# RED BALLOON SECURITY

## SPECIAL EFFECTS CLUB

PROUDLY PRESENTS


CRYO

MECHA
NICAL

# MEMORY


TRAK
TION

I can't see 'em Coming Down


I am a good sketch of Jay Z. (I)

I can't see 'em Coming Down

So I

Gotta Make The Slides


I am a good sketch of Jay Z. (!)

I can't see 'em Coming Down

So I

Gotta Make The Slides Cry


I am a good sketch of Jay Z. (!)

I can't see 'em Coming Down

So I

Gotta Make The Slides

Cry-O


I am a good sketch of Jay Z. (!)

I can't see 'em Coming Down

So I

Gotta Make the Slides

Cry-O


I am a good sketch of Jay Z. (!)

7 MONTHS OF A
DIFFERENT
FLAVOR OF CRUSHING
DEFEAT

This is a story of failure

7 MONTHS OF A
DIFFERENT
FLAVOR OF CRUSHING
DEFEAT

18 MONTHS OF SOUL
CRUSHING FAILURE

This is a story of failure
inside another story of failure,

7 MONTHS OF A DIFFERENT FLAVOR OF CRUSHING DEFEAT

BUT WE WON!

18 MONTHS OF SOUL CRUSHING FAILURE



This is a story of failure
inside another story of failure,
topped off with a drizzle of ep1c w1n.

# What did we win?

## Cryo-Mechanical RAM Content Extraction Against Modern Embedded Systems

Yuanzhe Wu
*Red Balloon Security*
New York, NY, USA
hans@redballoonsecurity.com

Grant Skipper
*Red Balloon Security*
New York, NY, USA
grant@redballoonsecurity.com

Ang Cui
*Red Balloon Security*
New York, NY, USA
ang@redballoonsecurity.com

***Abstract*—Cryogenic mechanical memory extraction provides a means to obtain a device's volatile memory content at runtime. Numerous prior works has have demonstrated successful exploitation of the Memory Remanence Effect on modern computers and mobile devices. While this approach is arguably one of the most direct paths to reading a target device's physical RAM content, several significant limitations exist. For example, prior works were done either on removable memory with standardized connectors, or with the use of a custom kernel/bootloader.**

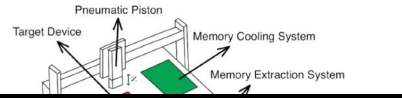
**We present a generalized and automated system that performs reliable RAM content extraction against modern embedded devices. Our cryo-mechanical apparatus is built using low-cost hardware that is widely available, and supports target devices using single or multiple DDR1|2|3 memory modules. We discuss several novel techniques and hardware modifications that allow our apparatus to exceed the spatial and temporal precision required to reliably perform memory extraction against modern embedded systems that have memory modules soldered directly onto the PCB, and use custom memory controllers that spread bits of each word of memory across multiple physical RAM chips.**

***Index Terms*—cold-boot, side-channel, memory extraction, reverse engineering, embedded security**

### I. Introduction

Modern high-performance embedded systems typically store firmware code in nonvolatile flash memory, and load the code into volatile dynamic random access memory (DRAM) during boot-up. The code and data contents of the device is often useful for security analysis. Firmware binaries can

rate (DDR)1, DDR2, and DDR3 memory modules. As shown in Figure 1, our system consists of a modified low-cost commercial off-the-shelf (COTS) computer numerical control (CNC) machine, a memory reader device implemented with an Field-Progammable-Gate-Array (FPGA), and controller implemented using an ESP32 [3] module and microPython [4]. This process involved cooling the memory chip, booting up the target device, physically transferring the chip to the readout platform, and recovering data. The entire apparatus can be built with widely available parts costing approximately $2,000 USD. The remainder of this paper discusses novel techniques and hardware modifications we developed to enable the described apparatus to perform reliable cryo-mechanical RAM content extraction on single and multi-memory-chip embedded devices. We demonstrate that our system can successfully perform memory extraction and reconstruction against an embedded device that uses a custom black-box memory controller and five physical RAM chips.




W00T 2023

## Uprooting Trust: Learnings from an Unpatchable Hardware Root-of-Trust Vulnerability in Siemens S7-1500 PLCs

Yuanzhe Wu
*Red Balloon Security*
*New York, NY, USA*
*hans@redballoonsecurity.com*

Grant Skipper
*Red Balloon Security*
*New York, NY, USA*
*grant@redballoonsecurity.com*

Ang Cui
*Red Balloon Security*
*New York, NY, USA*
*ang@redballoonsecurity.com*

***Abstract*—Over the past decade, low-cost hardware cryptocoprocessors have become an attractive solution for improving device security on embedded systems. Relying on dedicated components to offload security operations, however, presents unique challenges to overall system security. When implemented incorrectly, these components may be abused by adversaries to infiltrate Root-of-Trust (RoT) protections and compromise the greater system. Unlike software-based RoT, when a hardware-based RoT is found vulnerable to tampers there are few remedies to 'patch' or defend against attacks.**

**This work presents a case study for addressing real-world security practices related to implementing hardware RoT for embedded systems via discrete co-processing components. Furthermore, we identify design fallacies, which we have encountered with increasing frequency in commercial embedded systems. Through this investigation, we provide practical mitigating solutions for integrating secure RoT peripherals for use on embedded hardware. Specifically, this assessment is conducted by uncovering novel vulnerabilities related to the discrete RoT implementation on the Siemens S7-1500 series Programmable Logic Controllers (PLCs). Our**

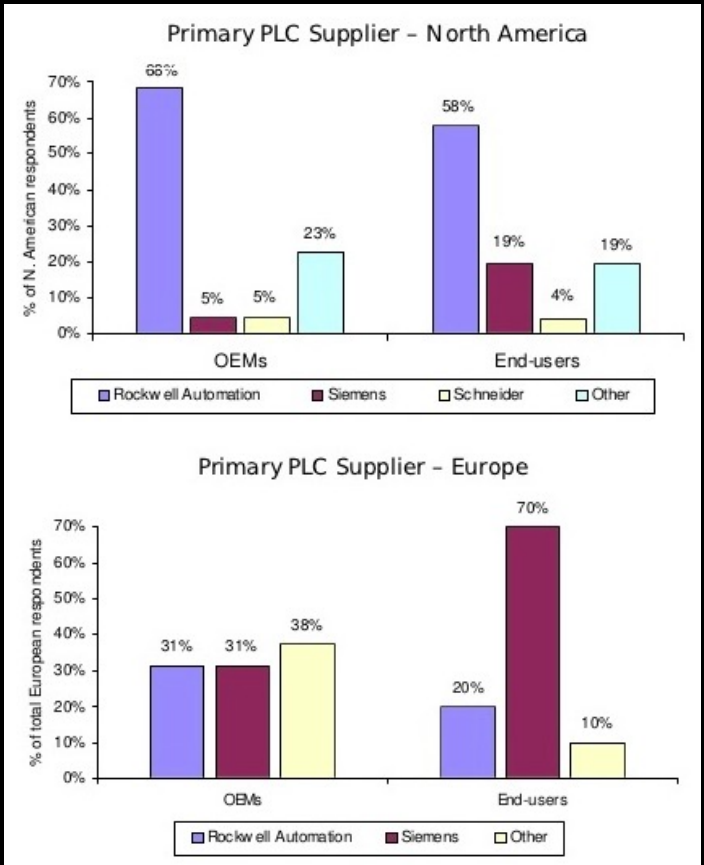
Trusted Platform Modules (TPMs) are one of the most common hardware cryptography peripherals available today. TPMs are typically found in higher-end computing environments, such as personal computers. It is relatively uncommon to find TPMs in embedded systems, in part due to the relatively high cost of these components. Over the last decade, however, cryptographic co-processors have become significantly cheaper to produce, and thus more affordable and widely available. This development has led to the proliferation of independent cryptographic ICs in embedded consumer electronics, and has transformed the ecology of embedded system security.

HOST 2023

[1] Wu, Yuanzhe, Grant Skipper, and Ang Cui. "Cryo-Mechanical RAM Content Extraction Against Modern Embedded Systems." *17th IEEE Workshop on Offensive Technologies (WOOT).* San Francisco, CA, USA, 2023.

[2] Wu, Yuanzhe, Grant Skipper, and Ang Cui. "Uprooting Trust: Learnings from an Unpatchable Hardware Root-of-Trust Vulnerability in Siemens S7-1500 PLCs." *2023 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*. IEEE Computer Society, 2023.

# What did we really win?






## SSA-482757: Missing Immutable Root of Trust in S7-1500 CPU devices

Publication Date: 2023-01-10
Last Update: 2023-03-14
Current Version: V1.2
CVSS v3.1 Base Score: 4.6

### SUMMARY

Affected models of the S7-1500 CPU product family do not contain an Immutable Root of Trust in Hardware. With this the integrity of the code executed on the device can not be validated during load-time. An attacker with physical access to the device could use this to replace the boot image of the device and execute arbitrary code.

As exploiting this vulnerability requires physical tampering with the product, Siemens recommends to assess the risk of physical access to the device in the target deployment and to implement measures to make sure that only trusted personnel have access to the physical hardware.

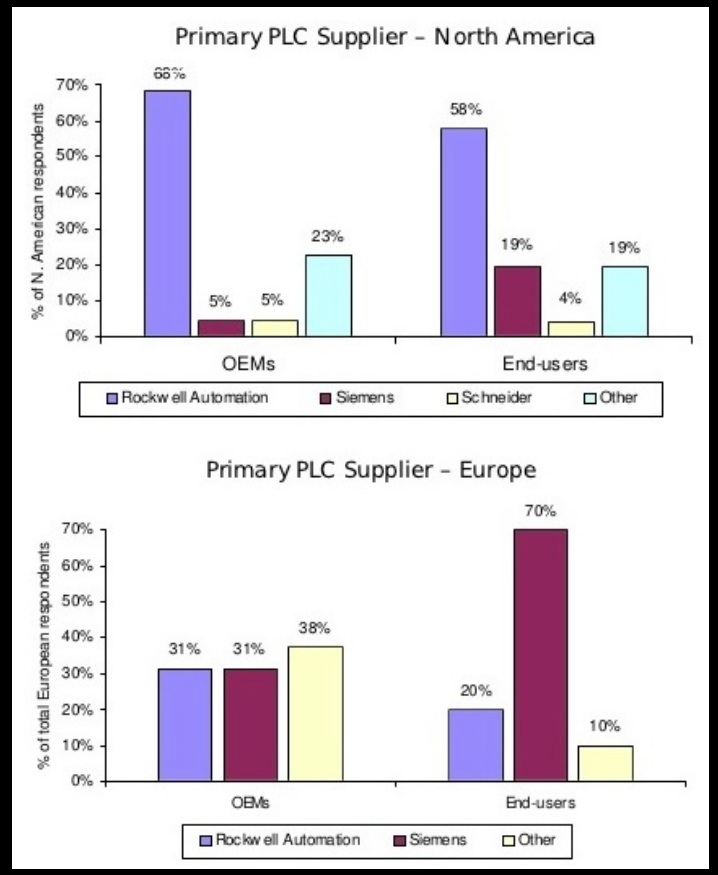
The vulnerability is related to the hardware of the product. Siemens has released new hardware versions for several CPU types of the S7-1500 product family in which this vulnerability is fixed and is working on new hardware versions for remaining PLC types to address this vulnerability completely. See the chapter “Additional Information” below for more details.

For more information please also refer to the related product support article: https://support.industry.siemens.com/cs/ww/en/view/109816536/.

