaknesses (listed by CWE number and description on the right) are relevant to each HW-View category (listed along the top on the left). A check mark indicates that a particular weakness is part of the corresponding HW category, highlighting areas of overlap and coverage.

1195: Manufacturing and Life Cycle Management Concerns	1196: Security Flow Issues	1197: Integration Issues	1198: Privilege Separation and Access Control Issues	1199: General Circuit and Logic Design Concerns	1201: Core and Compute Issues	1202: Memory and Storage Issues	1203: Peripherals, On-chip Fabric, and Interface/IO Problems	1205: Security Primitives and Cryptography Issues	1206: Power, Clock, Thermal, and Reset Concerns	1207: Debug and Test Problems	1208: Cross-Cutting Problems	1388: Physical Access Issues and Concerns	2025 MIHW	
					✓								CWE-226	Sensitive Information in Resource Not Removed Before Reuse
		✓											CWE-1189	Improper Isolation of Shared Resources on System-on-a-Chip (SoC)
									✓				CWE-1191	On-Chip Debug and Test Interface With Improper Access Control
			✓						✓				CWE-1234	Hardware Internal or Debug Modes Allow Override of Locks
								✓				✓	CWE-1247	Improper Protection Against Voltage and Clock Glitches
								✓					CWE-1256	Improper Restriction of Software Interfaces to Hardware Features
		✓											CWE-1260	Improper Handling of Overlap Between Protected Memory Ranges
		✓											CWE-1262	Improper Access Control for Register Interface
							✓					✓	CWE-1300	Improper Protection of Physical Side Channels
		✓		✓	✓								CWE-1421	Exposure of Sensitive Information in Shared Microarchitectural Structures during Transient Execution
		✓		✓	✓								CWE-1423	Exposure of Sensitive Information caused by Shared Microarchitectural Predictor State that Influences Transient Execution
														Expert Insights
			✓										CWE-1231	Improper Prevention of Lock Bit Modification
			✓										CWE-1233	Security-Sensitive Hardware Controls with Missing Lock Bit Protection
									✓				CWE-1244	Internal Asset Exposed to Unsafe Debug Access Level or State
									✓				CWE-1272	Sensitive Information Uncleared Before Debug/Power State Transition
							✓						CWE-1431	Driving Intermediate Cryptographic State/Results to Hardware Module Outputs

Table 1 - Coverage of 2025 MIHW and Expert Insights Weaknesses Across Hardware View Categories

Suggested Use Cases

The 2025 MIHW is a practical resource for a wide range of stakeholders in the broader semiconductor community.

Security Architects & Designers:

- Raise internal awareness of potential security weaknesses.
- Prioritize mitigations and resources to address the most important weaknesses.

Hardware Consumers:

- Provide clarity on the most important weakness to be covered when making acquisition decisions.
- Hold suppliers accountable for strong security practices.

Design Teams:

- Develop more structured and ordered review checklists based on the most important weaknesses.

Security Researchers:

- Provide insights into weaknesses that require investigation and mitigation strategies.

Test Engineers:

- Better able to focus testing efforts that address the most important weaknesses.
- Identify weaknesses in new hardware designs.

EDA Tool Vendors:

- Guide automated tool support to identify weaknesses that are deemed most important for the industry.

Educators:

- Structure course material and research on the weaknesses that are most important.

Rationale for MIHW Refresh

The decision to update the CWE Most Important Hardware Weaknesses (MIHW) was driven by significant changes in the hardware security landscape and the evolution of the Hardware CWE corpus since the last update in October 2021 (based on CWE version 4.6). Since then and through CWE version 4.17, the CWE hardware view has introduced several new and updated entries, including the addition of new classes, categories, and base weaknesses relevant to emerging hardware security concerns.

Additionally, there has been increased attention to hardware security in recent years, resulting in a greater availability of data to inform the analysis and prioritization of hardware weaknesses.

Methodology

For the 2025 MIHW, the CWE Program combined expert opinions along with publicly disclosed vulnerability data from CVE™, security advisories, conferences, and research papers. An ad-hoc working group from the Hardware CWE SIG was formed in December 2024 to undertake this refresh. The working group utilized a hybrid approach because hardware weakness data, unlike software, is still limited in availability. Input from Subject Matter Experts helps provide a clearer and more complete view of current hardware weakness trends.

