HW-101 Anchor Reading Guide

4,317 words · ~20 min read

---

*VCA-HW-101 cross-chapter reading-guide handout. Companion to the catalog page at `https://virtuscyberacademy.org/vca-hw-101`. Audience: Belt-3 hardware-track students arriving from the catalog's distilled "What Belt-3 Hardware Track Graduates Recognize" register. *

The catalog page tells you WHAT the course covers. This guide tells you HOW to read the canonical anchors that build the Belt-3: which books, which talks and tutorials, in which order, what to extract on each pass, and how the anchors compose into a coherent vocabulary that prepares you for RE-101 embedded teardowns, ADV-101 hardware-CVE work, and the broader hardware-hacking practitioner community.

---

§0. What this guide is for

HW-101 is the academy's hardware-track foundations course. Five anchors carry the Belt-3: a triple of practitioner-narrative books (bunnie Huang's *The Hardware Hacker* and *Hacking the Xbox*, plus van Woudenberg and O'Flynn's *The Hardware Hacking Handbook*) for the down-to-earth-narrative core, plus Joe Grand's DEF CON Hardware Hacking Village training corpus and the Adafruit Learn plus SparkFun Tutorials community as the build-it-yourself complement. Three supplementary anchors (Schlaepfer and Oskay's *Open Circuits*; Craig Smith's *Car Hacker's Handbook*; Goodspeed and PoC||GTFO writing) are mentioned in §0 framing but do not earn full per-anchor walks at the Belt-3.

The five primary anchors do not compose a textbook tour. The bunnie triple plus van Woudenberg and O'Flynn provide the practitioner-narrative depth that the discipline reads itself through; Joe Grand and Adafruit and SparkFun provide the get-your-hands-on-the-bench complement. By the end of HW-101 a student should be able to (a) discuss debug-interface inheritance (JTAG/SWD/UART/ICSP), supply-chain framing, fault-injection and side-channel attack families, and the Tang Primer 25K toolchain in the same vocabulary the practitioner community uses, (b) build small hardware projects on

the bench (oscilloscope-anchored, soldering-anchored, JTAG-anchored), and (c) move into RE-101 with the practitioner-foundation literacy that the embedded-RE engagements assume.

This guide is opinionated by design. It is not a comprehensive bibliography. Anchors that other peer programs lean on (Horowitz and Hill's *Art of Electronics* read cover to cover; the IEEE Embedded Systems handbook; specific microprocessor datasheets read in isolation) are deliberately not the primary anchors at this level because they are encyclopedic, weighty, or out-of-genre. HW-101 graduates know the comprehensive material exists; they were trained on the opinionated material that the hardware-hacking discipline writes itself with.

The guide reads bunnie *Hacking the Xbox* before bunnie *The Hardware Hacker* before van Woudenberg and O'Flynn because the genre's foundational text comes first, the modern Shenzhen-and-supply-chain framing builds on it, and the modern applied-attacks handbook builds on both. Joe Grand and Adafruit and SparkFun read in parallel with the narrative pair: students who read while also building have the right Belt-3; students who read without building have textbook fluency and no bench fluency.

---

§1. The anchor reading register

Five anchors. Read in this order on first pass; revisit per the per-anchor walks below for capstone preparation.

Anchor 1: Andrew "bunnie" Huang, *Hacking the Xbox: An Introduction to Reverse Engineering*

Edition / pointer: Andrew "bunnie" Huang, *Hacking the Xbox: An Introduction to Reverse Engineering*, No Starch Press, 2003 (FREE PDF via the author's website with a Lawrence Lessig foreword; legal-precedent text). The original printed edition is hard to find; the free PDF is canonical.

Why this matters at Belt-3: bunnie Huang's *Hacking the Xbox* is the foundational text of the modern hardware-hacking genre. The book walks bunnie's reverse-engineering of the original Xbox's security architecture: the LDT bus tap, the TSOP flash, the eFuse, the bootloader RC4-and-HMAC chain, the jam-table protection, the public-key signature verification. The book is opinionated about why hardware-RE matters (a hardware platform is a contract between vendor and owner; RE is what lets the owner audit the contract) and about how it is done (a bench, a logic analyser, patience, and the willingness to break the platform until it talks). A Belt-3 graduate who has read

Hacking the Xbox recognises the genre's voice, knows the bench's primary tools by name, and understands why the discipline frames itself as an investigation rather than as a destruction. Lessig's foreword places the book in legal context; reading the foreword installs the academy's ethical-framing register.