### AFFECTED PRODUCTS AND SOLUTION

| Affected Product and Versions | Remediation |
|---|---|
| SIMATIC Drive Controller CPU 1504D TF (6ES7615-4DF10-0AB0): All versions | Currently no fix is planned See recommendations from section Workarounds and Mitigations |
| SIMATIC Drive Controller CPU 1507D TF (6ES7615-7DF10-0AB0): All versions | Currently no fix is planned See recommendations from section Workarounds and Mitigations |
| SIMATIC S7-1500 CPU 1510SP F-1 PN (6ES7510-1SJ00-0AB0): All versions | Currently no fix is planned See recommendations from section Workarounds and Mitigations |
| SIMATIC S7-1500 CPU 1510SP F-1 PN (6ES7510-1SJ01-0AB0): All versions | Currently no fix is planned See recommendations from section Workarounds and Mitigations |
| SIMATIC S7-1500 CPU 1510SP-1 PN (6ES7510-1DJ00-0AB0): All versions | Currently no fix is planned See recommendations from section Workarounds and Mitigations |
| SIMATIC S7-1500 CPU 1510SP-1 PN (6ES7510-1DJ01-0AB0): All versions | Currently no fix is planned See recommendations from section Workarounds and Mitigations |

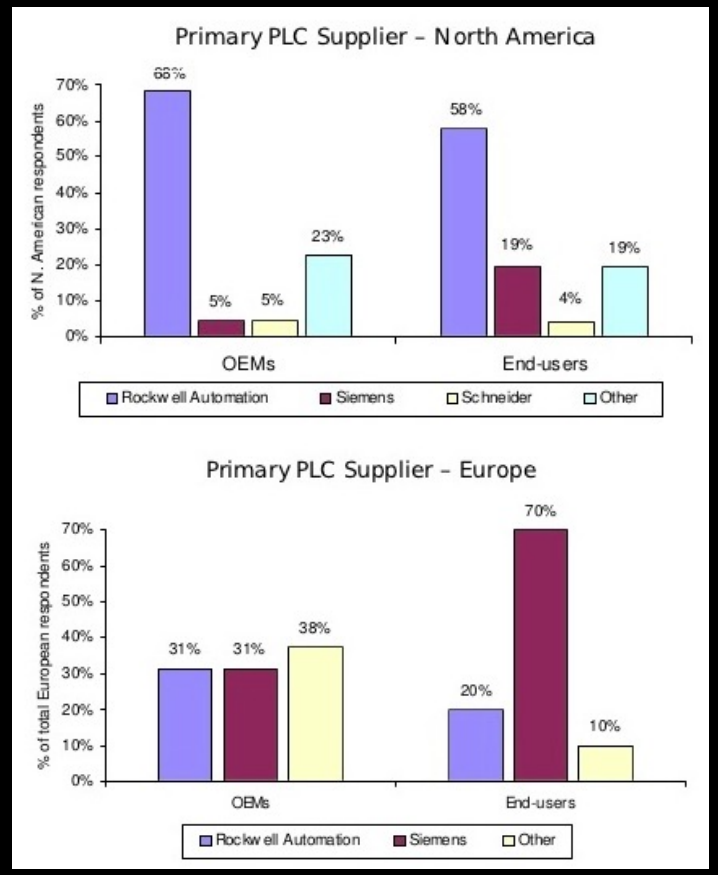
# What did we really win?






| | |
|---|---|
| SIMATIC S7-1500 CPU 1512SP F-1 PN (6ES7512-1SK01-0AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIMATIC S7-1500 CPU 1512SP-1 PN (6ES7512-1DK00-0AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIMATIC S7-1500 CPU 1512SP-1 PN (6ES7512-1DK01-0AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIMATIC S7-1500 CPU 1513-1 PN (6ES7513-1AL00-0AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIMATIC S7-1500 CPU 1513-1 PN (6ES7513-1AL01-0AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIMATIC S7-1500 CPU 1513-1 PN (6ES7513-1AL02-0AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIMATIC S7-1500 CPU 1513F-1 PN (6ES7513-1FL00-0AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIMATIC S7-1500 CPU 1513F-1 PN (6ES7513-1FL01-0AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIMATIC S7-1500 CPU 1513F-1 PN (6ES7513-1FL02-0AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIMATIC S7-1500 CPU 1513R-1 PN (6ES7513-1RL00-0AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIMATIC S7-1500 CPU 1515-2 PN (6ES7515-2AM00-0AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIMATIC S7-1500 CPU 1515-2 PN (6ES7515-2AM01-0AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIMATIC S7-1500 CPU 1515-2 PN (6ES7515-2AM02-0AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |

# What did we really win?

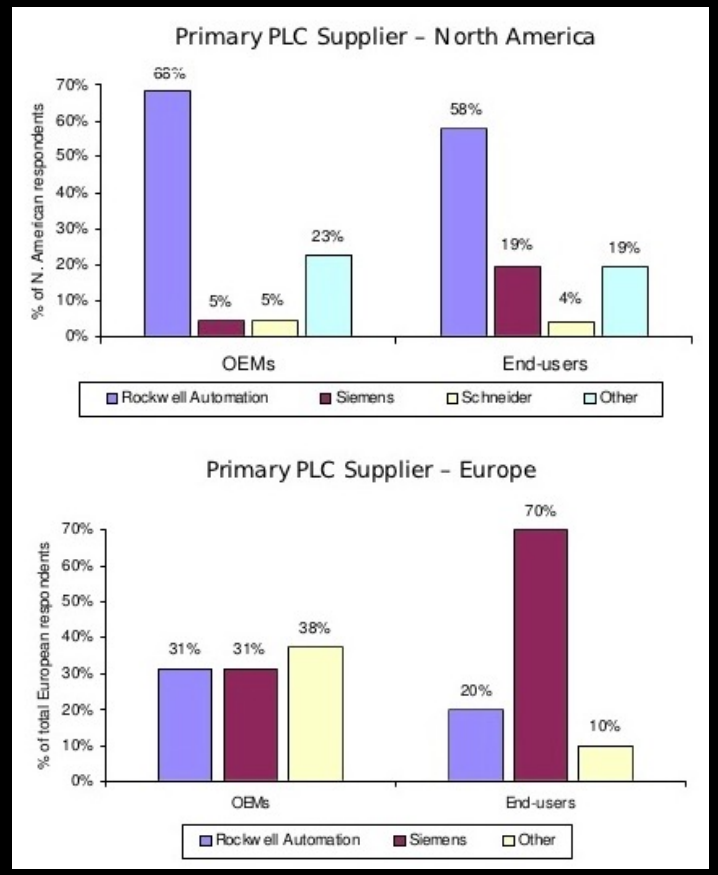



Zoom out



| | |
|---|---|
| SIMATIC S7-1500 CPU 1515F-2 PN (6ES7515-2FM00-0AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIMATIC S7-1500 CPU 1515F-2 PN (6ES7515-2FM01-0AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIMATIC S7-1500 CPU 1515F-2 PN (6ES7515-2FM02-0AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIMATIC S7-1500 CPU 1515R-2 PN (6ES7515-2RM00-0AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIMATIC S7-1500 CPU 1515T-2 PN (6ES7515-2TM01-0AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIMATIC S7-1500 CPU 1515TF-2 PN (6ES7515-2UM01-0AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIMATIC S7-1500 CPU 1516-3 PN/DP (6ES7516-3AN00-0AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIMATIC S7-1500 CPU 1516-3 PN/DP (6ES7516-3AN01-0AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIMATIC S7-1500 CPU 1516-3 PN/DP (6ES7516-3AN02-0AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIMATIC S7-1500 CPU 1516F-3 PN/DP (6ES7516-3FN00-0AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIMATIC S7-1500 CPU 1516F-3 PN/DP (6ES7516-3FN01-0AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIMATIC S7-1500 CPU 1516F-3 PN/DP (6ES7516-3FN02-0AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIMATIC S7-1500 CPU 1516T-3 PN/DP (6ES7516-3TN00-0AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |

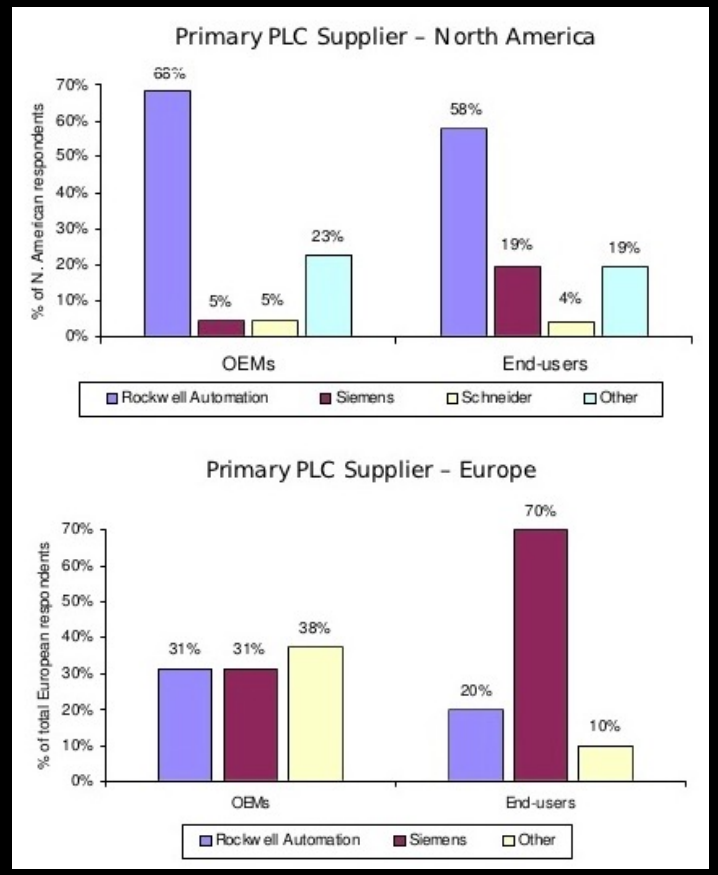
# What did we really win?






| | |
|---|---|
| SIMATIC S7-1500 CPU 1516TF-3 PN/DP (6ES7516-3UN00-0AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIMATIC S7-1500 CPU 1517-3 PN/DP (6ES7517-3AP00-0AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIMATIC S7-1500 CPU 1517F-3 PN/DP (6ES7517-3FP00-0AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIMATIC S7-1500 CPU 1517H-3 PN (6ES7517-3HP00-0AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIMATIC S7-1500 CPU 1517T-3 PN/DP (6ES7517-3TP00-0AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIMATIC S7-1500 CPU 1517TF-3 PN/DP (6ES7517-3UP00-0AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIMATIC S7-1500 CPU 1518-4 PN/DP (6ES7518-4AP00-0AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIMATIC S7-1500 CPU 1518-4 PN/DP MFP (6ES7518-4AX00-1AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIMATIC S7-1500 CPU 1518F-4 PN/DP (6ES7518-4FP00-0AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIMATIC S7-1500 CPU 1518F-4 PN/DP MFP (6ES7518-4FX00-1AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIMATIC S7-1500 CPU 1518HF-4 PN (6ES7518-4JP00-0AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIMATIC S7-1500 CPU 1518T-4 PN/DP (6ES7518-4TP00-0AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIMATIC S7-1500 CPU 1518TF-4 PN/DP (6ES7518-4UP00-0AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |

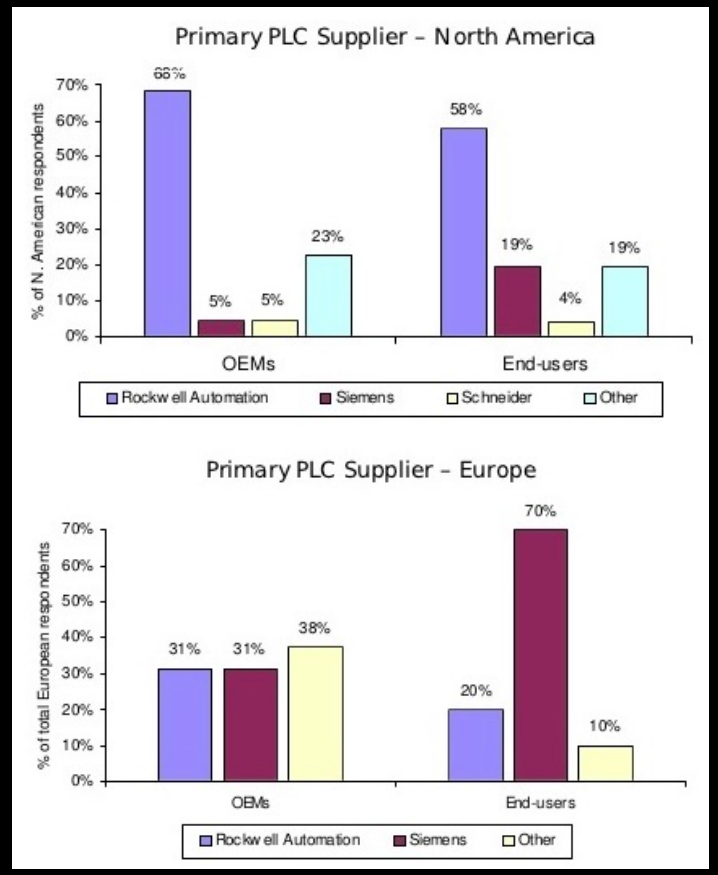
# What did we really win?






| | |
|---|---|
| SIMATIC S7-1500 CPU S7-1518-4 PN/DP ODK (6ES7518-4AP00-3AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIMATIC S7-1500 CPU S7-1518F-4 PN/DP ODK (6ES7518-4FP00-3AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIMATIC S7-1500 ET 200pro: CPU 1513PRO F-2 PN (6ES7513-2GL00-0AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIMATIC S7-1500 ET 200pro: CPU 1513PRO-2 PN (6ES7513-2PL00-0AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIMATIC S7-1500 ET 200pro: CPU 1516PRO F-2 PN (6ES7516-2GN00-0AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIMATIC S7-1500 ET 200pro: CPU 1516PRO-2 PN (6ES7516-2PN00-0AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIPLUS ET 200SP CPU 1510SP F-1 PN (6AG1510-1SJ01-2AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIPLUS ET 200SP CPU 1510SP F-1 PN RAIL (6AG2510-1SJ01-1AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIPLUS ET 200SP CPU 1510SP-1 PN (6AG1510-1DJ01-2AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIPLUS ET 200SP CPU 1510SP-1 PN (6AG1510-1DJ01-7AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIPLUS ET 200SP CPU 1510SP-1 PN RAIL (6AG2510-1DJ01-1AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIPLUS ET 200SP CPU 1510SP-1 PN RAIL (6AG2510-1DJ01-4AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIPLUS ET 200SP CPU 1512SP F-1 PN (6AG1512-1SK00-2AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |

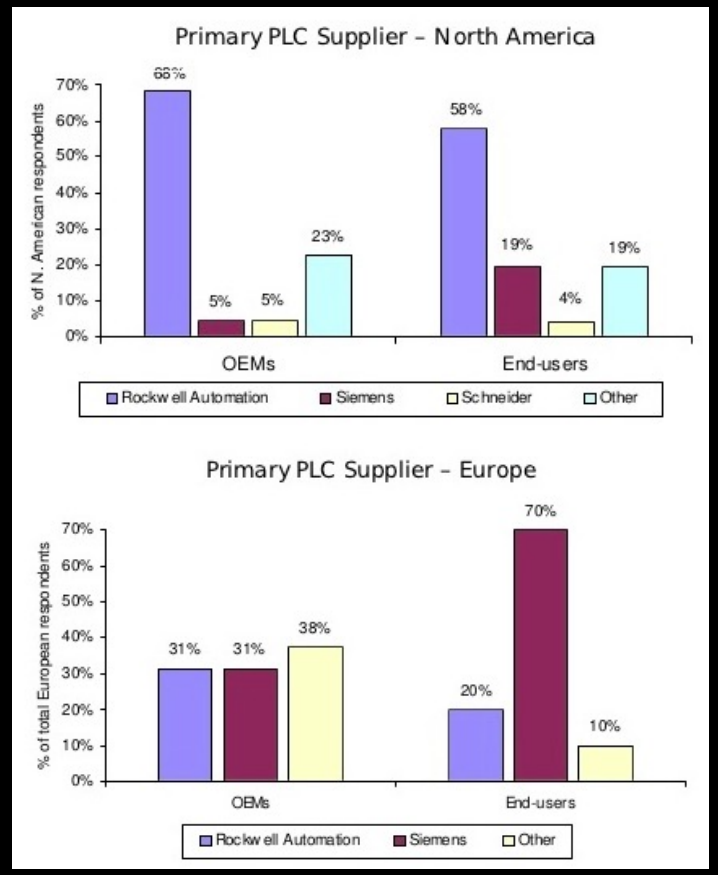
# What did we really win?






| | |
|---|---|
| SIPLUS ET 200SP CPU 1512SP F-1 PN (6AG1512-1SK01-2AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIPLUS ET 200SP CPU 1512SP F-1 PN (6AG1512-1SK01-7AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIPLUS ET 200SP CPU 1512SP F-1 PN RAIL (6AG2512-1SK01-1AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIPLUS ET 200SP CPU 1512SP F-1 PN RAIL (6AG2512-1SK01-4AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIPLUS ET 200SP CPU 1512SP-1 PN (6AG1512-1DK01-2AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIPLUS ET 200SP CPU 1512SP-1 PN (6AG1512-1DK01-7AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIPLUS ET 200SP CPU 1512SP-1 PN RAIL (6AG2512-1DK01-1AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIPLUS ET 200SP CPU 1512SP-1 PN RAIL (6AG2512-1DK01-4AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIPLUS S7-1500 CPU 1511-1 PN (6AG1511-1AK00-2AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIPLUS S7-1500 CPU 1511-1 PN (6AG1511-1AK01-2AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIPLUS S7-1500 CPU 1511-1 PN (6AG1511-1AK01-7AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIPLUS S7-1500 CPU 1511-1 PN (6AG1511-1AK02-2AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIPLUS S7-1500 CPU 1511-1 PN (6AG1511-1AK02-7AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |

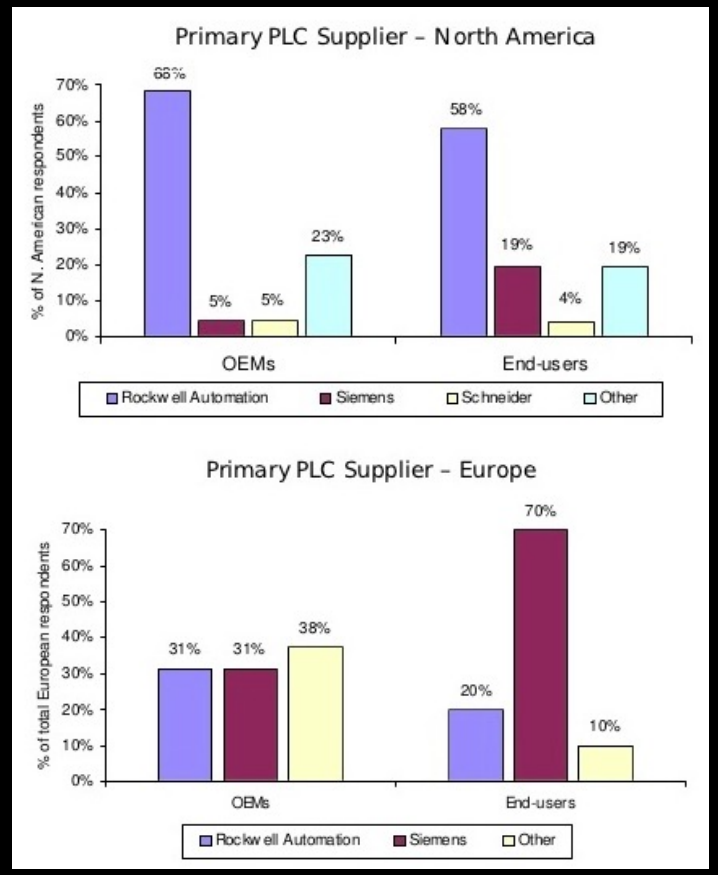
# What did we really win?






| | |
|---|---|
| SIPLUS S7-1500 CPU 1511-1 PN T1 RAIL (6AG2511-1AK01-1AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIPLUS S7-1500 CPU 1511-1 PN T1 RAIL (6AG2511-1AK02-1AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIPLUS S7-1500 CPU 1511-1 PN TX RAIL (6AG2511-1AK01-4AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIPLUS S7-1500 CPU 1511-1 PN TX RAIL (6AG2511-1AK02-4AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIPLUS S7-1500 CPU 1511F-1 PN (6AG1511-1FK00-2AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIPLUS S7-1500 CPU 1511F-1 PN (6AG1511-1FK01-2AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIPLUS S7-1500 CPU 1511F-1 PN (6AG1511-1FK02-2AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIPLUS S7-1500 CPU 1513-1 PN (6AG1513-1AL00-2AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIPLUS S7-1500 CPU 1513-1 PN (6AG1513-1AL01-2AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIPLUS S7-1500 CPU 1513-1 PN (6AG1513-1AL01-7AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIPLUS S7-1500 CPU 1513-1 PN (6AG1513-1AL02-2AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIPLUS S7-1500 CPU 1513-1 PN (6AG1513-1AL02-7AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIPLUS S7-1500 CPU 1513F-1 PN (6AG1513-1FL00-2AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |

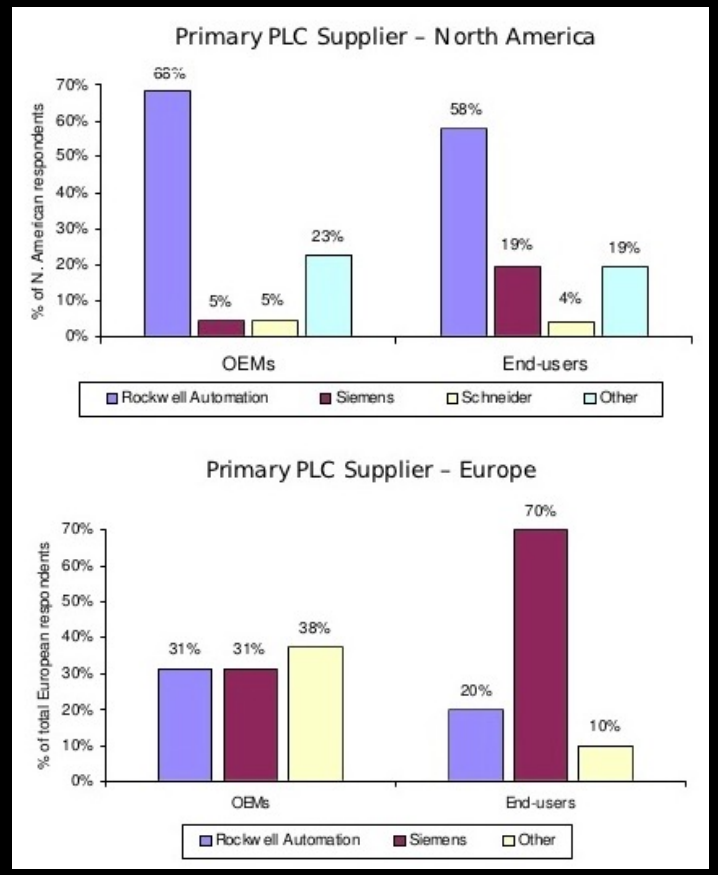
# What did we really win?