The following is a high-level overview of the analysis process (Figure 1 provides a high-level overview of the methodology):

1. **Weakness Data Collection (WDC):** Collect and analyze hardware weakness data from key sources
2. **Expert Poll 1 (EP1):** Consult HW Security Experts (from the HW SIG) to decide which CWEs to include or exclude
3. **Expert Poll 2 (EP2):** Combine data analysis and expert input, then rate them using a Likert scale
4. **List Generation:** Tally rankings and create a final unranked list based on cut-off criteria

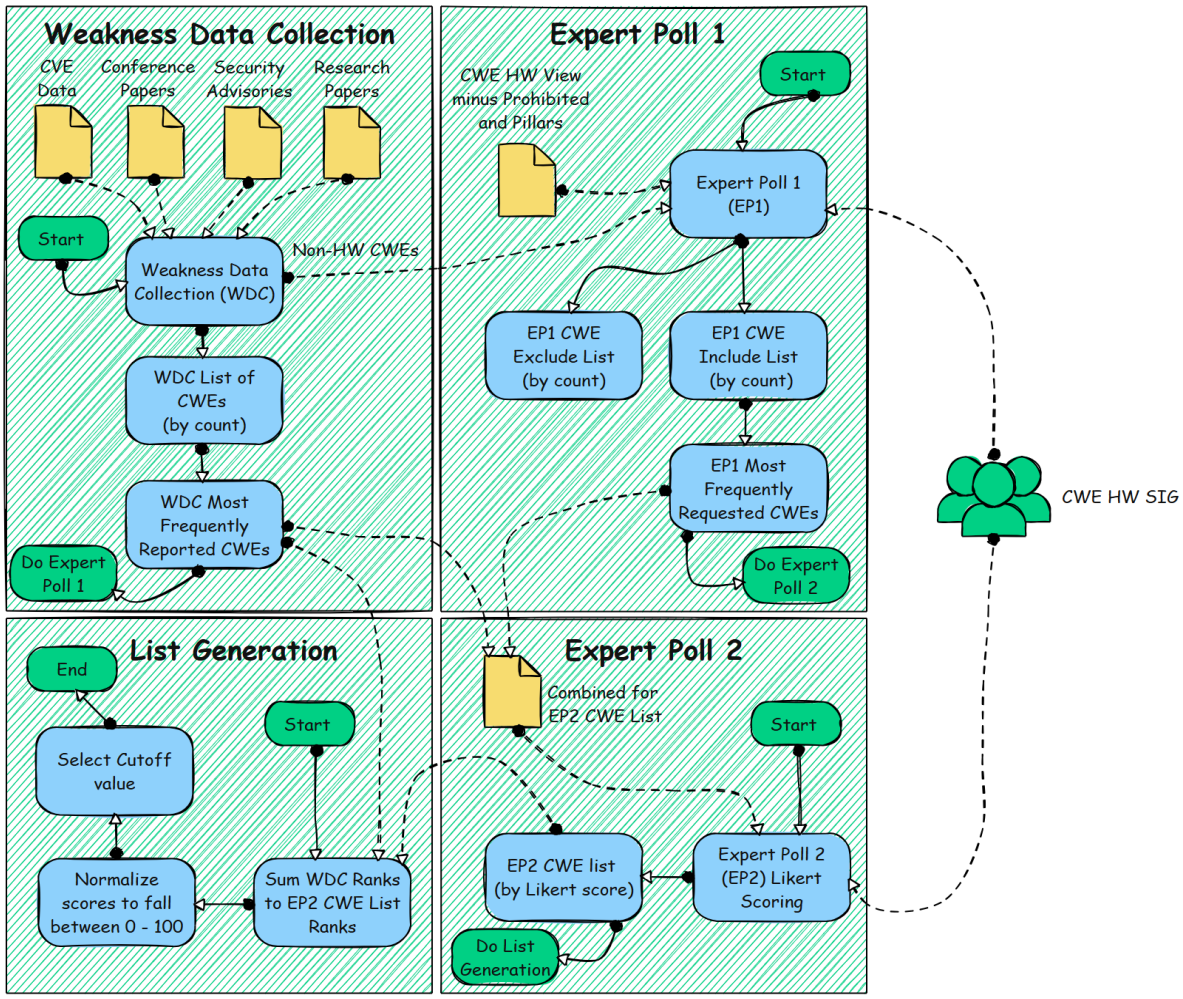

Figure 1 - High-level overview of the 2025 MIHW methodology

Weakness Data Collection

The data collection process for the 2025 MIHW began with collecting hardware relevant CVE data in order to tally their mapped CWE entries. We collected data from CVE, security advisories, research papers, and conference papers. CVE data was downloaded on 2/25/2025 and only for entries whose IDs conformed to CVE-2021-XXXX to CVE-2024-XXXX. To support the identification of hardware-related vulnerabilities, we employed a large language model (LLM) to assist in analyzing CVE descriptions and estimating their relevance to hardware weaknesses[1]. To enhance the model's performance, we employed prompt engineering techniques, including persona-based, reflection-driven, and template-based prompting patterns. The LLM was first validated using a curated dataset to ensure its accuracy and reliability. Once tested, the model was applied to the downloaded CVE data. Each entry was classified individually based on its description. Following manual review, 1,026 CVE Records were identified having hardware-related root causes.

Vendor-issued security advisories were also collected manually as well as using a custom web crawler. These advisories, which often include CVE identifiers, were queried via the NVD API to retrieve detailed vulnerability descriptions. These descriptions were classified using the same LLM framework mentioned previously, resulting in the identification of 202 security advisories from 13 leading semiconductor companies (e.g., AMD, Apple, ARM, Cisco, HP, Huawei, IBM, Intel, NVIDIA, Samsung, Siemens, ST Micro, Texas Instruments).

In addition, the working group reviewed 18 research papers and 114 conference papers from nine prominent conferences, including ACM CCS, Black Hat USA, CHES, HPCA, ISCA, MICRO, Security and Privacy, USENIX, and the Workshop on Offensive Technologies. Many of these papers contained CVE Records with existing CWE mappings. For those without mappings, the working group either assigned appropriate mappings or excluded them from the dataset if there was insufficient detail to determine the weakness. This rigorous process ensured that only relevant and well-defined hardware weaknesses were included in the final dataset of CVE Records based on hardware weaknesses.