Suggested reading order: First. Read bunnie *Hacking the Xbox* before any other anchor because it is the genre's foundational text and its vocabulary is what the other anchors assume. The free-PDF availability makes the read low-friction.

Cross-link to academy artifacts: HW-101 Lab 1 (introduction to the bench; oscilloscope and logic analyser); HW-101 Lab 7 (debug-interface discovery against an academy-provided board); RE-101 Lab 8 (firmware analysis on the SB6141 SPI flash; bunnie's Xbox flash-tap analysis is the structural analog); ADV-101 (CVE-to-tool work where the target is hardware; bunnie's reverse-engineering frame is the methodology anchor).

Anchor 2: Andrew "bunnie" Huang, *The Hardware Hacker: Adventures in Making and Breaking Hardware*

Edition / pointer: Andrew "bunnie" Huang, *The Hardware Hacker: Adventures in Making and Breaking Hardware*, No Starch Press, 2017 (ISBN 978-1-59327-758-1). The Shenzhen-factory and supply-chain narrative anchor; bunnie's second book and the discipline's modern register.

Why this matters at Belt-3: *The Hardware Hacker* is bunnie's modern follow-on to *Hacking the Xbox*. Where the earlier book walks one hardware platform's reverse-engineering, the later book walks the broader practitioner ecosystem: the Shenzhen factories where most consumer hardware is made; the supply-chain patterns that determine what a hacker can buy and what they cannot; the open-hardware movement that bunnie helps lead through Chibitronics, NeTV, and Precursor. A Belt-3 graduate who has read *The Hardware Hacker* understands that hardware does not appear from nothing; it is manufactured under specific economic and ecosystem constraints that determine what is hackable and what is not. The Shenzhen-factory framing is the academy's primary supply-chain-as-textbook anchor.

Suggested reading order: Second. Read after *Hacking the Xbox* because the modern Shenzhen-and-supply-chain framing builds on the earlier reverse-engineering register. Students should treat the Shenzhen chapters as the central read; the chapters on bunnie's specific products are valuable but supplementary.

Cross-link to academy artifacts: HW-101 Lab 5 (BoM analysis on a teardown subject; bunnie's Shenzhen framing is the analytical foundation); HW-101 capstone (student-fabricated Arduino-based data logger; the supply-chain awareness is part of the engineering report); RE-101 (the SB6141 lab target is itself a Shenzhen-supply-chain artifact; reading bunnie before SB6141 makes the lab target legible). The forward-pointer to RE-101 Lab 8 is structural: bunnie's analysis of the Xbox flash tap maps directly onto the SB6141 SPI flash dump.

Anchor 3: Jasper van Woudenberg + Colin O'Flynn, *The Hardware Hacking Handbook: Breaking Embedded Security with Hardware Attacks*

Edition / pointer: Jasper van Woudenberg and Colin O'Flynn, *The Hardware Hacking Handbook: Breaking Embedded Security with Hardware Attacks*, No Starch Press, 2021 (ISBN 978-1-59327-748-2). The modern applied-attacks handbook; covers fault injection, side-channel analysis, glitching, JTAG and SWD attack patterns, chip-off rework.

Why this matters at Belt-3: *The Hardware Hacking Handbook* is the bench-anchored applied-attacks reference. Where bunnie's two books frame the discipline and the ecosystem, van Woudenberg and O'Flynn walk the specific attack families a practitioner exercises against embedded systems. Fault injection (voltage glitching; clock glitching; electromagnetic fault injection) is the canonical "make the chip skip an instruction" attack; side-channel analysis (power analysis; timing analysis) is the canonical "measure what the chip is doing while it does it" attack; chip-off rework (heat-gun and BGA reflow patterns) is the canonical "extract the silicon from its package and read it directly" attack. A Belt-3 graduate who has read van Woudenberg and O'Flynn knows the attack families by name, can describe what each one does at a high level, and understands which targets each attack family is appropriate for.