| | |
|---|---|
| SIPLUS S7-1500 CPU 1513F-1 PN (6AG1513-1FL01-2AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIPLUS S7-1500 CPU 1513F-1 PN (6AG1513-1FL02-2AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIPLUS S7-1500 CPU 1515F-2 PN (6AG1515-2FM01-2AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIPLUS S7-1500 CPU 1515F-2 PN (6AG1515-2FM02-2AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIPLUS S7-1500 CPU 1515F-2 PN RAIL (6AG2515-2FM02-4AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIPLUS S7-1500 CPU 1515F-2 PN T2 RAIL (6AG2515-2FM01-2AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIPLUS S7-1500 CPU 1515R-2 PN (6AG1515-2RM00-7AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIPLUS S7-1500 CPU 1515R-2 PN TX RAIL (6AG2515-2RM00-4AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIPLUS S7-1500 CPU 1516-3 PN/DP (6AG1516-3AN00-2AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIPLUS S7-1500 CPU 1516-3 PN/DP (6AG1516-3AN00-7AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIPLUS S7-1500 CPU 1516-3 PN/DP (6AG1516-3AN01-2AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIPLUS S7-1500 CPU 1516-3 PN/DP (6AG1516-3AN01-7AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIPLUS S7-1500 CPU 1516-3 PN/DP (6AG1516-3AN02-2AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |

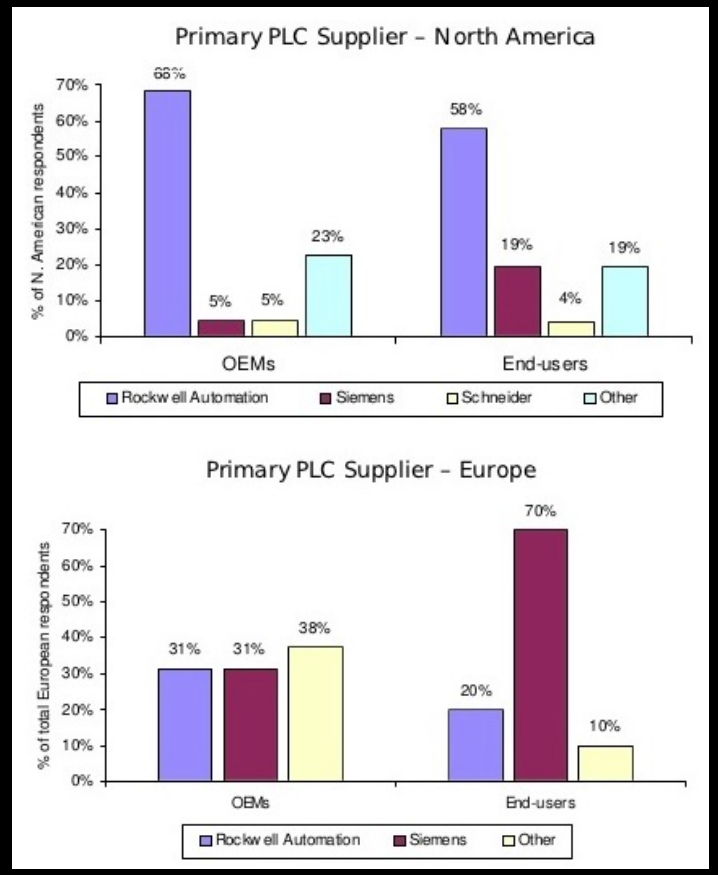
# What did we really win?






| | |
|---|---|
| SIPLUS S7-1500 CPU 1516-3 PN/DP (6AG1516-3AN02-7AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIPLUS S7-1500 CPU 1516-3 PN/DP RAIL (6AG2516-3AN02-4AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIPLUS S7-1500 CPU 1516-3 PN/DP TX RAIL (6AG2516-3AN01-4AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIPLUS S7-1500 CPU 1516F-3 PN/DP (6AG1516-3FN00-2AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIPLUS S7-1500 CPU 1516F-3 PN/DP (6AG1516-3FN01-2AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIPLUS S7-1500 CPU 1516F-3 PN/DP (6AG1516-3FN02-2AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIPLUS S7-1500 CPU 1516F-3 PN/DP RAIL (6AG2516-3FN02-2AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIPLUS S7-1500 CPU 1516F-3 PN/DP RAIL (6AG2516-3FN02-4AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIPLUS S7-1500 CPU 1517H-3 PN (6AG1517-3HP00-4AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIPLUS S7-1500 CPU 1518-4 PN/DP (6AG1518-4AP00-4AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIPLUS S7-1500 CPU 1518-4 PN/DP MFP (6AG1518-4AX00-4AC0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIPLUS S7-1500 CPU 1518F-4 PN/DP (6AG1518-4FP00-4AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIPLUS S7-1500 CPU 1518HF-4 PN (6AG1518-4JP00-4AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |

# What did we really win?






## WORKAROUNDS AND MITIGATIONS

Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk:

- Restrict physical access to affected devices to trusted personnel to avoid hardware tampering (e.g., place the devices in locked control cabinets)

Please follow the General Security Recommendations.

## GENERAL SECURITY RECOMMENDATIONS

As a general security measure, Siemens strongly recommends to protect network access to devices with appropriate mechanisms. In order to operate the devices in a protected IT environment, Siemens recommends to configure the environment according to Siemens' operational guidelines for Industrial Security (Download: https://www.siemens.com/cert/operational-guidelines-industrial-security), and to follow the recommendations in the product manuals. Additional information on Industrial Security by Siemens can be found at: https://www.siemens.com/industrialsecurity

## PRODUCT DESCRIPTION

SIMATIC Drive Controllers have been designed for the automation of production machines, combining the functionality of a SIMATIC S7-1500 CPU and a SINAMICS S120 drive control.

SIMATIC S7-1500 CPU products have been designed for discrete and continuous control in industrial environments such as manufacturing, food and beverages, and chemical industries worldwide.

The SIMATIC S7-1500 MFP CPUs provide functionality of standard S7-1500 CPUs with the possibility to run C/C++ Code within the CPU-Runtime for execution of own functions / algorithms implemented in C/C++ and an additional second independent runtime environment to execute C/C++ applications parallel to the STEP 7 program if required.

The SIMATIC S7-1500 ODK CPUs provide functionality of standard S7-1500 CPUs but additionally provide the possibility to run C/C++ Code within the CPU-Runtime for execution of own functions / algorithms implemented in C/C++. They have been designed for discrete and continuous control in industrial environments such as manufacturing, food and beverages, and chemical industries worldwide.

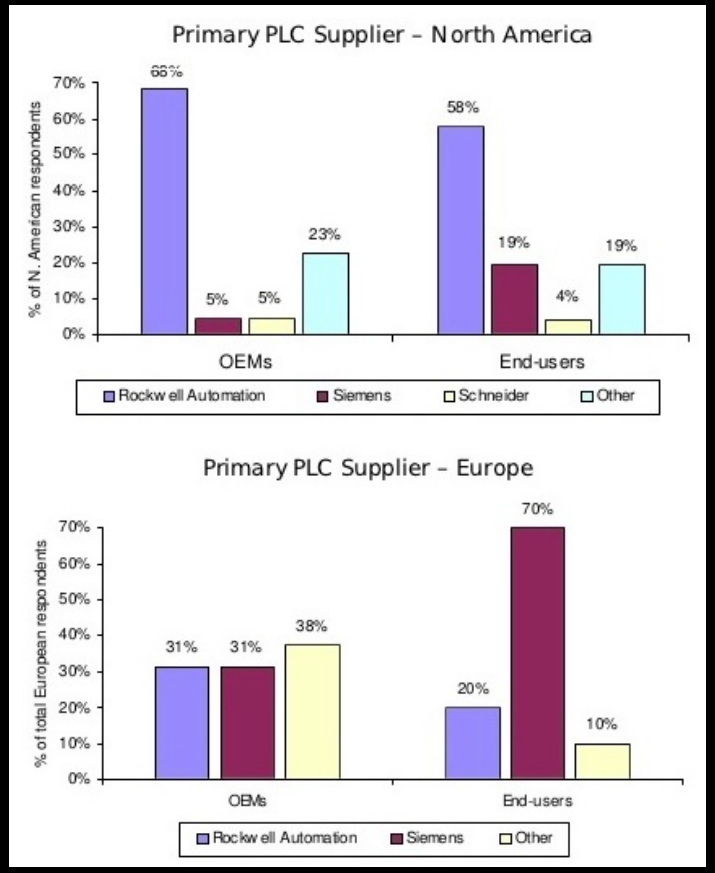
SIPLUS extreme products are designed for reliable operation under extreme conditions and are based on SIMATIC, LOGO!, SITOP, SINAMICS, SIMOTION, SCALANCE or other devices. SIPLUS devices use the same firmware as the product they are based on.

## VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.1 (CVSS v3.1) (https://www.first.org/cvss/). The CVSS environmental score is specific to the customer's environment and will impact the overall CVSS score. The environmental score should therefore be individually defined by the customer to accomplish final scoring.

An additional classification has been performed using the CWE classification, a community-developed list of common software security weaknesses. This serves as a common language and as a baseline for weakness identification, mitigation, and prevention efforts. A detailed list of CWE classes can be found at: https://cwe.mitre.org/.

# What did we really win?




Siemens Security Advisory by Siemens ProductCERT

## WORKAROUNDS AND MITIGATIONS

Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk:

- Restrict physical access to affected devices to trusted personnel to avoid hardware tampering (e.g., place the devices in locked control cabinets)

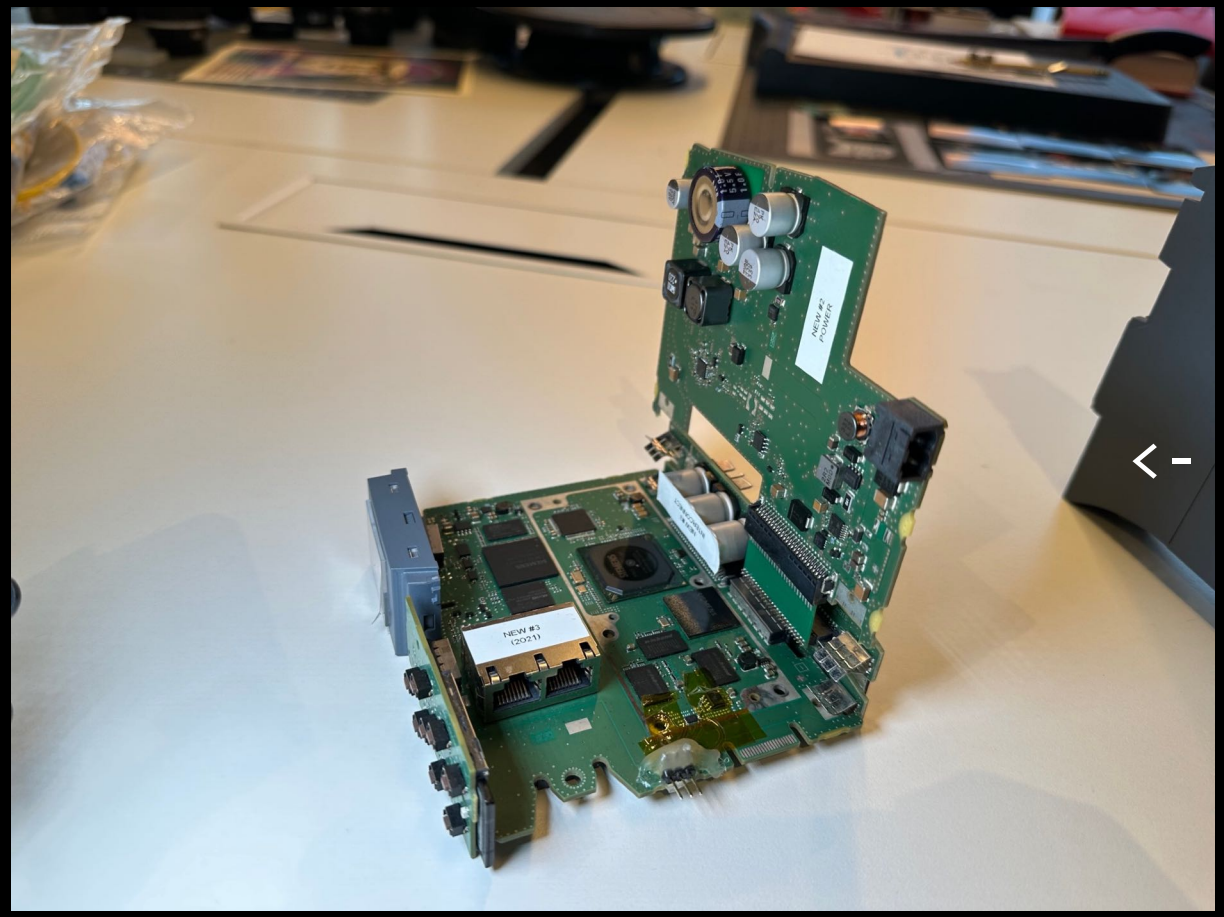
Please follow the General Security Recommendations.