A total of 4,112 entries were analyzed. Of these, 3,034 were excluded because they were determined to be software, firmware, or protocol-related vulnerabilities. To avoid double counting, 234 duplicate entries, often arising from overlap between sources such as research papers and CVE databases, were also removed. Among the remaining entries, 350 described vulnerabilities in hardware devices where the root cause could not be clearly identified as hardware-related. Additionally, 16 entries lacked sufficient detail to determine the root cause. Ultimately, only 478 entries (approximately 11.5% of the original dataset) provided enough information to categorize them as hardware vulnerabilities and map them to specific CWEs. This limited level of detail highlights the need to supplement CVE data analysis with expert polling, as many hardware vulnerabilities lack comprehensive disclosure of design weaknesses in published records, unlike software vulnerabilities.

[1] This work was based on a precursor solution published in ACM TODAES: https://dl.acm.org/doi/abs/10.1145/3737459

A subgroup of the HW CWE SIG verified the CWE mappings in the CVE dataset to ensure consistency and accuracy, then created a pivot table to create a frequency count of CWE entries. The pivot table contained a list of 122 unique CWE IDs. There was one element in the pivot table named 'Gap'. This is what the working group assigned to items that were clearly a hardware issue but there wasn't an appropriate CWE entry to assign. Some of the CVE mappings to CWEs included entries that are not in the hardware view. This list was then provided as a reference to respondents when conducting the first expert poll.

Expert Poll 1

The first expert poll invited members of the HW CWE SIG to identify CWEs that, in their expert judgment, should be included in or excluded from the Most Important Hardware Weaknesses (MIHW). To guide their evaluations, the HW CWE team provided a set of significance questions[2] (see "Significance Questions Used") addressing factors such as prevalence, detection, mitigation, exploitability, and other relevant metrics. These questions were consistent with the nine significance questions used in the 2021 MIHW refresh. Respondents also received a spreadsheet summarizing the top weaknesses identified through the above mentioned data collection and analysis, as well as a list of CWEs to reference for their MIHW nominations. This list included all CWEs from the HW View (CWE-1194) that are neither pillars nor prohibited, as well as additional CWEs identified during the data collection process.