Suggested reading order: Third. Read after the bunnie pair because the attack-family vocabulary is most useful when the genre's foundational and ecosystem framing are already installed. Students should treat the introductory and overview chapters as the Belt-3 read; the deep-dive chapters on specific attack-tool implementations belong at HW-201 register.

Cross-link to academy artifacts: HW-101 Lab 8 (debug-interface attack progression on an academy-provided target); HW-101 Lab 9 (introduction to side-channel analysis with the ChipWhisperer); RE-101 Lab 10 (chip-off-and-direct-read against the SB6141 flash; van Woudenberg's chapter on chip-off is the methodology anchor); ADV-101 (hardware-CVE work where fault injection or side-channel analysis is the attack vector).

Anchor 4: Joe Grand DEF CON Hardware Hacking Village training corpus

Edition / pointer: Joe Grand (Kingpin), DEF CON Hardware Hacking Village training corpus (FREE on Internet Archive plus YouTube via greatscottgadgets.com and the DEF CON channel; the DEF CON 14 introduction; the DEF CON 21 JTAGulator introduction; the ongoing HHV programming). Joe Grand is L0pht alumnus, JTAGulator inventor, and the discipline's most-cited working educator after bunnie.

Why this matters at Belt-3: The Joe Grand corpus is the academy's primary build-it-yourself training reference. Where the bunnie and van Woudenberg pairs are read as books, Joe Grand's talks and tutorials are watched and walked; the videos cover specific bench techniques (probing live boards; identifying JTAG headers; using the JTAGulator to discover unknown debug interfaces) at the practitioner-tier register. The DEF CON 21 JTAGulator introduction is the most-cited single talk in the corpus; students should walk it as a Lab 7 companion. The ongoing HHV programming is the discipline's annual practitioner-update channel.

Suggested reading order: Fourth. Walk the Joe Grand corpus after the book triple because the bench techniques are most useful when the discipline's framing and the attack-family vocabulary are already installed. Students should treat the DEF CON 21 JTAGulator talk plus the HHV introductory talks as the Belt-3 walk; the deeper material belongs at HW-201 capstone register.

Cross-link to academy artifacts: HW-101 Lab 7 (JTAG discovery with the JTAGulator); HW-101 Lab 8 (Bus Pirate exercises against unknown boards); RE-101 Lab 11 (live-board JTAG probing on the SB6141; Joe Grand's methodology is the procedural anchor). The JTAGulator pattern is the canonical "discover the debug interface from a board you have never seen before" exercise; reading Joe Grand before HW-101 Lab 7 lets the student walk the lab with the methodology already in head.

Anchor 5: Adafruit Learn + SparkFun Tutorials

Edition / pointer: Adafruit Learn (free; learn.adafruit.com) plus SparkFun Tutorials (free; sparkfun.com/tutorials). Two community tutorial corpora maintained by two of the largest open-hardware retailers; the canonical entry-tier hands-on hardware reference.

Why this matters at Belt-3: Adafruit Learn and SparkFun Tutorials are the academy's primary entry-tier-fundamentals references for HW-101 students. The corpora cover thousands of hands-on projects at every level from beginner to advanced; the academy's HW-101 lab harness draws specific tutorials as Lab 1 through Lab 6 companions. A Belt-3 graduate who has walked the canonical entry-tier tutorials (basic breadboarding; Arduino IDE introduction; digital and analogue I/O; serial

communication; I2C and SPI) has the bench fluency the academy assumes for Labs 7 onward. The corpora are also the academy's primary part-sourcing reference; students who buy from Adafruit or SparkFun get parts that work with the tutorials, which keeps the bench progression smooth.

Suggested reading order: Fifth. Walk the relevant tutorials in parallel with the academy's Labs 1-6 rather than reading them in advance; the tutorials are companions, not prerequisites. Students who already have entry-tier hardware experience can skim; students new to the bench should walk the Adafruit-Arduino-introduction series and the SparkFun-soldering series in their entirety.