## GENERAL SECURITY RECOMMENDATIONS

| | |
|---|---|
| SIMATIC S7-1500 CPU 1510SP F-1 PN (6ES7510-1SJ00-0AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIMATIC S7-1500 CPU 1510SP F-1 PN (6ES7510-1SJ01-0AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIMATIC S7-1500 CPU 1510SP-1 PN (6ES7510-1DJ00-0AB0):<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |
| SIMATIC S7-1500 CPU 1510SP-1 PN (6ES7510 | Currently no fix is planned |

Maybe a technical achievement win for researchers.
But inexcusable lose for the world.

What did we really really win?

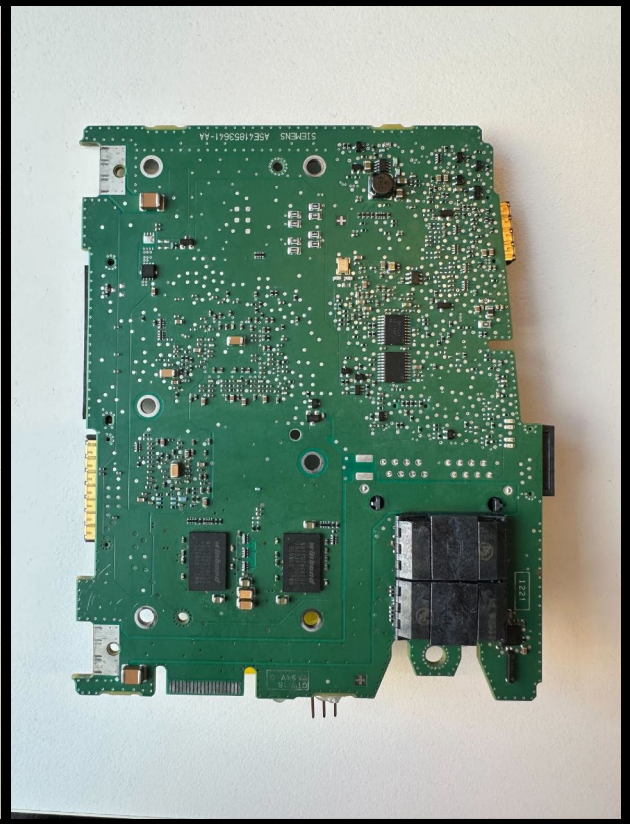



We stared at

<- this

Until it cried uncle. -)

# What’s the big deal with that board?

Siemens Simatic S7-1500 Line

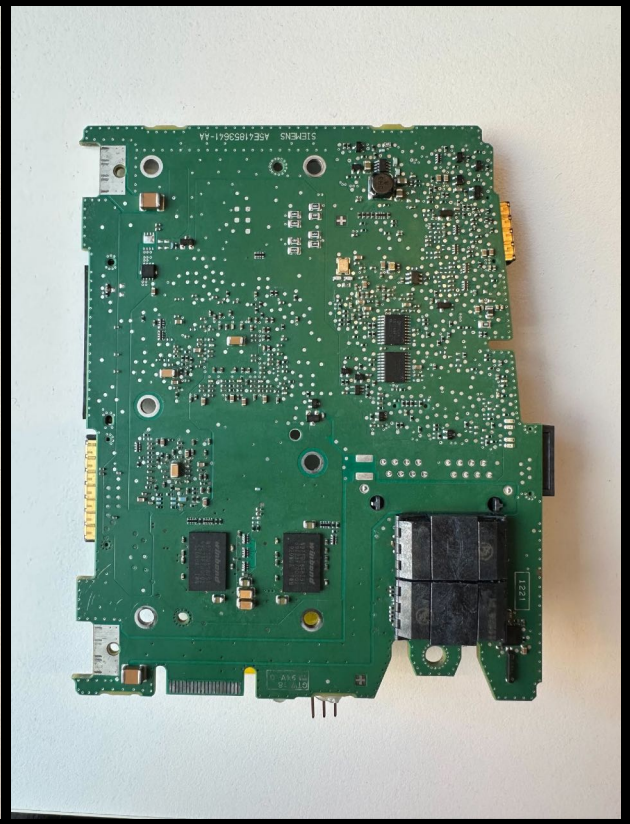
Current Prime Time PLC offering

Current design in service since 2012

Siemens ~= 31% global ICS marketshare

So the S7-1500 line runs.. Xyz% of the world today

# What’s the big deal with that board?

Custom SOC, integrated design, very good product “finishing”, ie no jtag, no uart, no obvious debug jumpers, basically BGA everything, encrypted flash bootloader code at rest.

Did not find debug/introspection interface, encrypted firmware at rest, what next?

# Did not find debug/introspection interface, encrypted firmware at rest, what next?


Fault injection?

Power, EM, Clock, etc. But no debug output

# Did not find debug/introspection interface, encrypted firmware at rest, what next?


Fault injection?

Power, EM, Clock, etc. But no debug output

Decap and do (???) fancy ninja stuff?

Each try costs ~$1,500USD, custom SoC screams extra complicated

# Did not find debug/introspection interface, encrypted firmware at rest, what next?


Fault injection?

Power, EM, Clock, etc. But no debug output

Decap and do (???) fancy ninja stuff?

Each try costs ~$1,500USD, custom SoC screams extra complicated

Try really really really hard to find jtag/debug interface?

Infinite loop –(

# Did not find debug/introspection interface, encrypted firmware at rest, what next?


Fault injection?

Power, EM, Clock, etc. But no debug output

Decap and do (???) fancy ninja stuff?

Each try costs ~$1,500USD, custom SoC screams extra complicated

Try really really really hard to find jtag/debug interface?

Infinite loop –(

Shout mean things at the board?

Shockingly ineffective

Build robot to rip its memory out at runtime, read its mind.

->

# “Cold boot” attacks well-known, well documented… they said.

Tradition Cold Boot Attack with DIMM slot and cooling spray[1]

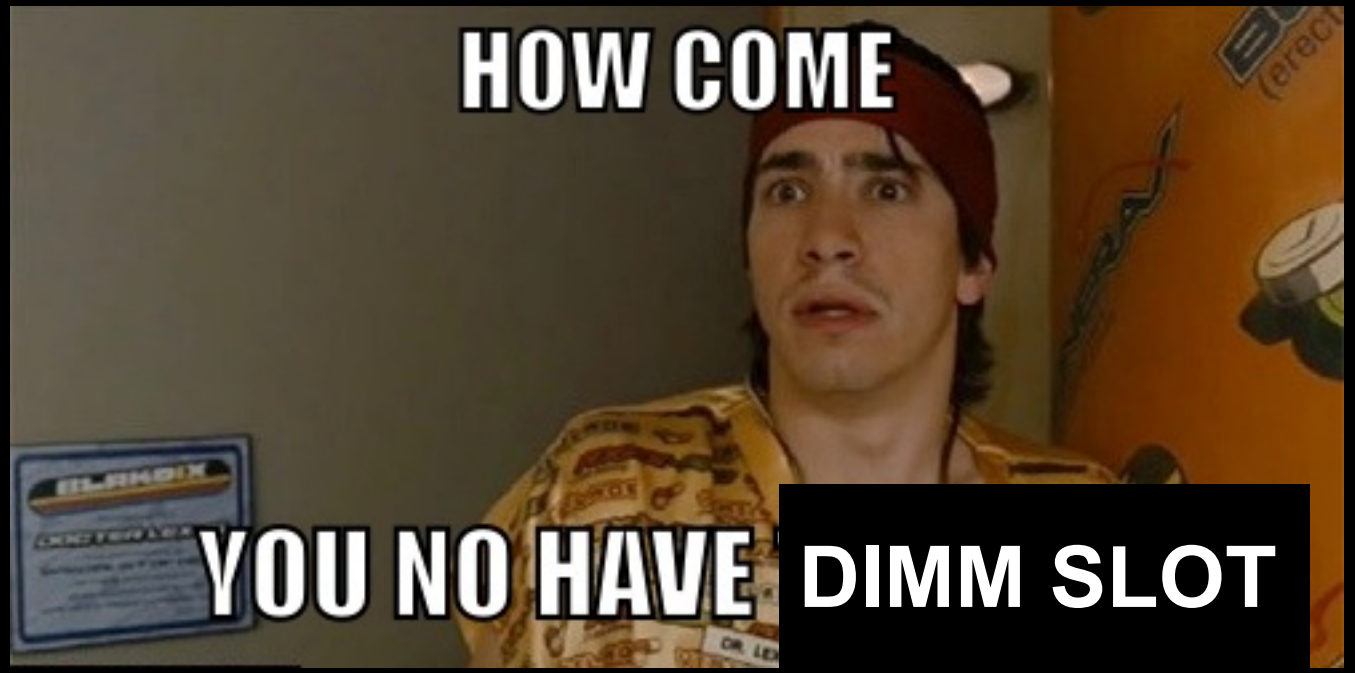
[1] Halderman, J. Alex, et al. "Lest we remember: cold-boot attacks on encryption keys." Communications of the ACM 52.5 (2009): 91-98.

# “Cold boot” attacks well-known, well documented… they said.

Tradition Cold Boot Attack with DIMM slot and cooling spray[1]


[1] Halderman, J. Alex, et al. "Lest we remember: cold-boot attacks on encryption keys." Communications of the ACM 52.5 (2009): 91-98.

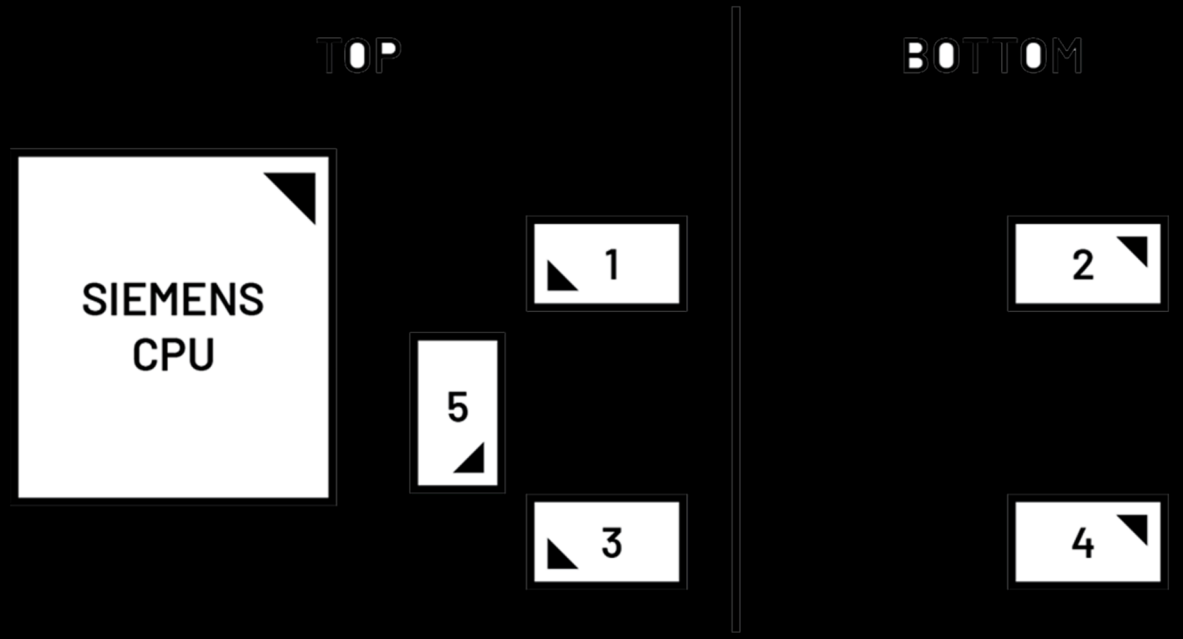
“Cold boot” attacks well-known, well documented… they said.