The poll was conducted using Microsoft Forms from June 4 to June 23, 2025. The original closing date of June 11 was extended at the request of SIG members. Seventeen responses were received. For the inclusion data, only 15 responses were analyzed due to one duplicate and one missing inclusion entry. For the exclusion data, only six responses were analyzed due to one duplicate entry, one malformed entry, and nine missing exclusion entries.

Significance Questions Used:

1. How frequently is this weakness detected after deployment?
2. Does mitigation of this weakness require hardware modifications?
3. How frequently is this weakness detected during design?
4. How frequently is this weakness detected during testing?
5. Can the weakness be mitigated after the device has been fielded?
6. Is physical access required to exploit this weakness?
7. Can this weakness be exploited entirely via software?
8. Is a single exploit applicable to a wide range or family of devices?
9. What methodologies do you use to identify and prevent both known and emerging weaknesses?

[2] These were referred to as "points of consideration" on the survey form.

Expert Poll 1 Data Analysis

The respondents' inclusion lists were imported into Excel, where the "Text to Columns" function was used to convert CSV data into individual cells. The resulting data was then copied and transposed into columns. This process was repeated for the 15 valid inclusion lists, consolidating all CWE IDs provided by respondents into a single column.

We encountered several data anomalies, including missing commas between CWE IDs, double commas, embedded new lines, and leading spaces. To address these issues, we used a regular expression to identify malformed CWE IDs, conducted visual inspections for double commas and new lines, and applied the Excel TRIM() function to remove leading spaces. The same process was used for the six valid exclusion lists from the poll.

After data cleanup, respondents submitted a total of 267 CWE IDs for inclusion and 29 for exclusion. An Excel pivot table was then used to generate unique lists of CWE IDs with corresponding frequency counts in descending order, resulting in 114 unique CWE IDs for inclusion and 26 for exclusion. A second CWE Team member verified the analysis results using custom programs and common utilities in a Linux environment, without the use of Excel.

Expert Poll 2

The second poll asked experts to rank a subset of hardware weaknesses using a Likert scale. The set of weaknesses included in the second poll was determined by combining the top 20 (plus any other items that tied with the 20th) expert-prioritized CWEs from the first poll (using a frequency cutoff of 4) with the top 20 CWEs (plus any other items that tied with the 20th) from the weakness data collection phase (using a frequency cutoff of 10), resulting in a total of 36 unique CWEs for evaluation. The weaknesses were organized according to hardware view categories to facilitate structured assessment.

Our intention for the exclusion list from the first expert poll was to remove or downgrade a CWE from the inclusion list if there was strong consensus for exclusion. However, there was no strong support to exclude any of the top-ranked CWEs, so the exclusion list had no effect on the final set.

Upon a final review of the Export Poll 1 analysis, we discovered that some data anomalies were not identified during the generation of the dataset for Export Poll 2. Consequently, two additional CWEs (CWE-1239 and CWE-1310) were incorrectly included in the Export Poll 2 rankings, despite not meeting the established cut-off parameters. After correcting these anomalies and recompiling the dataset, we verified that no CWEs were excluded resulting in no impact to the poll. This issue was identified after Expert Poll 2 had already been conducted.

The 2nd poll was conducted using Microsoft Forms and was open from June 27, 2025, to July 11, 2025. A total of 21 responses were received; however, one was empty and two were duplicates, resulting in 18 valid responses.