Cross-link to academy artifacts: HW-101 Labs 1-6 (every primary lab has a named Adafruit or SparkFun tutorial companion); HW-101 capstone (the student-fabricated data logger draws on multiple Adafruit and SparkFun tutorials for component selection and wiring); the Tang Primer 25K toolchain (Adafruit and SparkFun do not directly cover the Tang Primer 25K, but the breadboarding and digital-I/O fundamentals are platform-independent).

---

§2. bunnie *Hacking the Xbox* deep walk: the genre's foundational reverse-engineering text

bunnie's *Hacking the Xbox* is the discipline's foundational text. Read for the genre voice and the bench-discipline vocabulary as the book's central operational primitives.

What to extract

A Belt-3 graduate should carry the following five facts from the book:

1. **The book frames hardware-RE as investigation.** The chapters walk bunnie's actual investigative path against the original Xbox: hypothesis, test, observation, refinement. The investigative frame is the genre's signature; subsequent practitioner texts inherit it.
2. **The bench's primary tools are oscilloscope, logic analyser, soldering iron, and patience.** The book introduces each tool in context. A Belt-3 graduate should be able to name what each tool does and what kinds of evidence each one collects.
3. **A debug interface is the practitioner's canonical entry point.** The Xbox's LPC bus tap is the book's central example; the LPC bus carried boot data the bootloader could not encrypt. A Belt-3 graduate should recognise that production hardware almost always has debug interfaces (JTAG, SWD, UART, ICSP, JTAG-equivalent) and that finding them is the practitioner's first move.

4. **Cryptographic protections fail under bench-level attack.** The book walks the Xbox bootloader's RC4 and HMAC chain and shows how a tap on the bus reveals the protected data anyway. The lesson is not that the cryptography is bad; it is that the cryptography's threat model did not include a bench. A Belt-3 graduate should be able to articulate the difference between cryptographic security under a software-only threat model and cryptographic security under a hardware-level threat model.
5. **Lessig's foreword places the book in legal context.** The book is a teaching text, not an exploit guide; the legal context (DMCA, CFAA, exemptions for security research) is what makes the discipline practicable. A Belt-3 graduate should be familiar with the foreword's argument and the academy's ethical-framing register.

What is out-of-scope at Belt-3

The book's specific Xbox-internal details (the exact RC4 key derivation; the eFuse layout; the XCodes virtual machine) are interesting period material and out-of-scope at the practitioner-foundation tier. The legal-history details belong at the academy's ethics-and-disclosure register; HW-101 students should know the foreword exists and not be expected to walk the case law.

Cross-anchor connections

bunnie's investigative frame is the foundation *The Hardware Hacker* builds on; reading *Hacking the Xbox* first makes the modern Shenzhen-and-supply-chain framing legible as a continuation rather than as a separate book. bunnie's bench-tool vocabulary lands directly on van Woudenberg and O'Flynn's attack-family vocabulary; the bench tools are how the attacks are exercised. bunnie's debug-interface emphasis lands on the Joe Grand JTAGulator material; reading bunnie before walking the Joe Grand corpus makes the JTAGulator's purpose immediately legible.

---

§3. bunnie *The Hardware Hacker* deep walk: Shenzhen and the supply-chain frame

bunnie's modern follow-on is the discipline's supply-chain-as-textbook anchor. Read for the Shenzhen-factory framing as the book's central operational primitive.

What to extract

A Belt-3 graduate should carry the following five facts from the book:

1. **Most consumer hardware is manufactured in Shenzhen.** The bunnie Shenzhen-factory chapters walk the practitioner through the actual manufacturing ecosystem; the chapters are reportage, not documentary distance. A Belt-3 graduate should be familiar with the Shenzhen ecosystem at the practitioner-narrative tier.
2. **The supply chain determines what is hackable.** Components that exist on the market in volume are hackable; components that do not are not. bunnie's framing is that hackability is downstream of supply-chain economics, not just engineering choices. A Belt-3 graduate should be able to articulate this argument.
3. **Open hardware is a deliberate counter-pattern.** bunnie has built and helped build open-hardware platforms (Chibitronics; NeTV; Precursor; the Novena laptop) as deliberate counters to the closed-hardware default. Open hardware is a discipline-internal stance, not a moral one; the academy's framing inherits bunnie's stance.
4. **BoM (Bill of Materials) analysis is a practitioner skill.** Reading a BoM tells you what the hardware is made of, where the components came from, and what attacks are tractable against them. HW-101 Lab 5 exercises BoM analysis on a real teardown subject.
5. **Counterfeit components are real, and the practitioner notices them.** The book walks specific examples of counterfeit chips that look identical to the legitimate part but behave differently. A Belt-3 graduate should know that the counterfeit-component problem exists and not be expected to recognise specific counterfeits at this level.