“Cold boot” attacks well-known, well documented… they said.

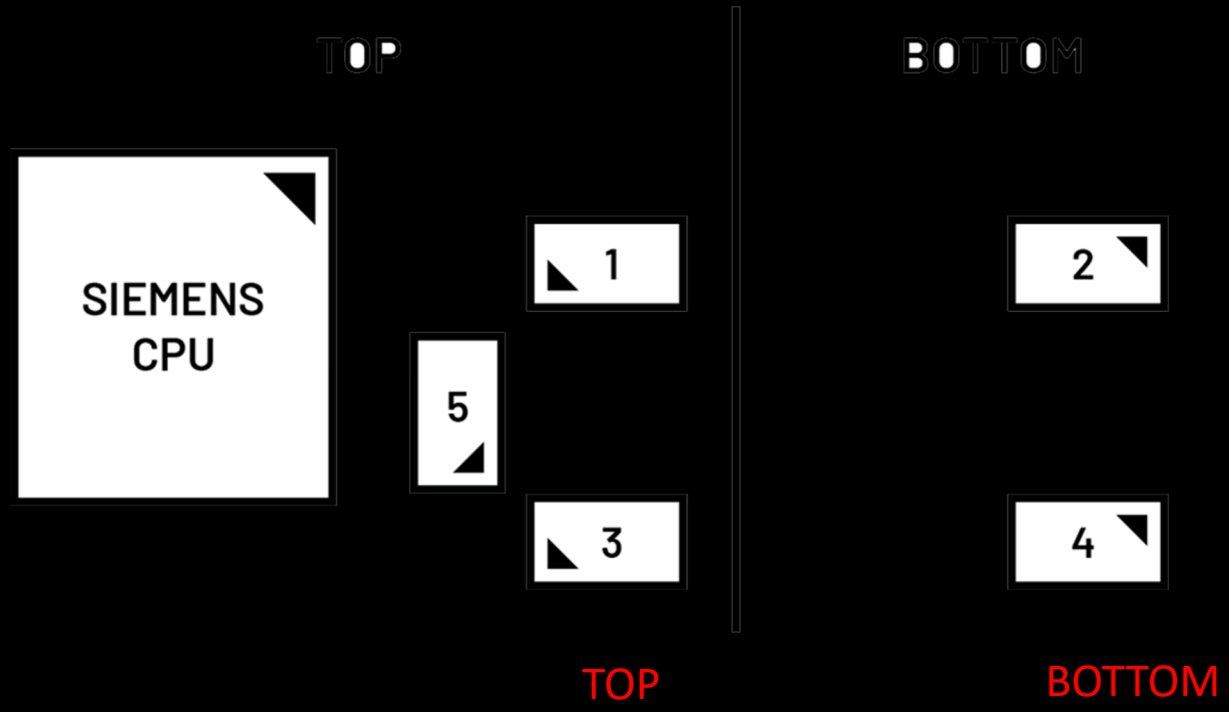

Things got more suck when we thought about it for more than 1 second.

“Cold boot” attacks well-known, well documented… they said.


5 LPDDR1 RAM chips

“Cold boot” attacks well-known, well documented… they said.

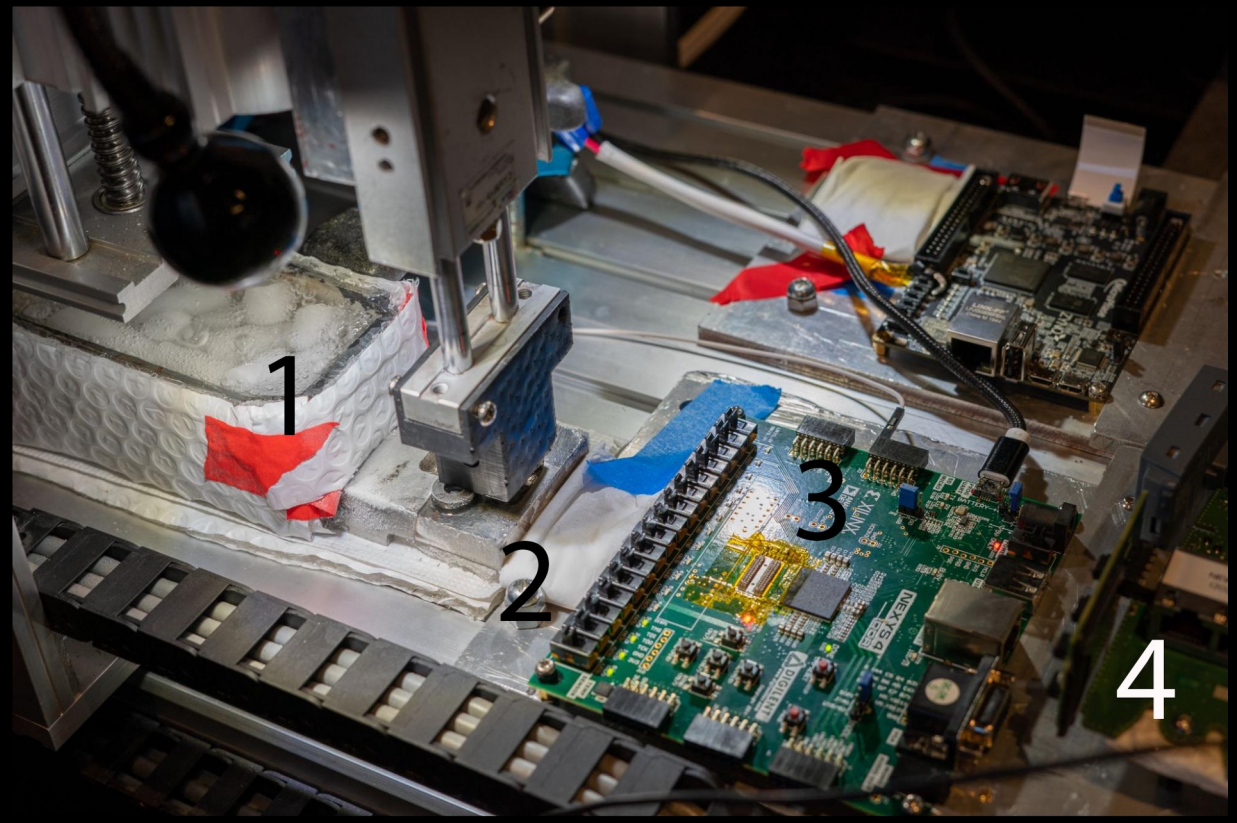




5 LPDDR1 RAM chips

# The plan


1. Frankenstein a CNC to mechanically remove memory chip at runtime
2. Rip each of 5 RAM chips at the same point in execution across multiple runs
3. Combine content of RAM dumps
4. ???
5. Read unencrypted boot code and.. win?

This talk focuses on practical tips. For more details, see WOOT 2023 paper




# Cryo-Mechanical RAM Content Extraction Against Modern Embedded Systems

Yuanzhe Wu
*Red Balloon Security*
New York, NY, USA
hans@redballoonsecurity.com

Grant Skipper
*Red Balloon Security*
New York, NY, USA
grant@redballoonsecurity.com

Ang Cui
*Red Balloon Security*
New York, NY, USA
ang@redballoonsecurity.com

***Abstract*—Cryogenic mechanical memory extraction provides a means to obtain a device's volatile memory content at runtime. Numerous prior works has have demonstrated successful exploitation of the Memory Remanence Effect on modern computers and mobile devices. While this approach is arguably one of the most direct paths to reading a target device's physical RAM content, several significant limitations exist. For example, prior works were done either on removable memory with standardized connectors, or with the use of a custom kernel/bootloader.**

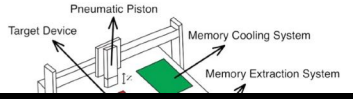
**We present a generalized and automated system that performs reliable RAM content extraction against modern embedded devices. Our cryo-mechanical apparatus is built using low-cost hardware that is widely available, and supports target devices using single or multiple DDR1|2|3 memory modules. We discuss several novel techniques and hardware modifications that allow our apparatus to exceed the spatial and temporal precision required to reliably perform memory extraction against modern embedded systems that have memory modules soldered directly onto the PCB, and use custom memory controllers that spread bits of each word of memory across multiple physical RAM chips.**

***Index Terms*—cold-boot, side-channel, memory extraction, reverse engineering, embedded security**

## I. Introduction

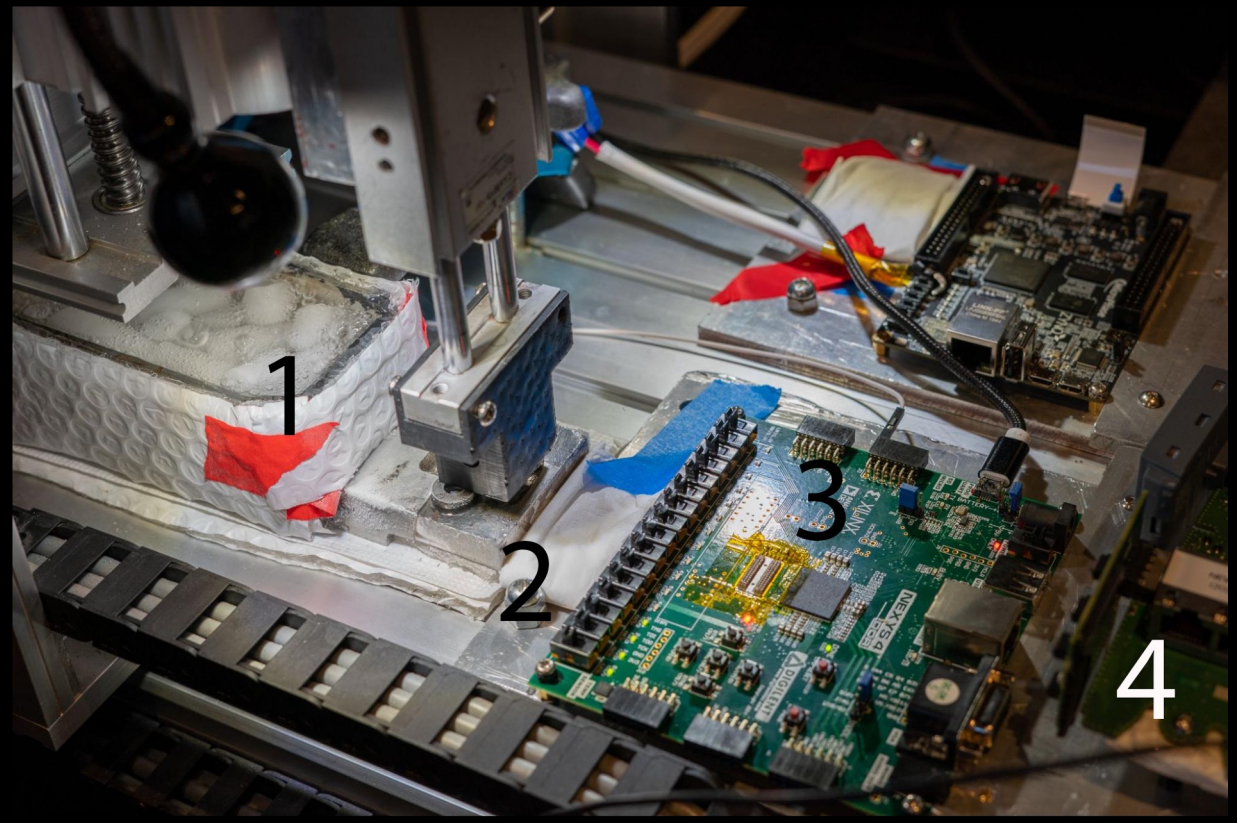
Modern high-performance embedded systems typically store firmware code in nonvolatile flash memory, and load the code into volatile dynamic random access memory (DRAM) during boot-up. The code and data contents of the device is often useful for security analysis. Firmware binaries can

rate (DDR)1, DDR2, and DDR3 memory modules. As shown in Figure 1, our system consists of a modified low-cost commercial off-the-shelf (COTS) computer numerical control (CNC) machine, a memory reader device implemented with an Field-Progammable-Gate-Array (FPGA), and controller implemented using an ESP32 [3] module and microPython [4]. This process involved cooling the memory chip, booting up the target device, physically transferring the chip to the readout platform, and recovering data. The entire apparatus can be built with widely available parts costing approximately $2,000 USD. The remainder of this paper discusses novel techniques and hardware modifications we developed to enable the described apparatus to perform reliable cryo-mechanical RAM content extraction on single and multi-memory-chip embedded devices. We demonstrate that our system can successfully perform memory extraction and reconstruction against an embedded device that uses a custom black-box memory controller and five physical RAM chips.