List Generation

The MIHW scoring methodology integrates both expert judgment and empirical data to prioritize and assess the importance of each CWE. The process begins by ranking the CWEs according to their Expert Poll 2 (EP2) Likert scores, using Excel's RANK.EQ function, which assigns a rank relative to other values in the list. Separately, each CWE is also ranked based on its Weakness Data Count (WDC), which reflects empirical data associated with each weakness. In cases where multiple CWEs have the same score, they are assigned the highest rank for that score. Each CWE thus receives two ranks: one based on expert opinion (EP2) and one based on empirical data (WDC). These two ranks are then summed for each CWE. To facilitate interpretation and comparability, the summed ranks are normalized to a 0–100 scale using the formula: 100 * (1 - ((Sum - 2) / 70)), where "Sum" is the combined EP2 and WDC ranks, 2 is the minimum possible sum (best), and 72 is the maximum possible sum (worst). This normalization ensures that higher scores represent higher priority or importance, with the best-performing CWEs receiving scores closer to 100 and the lowest-performing receiving scores closer to 0. Any CWEs that scored a 60 or higher were included in the list.

Limitations of the Methodology

While we have taken care to combine input from subject matter experts with available data, several limitations should be noted. First, there is a scarcity of CVE data submitted by hardware vendors, and the level of detail in CVE entries can vary significantly. The correctness of mapping CVEs to CWEs is not always guaranteed, and the quality of these mappings can impact our results. Additionally, hardware-related CVEs and vulnerability data are much less available compared to software, which limits the breadth of our analysis.

We also observed that some products identified as hardware included "software" CWEs, likely due to software interfaces or support applications. Another limitation is that some weaknesses may be eliminated in later development phases before product release, but it is still important for hardware developers to avoid introducing them in the first place. Finally, there is currently no standardized way to incorporate severity scores or impact weightings into our data analysis.

Call to Action

To make future editions of the MIHW even more robust and data-driven, we encourage the community to actively contribute to improving hardware vulnerability data. This includes publishing more detailed and accurate CVE Records, ensuring accurate and precise mappings to CWEs, and sharing insights on emerging hardware threats. By addressing the limitations outlined above, we can reduce reliance on expert opinion and build a stronger, more objective foundation for identifying the most important hardware weaknesses. We invite hardware vendors, researchers, and the broader security community to make use of the MIHW and to collaborate with us in enhancing the quality and depth of hardware vulnerability data for future updates. If you are interested in joining the Hardware CWE Special Interest Group (SIG), please email cwe@mitre.org.

Acknowledgments

The 2025 CWE Hardware team includes (in alphabetical order by last name): Steve Christey Coley, Bob Heinemann, Gananand Kini, and Alec Summers.

We extend our deepest gratitude to the 2025 MIHW Working Group (a subgroup of HW SIG members), whose dedication and hard work made the weakness data collection (WDC) possible. We are also sincerely thankful to the respondents of the MIHW polls for sharing their expert insights, and to all members of the HW SIG for their ongoing support and contributions.

Names are in alphabetical order by first name.

2025 MIHW Working Group:

Andreas Schweiger, Airbus
Arun Kanuparthi, Intel Corporation
Arun Jain, NXP
Hareesh Khattri, Intel Corporation
Irena Bojanova, NIST
Jason Oberg, Cycuity
Jason Fung, Intel Corporation
Jeremy Lee, Capsia Technologies
Keerthi Devraj, Siemens
Mitchell Poplingher, Lockheed Martin
Parbati Manna, Intel Corporation
Sandy Frost, Los Alamos National Laboratory
Shahram Jamshidi, Altera
Shivam Swami, AMD
Soheil Salehi, The University of Arizona
Thomas Ford, Dell
William Ferguson, ethicallyHackingspace(eHs)

MIHW Poll Respondents:

Amitabh Das, AMD
Arun Kanuparthi, Intel Corporation
Bruce Monroe, AMD
Hareesh Khattri, Intel Corporation
Jason Fung, Intel Corporation
Jason Oberg, Cycuity
Joe Jarzombek
Joerg Bormann, Siemens
JV Rajendran, Texas A&M University
Miltos Grammatikakis, Hellenic Mediterranean University
Mitchell Poplingher, Lockheed Martin
Mohan Lal, Nvidia
Nicole Fern, Keysight
Rachana Maitra, Marvell
Robert van Spyk, Nvidia
Sohrab Aftabjahani, Intel Corporation
Sylvain Guilley, Secure-iC
William Ferguson, ethicallyHackingspace(eHs)

... and many others who chose to remain anonymous.