What is out-of-scope at Belt-3

Specific bunnie-product chapters (the Novena laptop's design rationale; the Precursor's threat model) are interesting practitioner-narrative reading and out-of-scope at the Belt-3 tier. The chapters on specific Shenzhen-internal events (the original Maker Faire Shenzhen; specific factory tours) are valuable as practitioner-narrative entertainment rather than as foundational Belt-3 material.

Cross-anchor connections

The Shenzhen-and-supply-chain framing lands directly on the SB6141 lab target: the SB6141 is itself a Shenzhen-supply-chain artifact, and reading bunnie before RE-101 makes the lab target legible. The supply-chain framing reads against van Woudenberg and O'Flynn at the lab-tooling tier (the ChipWhisperer; the Bus Pirate; the JTAGulator are

themselves supply-chain artifacts the practitioner buys). The framing reads against Joe Grand and Adafruit and SparkFun: the build-it-yourself complement is supply-chain-aware by design; students who buy parts know which retailers and which components survive a teardown.

---

§4. van Woudenberg + O'Flynn deep walk: applied attacks on embedded systems

The applied-attacks handbook walks the modern bench-anchored attack families. Read for the attack-family vocabulary as the book's central operational primitive.

What to extract

A Belt-3 graduate should carry the following five facts from the book:

1. **Fault injection makes the chip skip an instruction.** Voltage glitching, clock glitching, and electromagnetic fault injection (EMFI) are the three primary fault-injection vectors. The shared mechanism is that a brief perturbation at the right time causes the chip to misexecute or skip a single instruction, which can bypass security checks (signature verification; PIN comparison; secure-boot gate). A Belt-3 graduate should know all three vectors by name.
2. **Side-channel analysis measures what the chip is doing while it does it.** Power analysis (Simple Power Analysis; Differential Power Analysis) and timing analysis are the primary side-channel families; both extract secret data (keys; PINs) by observing the chip's behaviour rather than its outputs. A Belt-3 graduate should know SPA and DPA at the conceptual register.
3. **JTAG and SWD attacks are debug-interface exploitations.** JTAG (the IEEE 1149.1 boundary-scan standard) and SWD (ARM's Serial Wire Debug) are the canonical debug interfaces on modern embedded systems; finding and exploiting them is a foundational practitioner skill. A Belt-3 graduate should know the difference between the two protocols and how they are attacked.
4. **Chip-off rework extracts the silicon from its package.** Heat-gun and BGA reflow patterns let the practitioner remove a chip from a board, place it in an adapter, and read its memory directly. The technique is destructive-to-the-board but non-destructive-to-the-silicon; it is the canonical last-resort technique when in-system attacks fail.

5. **The ChipWhisperer is the academy's primary applied-attacks platform.** O'Flynn's ChipWhisperer is open hardware specifically designed for fault-injection and side-channel analysis at the practitioner-foundation tier; the academy's HW-101 Lab 9 uses the ChipWhisperer for entry-tier exercises.

What is out-of-scope at Belt-3

Specific exploit-implementation details (the exact glitch parameters for a specific target; the specific power-trace alignment algorithm for a specific cipher) belong at HW-201 register. Advanced techniques (focused-ion-beam circuit edit; advanced fault-injection at automotive register; commercial-grade laser fault injection) are graduate-research material.

Cross-anchor connections

The attack-family vocabulary lands directly on bunnie's Xbox-bus-tap example: the Xbox attack is itself a debug-interface-and-bench-tool attack at the early-2000s register. The attack vocabulary lands on Joe Grand's JTAGulator: JTAG attack patterns are the canonical practitioner exercise. The attack vocabulary lands on the SB6141 lab target: chip-off and JTAG probing are the canonical RE-101 exercises against the SB6141.