[1] Wu, Yuanzhe, Grant Skipper, and Ang Cui. "Cryo-Mechanical RAM Content Extraction Against Modern Embedded Systems." *17th IEEE Workshop on Offensive Technologies (WOOT).* San Francisco, CA, USA, 2023. [Online]. Available: https://wootconference.org/papers/woot23-paper3.pdf

# Took lots of tinkering, fast forward to a working solution




Build sufficiently precise linear actuation on a budget

Find magical BGA RAM socket

Active closed-loop RAM cooling

Memory extraction timing

FPGA DDR{1|2|3} RAM dumper

# Preciseish linear actuation

Store Home Products Sale Items Top Selling New Arrivals Feedback


CNC Router Lathe Mini CNC Engraving Machine 3020 C
Machine for Wood PCB Plastic Carving

**US $581.68** ~~US $1,002.90~~ 42% off

US $10.00 Off Store Coupon Get coupons

Quantity:

1

Additional 5% off (3 Sets or more)
70 Sets available

Ships to United States

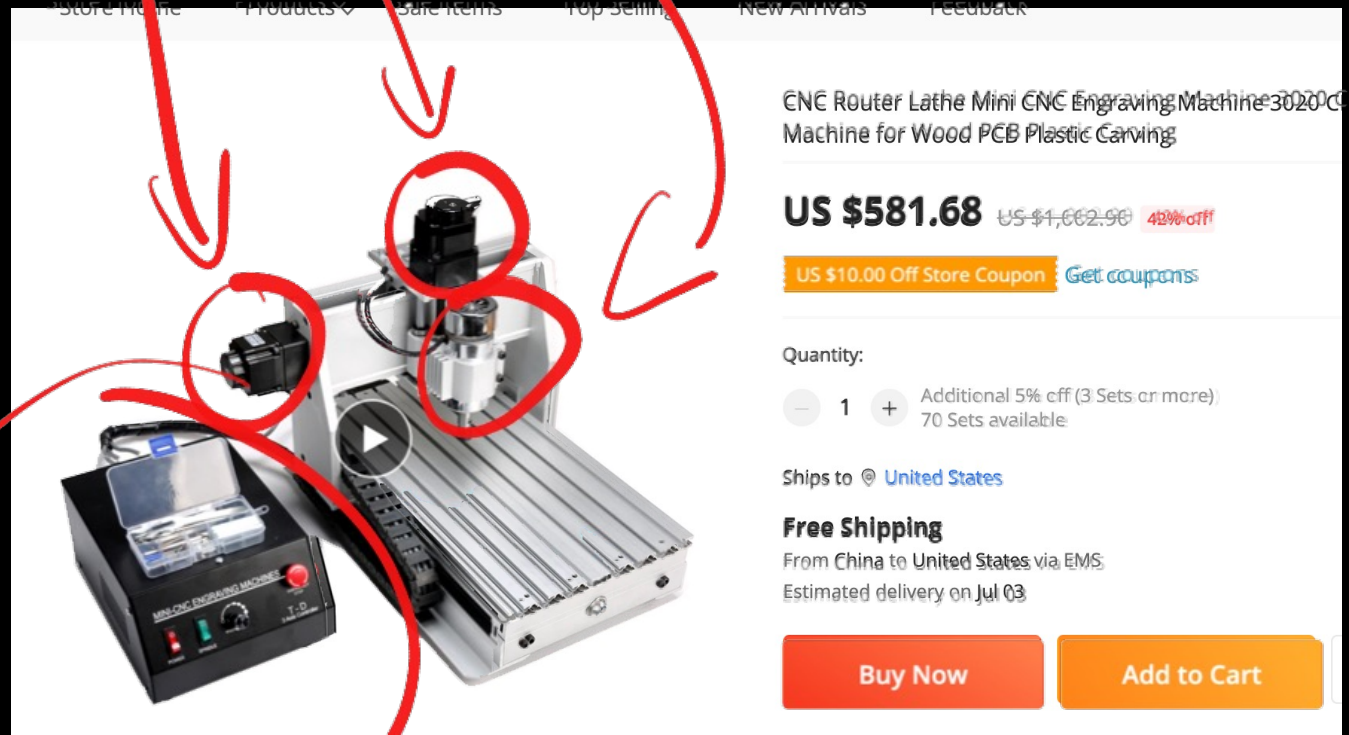
**Free Shipping**

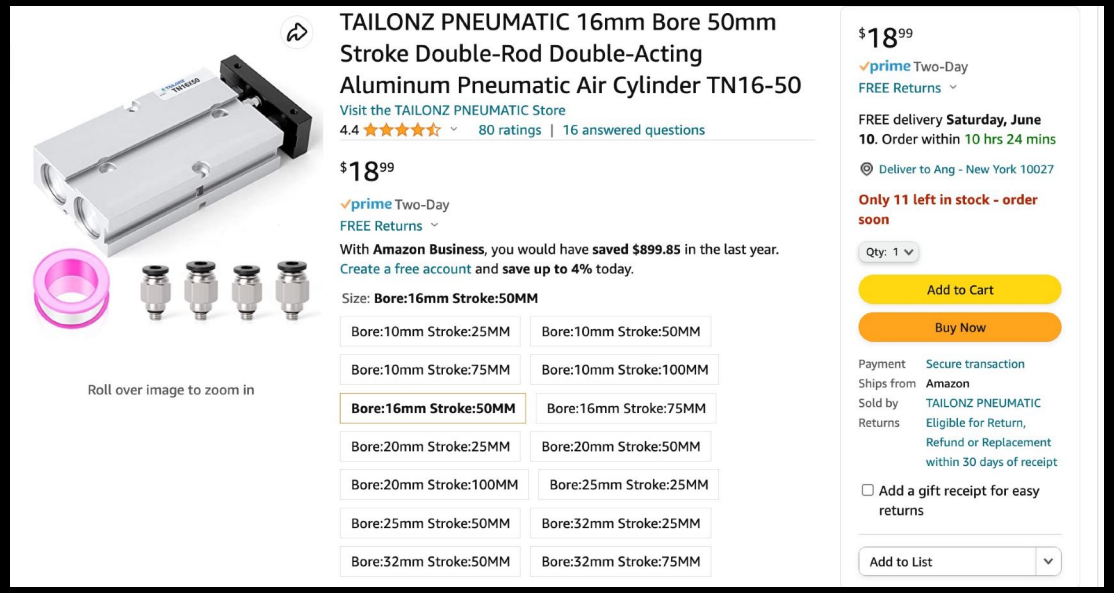
From China to United States via EMS

Estimated delivery on Jul 03

Buy Now Add to Cart

Junk This


Store Home
Products
Sale Items
Top Selling
New Arrivals
Feedback
CNC Router Lathe Mini CNC Engraving Machine 3020 C
Machine for Wood PCB Plastic Carving
US $581.68
US $1,662.96
42% off
US $10.00 Off Store Coupon
Get coupons
Quantity:
1
Additional 5% off (3 Sets or more)
70 Sets available
Ships to United States
Free Shipping
From China to United States via EMS
Estimated delivery on Jul 03
Buy Now
Add to Cart



TAILONZ PNEUMATIC 16mm Bore 50mm Stroke Double-Rod Double-Acting Aluminum Pneumatic Air Cylinder TN16-50

Visit the TAILONZ PNEUMATIC Store

4.4 ★★★★½ 80 ratings | 16 answered questions

$18.99

prime Two-Day

FREE Returns

With **Amazon Business**, you would have **saved $899.85** in the last year.
Create a free account and **save up to 4%** today.

Size: **Bore:16mm Stroke:50MM**

| | |
|---|---|
| Bore:10mm Stroke:25MM | Bore:10mm Stroke:50MM |
| Bore:10mm Stroke:75MM | Bore:10mm Stroke:100MM |
| **Bore:16mm Stroke:50MM** | Bore:16mm Stroke:75MM |
| Bore:20mm Stroke:25MM | Bore:20mm Stroke:50MM |
| Bore:20mm Stroke:100MM | Bore:25mm Stroke:25MM |
| Bore:25mm Stroke:50MM | Bore:32mm Stroke:25MM |
| Bore:32mm Stroke:50MM | Bore:32mm Stroke:75MM |

Roll over image to zoom in

$18.99

prime Two-Day

FREE Returns

FREE delivery **Saturday, June 10**. Order within 10 hrs 24 mins

Deliver to Ang - New York 10027

**Only 11 left in stock - order soon**

Qty: 1

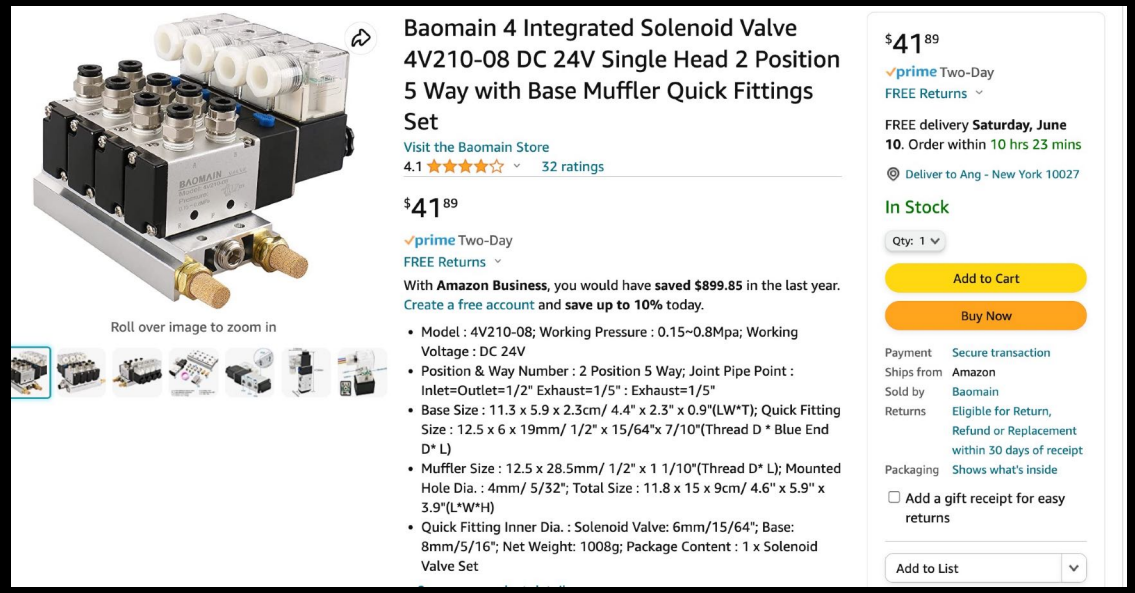
Add to Cart

Buy Now

Payment Secure transaction
Ships from Amazon
Sold by TAILONZ PNEUMATIC
Returns Eligible for Return, Refund or Replacement within 30 days of receipt

Add a gift receipt for easy returns

Add to List



Baomain 4 Integrated Solenoid Valve 4V210-08 DC 24V Single Head 2 Position 5 Way with Base Muffler Quick Fittings Set

Visit the Baomain Store

4.1 ★★★★☆ 32 ratings

$41.89

prime Two-Day

FREE Returns

With **Amazon Business**, you would have **saved $899.85** in the last year.
Create a free account and **save up to 10%** today.

