Hardware CWE SI Group
Meeting Minutes
November 14, 2025

Meeting Attendance

Bob Heinemann	Jagadish Nayak	Thomas Ford
Steve Christey	James Pangburn	Shafqat Ullah
Jason Fung	Parbati Manna	Jan Belohoubek
Andreas Schweiger	Rachana Maitra	Amitabh Das
Mitra Mirhassani	Mohan Lal	Hareesh Khattri
Raghul Saravanan	Vinod Viswanath	Soheil Salehi
Jeremy Lee	Sudipta Paria	Joerg Bormann

Agenda

- RTL Weaknesses Ad-Hoc Working Group Formation

Meeting Notes

Introduction and Administrative Announcements

Bob announced that the next HW CWE SIG meeting is scheduled for December 12, 2025 (topic TBD). CWE v4.19 is targeted for release on December 4, 2025, on a shorter-than-usual cycle. The Content Development Repository (CDR) remains the public intake and tracking mechanism for new CWE submissions, suggestions, and corrections; minutes, recordings, and slide materials are posted to the group's GitHub.

RTL (Register Transfer Level) Weaknesses Ad-Hoc Working Group Formation

Bob and Steve provided key context for the agenda. Multiple independent inputs over the last year raised RTL issues with potential security implications, including prior presentations and recent submissions on translation discrepancies and state-related problems.

From a CWE perspective, the focus is on identifying concrete developer/design mistakes and their security consequences rather than treating "use of RTL" itself as a weakness, and on clearly separating weaknesses from attack scenarios.

The discussion emphasized causal chains (for example, insecure optimization leading to a classic weakness that becomes exploitable), leveraging related existing entries (e.g.,

insecure automated optimizations, design/implementation inconsistencies, expected behavior violations), acknowledging gaps around state maintenance and propagation, and treating RTL as a mode of introduction that often leads to downstream CWEs while remaining open to new entries for hardware-specific patterns.

Ad-Hoc Working Group Model

The WG will be a temporary, outcome-driven effort that sunsets upon completion. Near-term steps include recruiting volunteers, holding a kickoff to select a chair, refining scope, defining deliverables, and setting success and "done" criteria, with most work occurring asynchronously and periodic synchronization meetings as needed. Expected outputs include mapping RTL scenarios to existing CWE entries, proposing clarifications or updates, drafting new entries where coverage is insufficient, and considering schema adjustments only with strong justification.

Lightning Talk Highlights

Jagadish Nayak showed how mis-coded RTL can expose sensitive data using a secure register example where a missing "else" clause creates an unintended latch that leaves data on a shared bus beyond the authorized window, noting lint can detect such patterns but often overwhelms users without security-focused triage and proposing a coherent CWE class for security-relevant RTL mis-coding patterns.

Raghul Saravanan and Sudipta Paria described translation mismatches where designs that appear correct in RTL simulation misbehave after synthesis due to issues like multiple drivers and incomplete sensitivity lists, reporting observations from open-source designs including CVEs and requesting CWE coverage for translation-induced weaknesses while building a detection tool they plan to open-source.

Joerg Bormann discussed divergences between simulated RTL and physical hardware, citing risks such as combinational loops, excessive propagation delays, and improper clock-domain crossings, and stressed that hardware-specific concerns like unused logic can enable side-channel, fault-injection, and availability attacks, with mitigation costs (e.g., resetting state bits) implying CWE guidance should reflect hardware realities rather than purely software-centric norms.

Tooling and Detection Discussion

Participants examined the roles and limits of linting, formal equivalence checking (FEC), Clock Domain Crossing (CDC) analysis, and static timing in detecting RTL weaknesses. Linting can surface many issues but requires careful configuration and security-focused rule sets to avoid drowning in warnings; FEC is standard for checking RTL versus gate-level netlists but not infallible and may miss integration-induced issues, with a preference for equivalence checkers independent of the synthesis vendor.

CDC formal checkers and timing analysis help, yet combinational loops formed at integration can be difficult to detect without global elaboration, and open-source flows have exhibited translation bugs and simulation/synthesis mismatches that some equivalence checks missed.

Customizable tools like Spyglass support targeted rules on high-risk blocks to reduce noise, but comprehensive coverage sometimes necessitates full design analysis, and the UF/GMU team is integrating their translation bug detector with commercial flows and planning a community release.

CWE Schema/Categorization Discussion

The group weighed extending existing CWE entries to include RTL-specific scenarios versus creating new RTL-focused entries and categories, aiming for clarity and usability without duplication.

Jason Fung emphasized the need for clear guidance on hardware weaknesses and the tradeoffs of grouping under existing entries versus defining new ones, while Hareesh Khattri noted CWE fields for methods of detection could be updated to reflect RTL-relevant tooling and practices and volunteered to help with analysis and proposals.

A recurring theme was distinguishing correctness-only issues from those that create security vulnerabilities.

Decisions and Actions

The group agreed to form the RTL Weaknesses Ad-Hoc Working Group. MITRE/CWE will issue a call for participation and schedule a kickoff meeting, and draft an initial charter outlining scope, goals, deliverables, and timeline.

Early WG tasks include collecting concrete, reproducible examples (preferably open-source) that demonstrate security impact, mapping scenarios to existing CWEs and identifying gaps, drafting proposals for new or updated entries, documenting chains from

RTL issues to downstream weaknesses, and developing hardware-aware detection and mitigation guidance covering configuration, tool independence, and best practices across lint, CDC, timing, and FEC.

Action Items

- **RTL Weaknesses Working Group Formation:** Coordinate with interested volunteers to set up an initial kickoff meeting for the RTL weaknesses ad hoc working group. (Bob)
- **RTL Weaknesses Working Group Participation:** Send an email to the provided address to express interest in joining the RTL weaknesses ad-hoc working group if not done during the meeting. (All interested participants**)**