---

§5. Joe Grand DEF CON HHV deep walk: build-it-yourself bench discipline

Joe Grand's training corpus is the academy's primary build-it-yourself anchor for bench techniques. Walk for the practitioner-tier methodology as the corpus's central operational primitive.

What to extract

A Belt-3 graduate should carry the following five facts from the corpus:

1. **JTAG discovery is the JTAGulator's purpose.** The DEF CON 21 talk introduces the JTAGulator, an open-hardware tool for discovering JTAG (and UART) interfaces on unknown boards. A Belt-3 graduate should be able to use the JTAGulator on an academy-provided target.
2. **Bus Pirate is the multi-protocol bench tool.** The Bus Pirate (Dangerous Prototypes; widely available) speaks I2C, SPI, JTAG, UART, and several other protocols and lets the practitioner exercise them from a serial-console interface. A Belt-3 graduate should be able to use the Bus Pirate to read an SPI flash on the bench.

3. **Probing live boards requires bench-safety discipline.** Joe Grand's corpus repeatedly emphasises that the practitioner can damage the board, the tool, or themselves; the discipline of probing carefully matters. A Belt-3 graduate should be able to articulate the bench-safety vocabulary (ground, voltage levels, current limits, electrostatic discharge).
4. **L0pht is the discipline's lineage anchor.** Joe Grand was a member of the L0pht Heavy Industries group in the 1990s; the group's testimony to the U.S. Senate in 1998 ("any of us could shut down the internet in 30 minutes") is a foundational moment for the discipline's professional emergence. A Belt-3 graduate should know the L0pht lineage.
5. **DEF CON HHV is the discipline's annual update channel.** The Hardware Hacking Village programs at DEF CON each year cover both foundational training and current-research talks. A Belt-3 graduate should know the venue and the rhythm.

What is out-of-scope at Belt-3

Specific exploit walkthroughs from individual HHV talks belong at HW-201 capstone register. The Joe-Grand-specific consulting-engagement war stories are practitioner-narrative entertainment and out-of-scope at the practitioner-foundation tier.

Cross-anchor connections

Joe Grand's bench-tool vocabulary lands directly on bunnie's Xbox-bus-tap example: the JTAGulator and the Bus Pirate are the modern equivalents of the bench setup bunnie walks. The bench-tool vocabulary lands on van Woudenberg and O'Flynn: the JTAG-attack vocabulary the handbook walks is exercised through the JTAGulator and the Bus Pirate at the bench.

---

§6. Adafruit + SparkFun deep walk: entry-tier hands-on hardware

Adafruit Learn and SparkFun Tutorials are the academy's primary entry-tier hands-on hardware references. Walk in parallel with HW-101 Labs 1-6.

What to extract

A Belt-3 graduate should carry the following four facts from the corpora:

1. **Breadboarding is the canonical entry-tier project pattern.** The two corpora's introductory tutorials walk basic breadboard wiring, the colour-coded wire conventions, and the standard component layouts. A Belt-3 graduate should be able to wire a circuit from a schematic onto a breadboard without trial and error.
2. **Arduino IDE is the entry-tier programming environment.** The two corpora use the Arduino IDE almost universally for entry-tier projects; the academy follows the convention. A Belt-3 graduate should be able to write, compile, and upload a basic Arduino sketch.
3. **Soldering is a learnable skill.** The SparkFun soldering tutorials walk the technique from temperature setting through tip preparation through joint inspection. A Belt-3 graduate should be able to produce inspection-quality joints on through-hole and basic SMD work.
4. **I2C and SPI are the entry-tier inter-chip communication protocols.** The two corpora cover both protocols at entry-tier with sample code and breakout boards. A Belt-3 graduate should be able to wire an I2C or SPI sensor to an Arduino and read its values.

What is out-of-scope at Belt-3

Advanced project tutorials (specific home-automation builds; specific data-logger projects) are valuable as practitioner-narrative entertainment and out-of-scope as required reading. The corpora's deep dives into specific component datasheets belong at HW-201 register.

Cross-anchor connections

The entry-tier corpora are the foundation Joe Grand's bench techniques assume; reading Adafruit and SparkFun before walking the Joe Grand corpus installs the breadboarding-and-soldering vocabulary that the JTAG and Bus Pirate exercises require. The corpora are also the academy's primary part-sourcing reference; the supply-chain awareness bunnie's books install lands directly on the part-selection decisions Adafruit and SparkFun make tractable.

---

§7. Summary: how the anchors compose at Belt-3

Anchor	Role	Belt-3 deliverable it supports
bunnie *Hacking the Xbox*	Genre foundation; reverse-engineering frame	Lab 7 debug-interface discovery; Lab 8 bench-tool exercises; the academy's ethical-framing register
bunnie *The Hardware Hacker*	Shenzhen and supply-chain framing	Lab 5 BoM analysis; capstone supply-chain awareness; SB6141 lab-target legibility
van Woudenberg + O'Flynn HHH	Applied-attacks vocabulary	Lab 9 ChipWhisperer side-channel analysis; RE-101 chip-off methodology; ADV-101 hardware-CVE work
Joe Grand DEF CON HHV	Build-it-yourself bench discipline	Lab 7 JTAGulator; Lab 8 Bus Pirate; the bench-safety discipline
Adafruit + SparkFun	Entry-tier hands-on foundation	Labs 1-6 walkthroughs; capstone component selection and wiring

The composition is opinionated by design. The bunnie pair plus van Woudenberg and O'Flynn provide the down-to-earth narrative core that the discipline reads itself through; Joe Grand and Adafruit and SparkFun provide the build-it-yourself complement that the discipline practices itself through. The five anchors do not reduce to one anchor; each earns its place because the others assume its content. The Belt-3 is what the composition produces.

---

§8. What's next at Belt-4 and Belt-5

HW-101 graduates carry the five-anchor foundation into RE-101 (Belt 4; embedded-systems reverse-engineering with the SB6141 cable modem as the lab target) and into ADV-101 (Belt 4; CVE-to-tool work where the target is hardware). The hardware track does not currently have a Belt-5 terminal course; advanced hardware work is integrated into RE-201 (Belt 5; burst-radio waveform RE) and into the academy's broader RE and AI capstone arcs.

Anchors that return at deeper register:

- **bunnie's pair returns at RE-101** as the structural-analog reference for the SB6141 firmware-extraction lab; bunnie's Xbox flash-tap analysis maps onto the SB6141 SPI-flash dump.
- **van Woudenberg + O'Flynn returns at RE-101** for the chip-off methodology and at ADV-101 for the fault-injection and side-channel attack families.

- **Joe Grand returns at RE-101** for the live-board JTAG-probing methodology against the SB6141.

The capstone work HW-101 prepares for: a student-fabricated Arduino-based data logger in a hand-built enclosure with a written engineering report. Students who carry the five-anchor foundation into the capstone produce stronger artifacts than students who learn the vocabulary during the capstone.

The hardware-track parallel credential pathway is less consolidated than the networking-track or RF-track equivalents (no single industry-standard credential like CCNA or ARRL Technician); the closest analog is the OffSec OSED (Exploit Developer) track, which is Belt-5 and assumes HW-101 plus RE-101 plus ADV-101 as foundation.

---

§9. Cross-references

Artifact	Path	Relationship
Catalog page (the page you arrived from)	`/vca-hw-101`	Distilled register; this guide is its forward-pointer destination
Companion handout: WIR-101 anchor reading guide	`/handouts/cross-chapter-wir-101-anchor-reading-guide.md`	Companion Belt-3 handout; wireless-track foundations
Companion handout: NET-101 anchor reading guide	`/handouts/cross-chapter-net-101-anchor-reading-guide.md`	Companion Belt-3 handout; networking-track foundations
Companion handout: PEN-101 anchor reading guide	`/handouts/cross-chapter-pen-101-anchor-reading-guide.md`	Companion Belt-3 handout; pentest-track foundations
RE-101 catalog page	`/vca-re-101`	Belt-4 RE-track; SB6141 embedded-RE capstone; HW-101 anchors return as structural references
ADV-101 catalog page	`/vca-adv-101`	Belt-4 PT/ADV-track; CVE-to-tool work where target is hardware

---