- Model : 4V210-08; Working Pressure : 0.15~0.8Mpa; Working Voltage : DC 24V
- Position & Way Number : 2 Position 5 Way; Joint Pipe Point : Inlet=Outlet=1/2" Exhaust=1/5" : Exhaust=1/5"
- Base Size : 11.3 x 5.9 x 2.3cm/ 4.4" x 2.3" x 0.9"(LW*T); Quick Fitting Size : 12.5 x 6 x 19mm/ 1/2" x 15/64"x 7/10"(Thread D * Blue End D* L)
- Muffler Size : 12.5 x 28.5mm/ 1/2" x 1 1/10"(Thread D* L); Mounted Hole Dia. : 4mm/ 5/32"; Total Size : 11.8 x 15 x 9cm/ 4.6" x 5.9" x 3.9"(L*W*H)
- Quick Fitting Inner Dia. : Solenoid Valve: 6mm/15/64"; Base: 8mm/5/16"; Net Weight: 1008g; Package Content : 1 x Solenoid Valve Set

Roll over image to zoom in

$41.89

prime Two-Day

FREE Returns

FREE delivery **Saturday, June 10**. Order within 10 hrs 23 mins

Deliver to Ang - New York 10027

In Stock

Qty: 1

Add to Cart

Buy Now

Payment Secure transaction
Ships from Amazon
Sold by Baomain
Returns Eligible for Return, Refund or Replacement within 30 days of receipt
Packaging Shows what's inside

Add a gift receipt for easy returns

Add to List

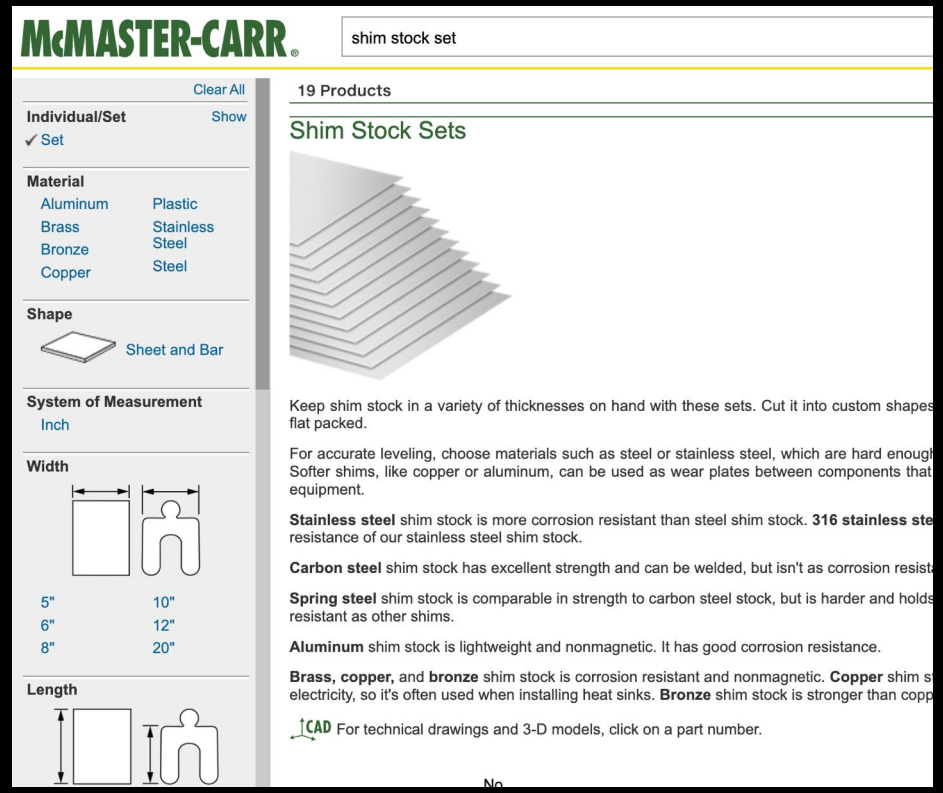
Used Pneumatic actuator for Z axis (memory chip mover)

10 PSI sweet spot


Things look square and parallel. But they are probably not.

Oh. Learn to turn screws the right way. No joke –(

You'll need a near infinite source of..




+ Patience

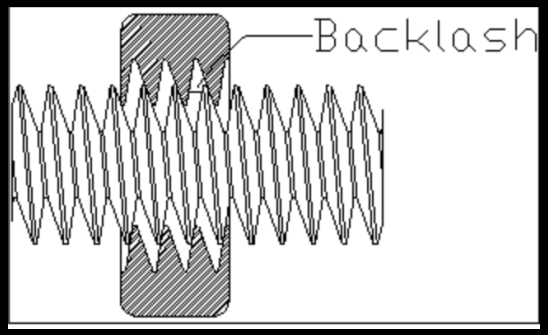
# Machine stuff – linear motion actuation and its discontents –(

# Machine stuff – linear motion actuation and its discontents –(

How does it know where it is? Steppers crave steps, but how far does each step move?

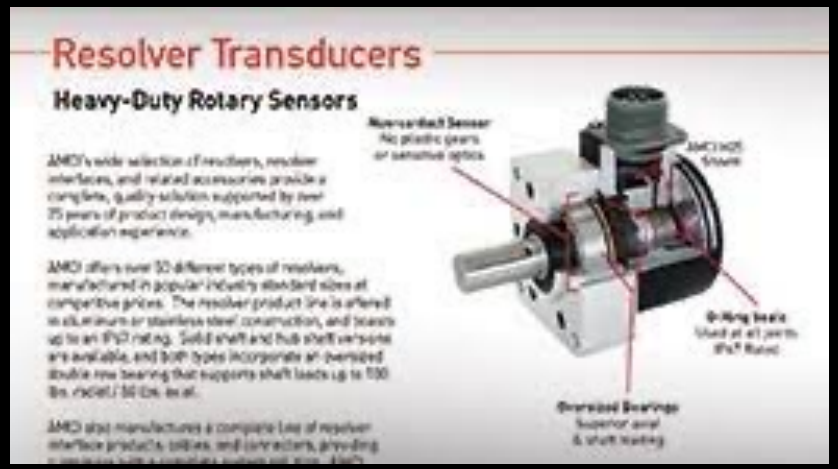
# Machine stuff – linear motion actuation and its discontents –(

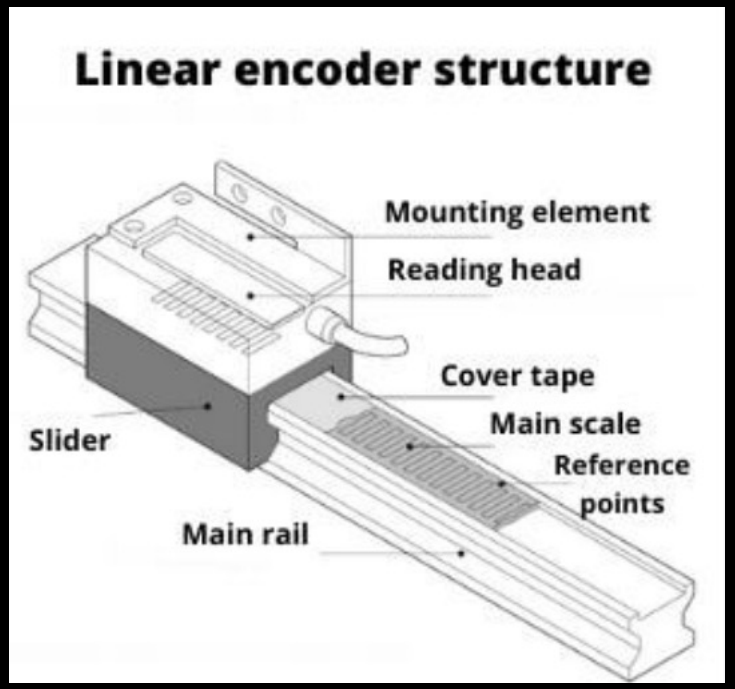
How does it know where it is? Steppers crave steps, but how far does each step move?

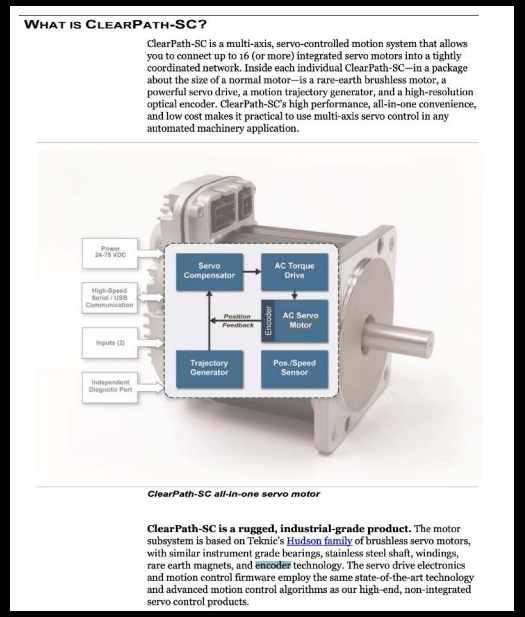

https://www.machinetoolhelp.com/Repairing/What_is_backlash.html

The right answer is simple. Convert money into luxurious hardware



Get 2x of these ~$300USD each



## What is ClearPath-SC?

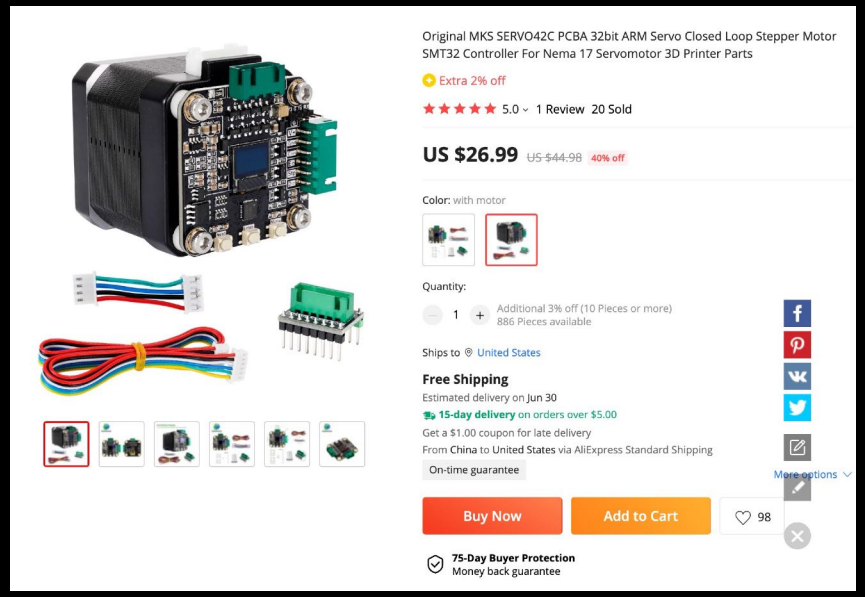
ClearPath-SC is a multi-axis, servo-controlled motion system that allows you to connect up to 16 (or more) integrated servo motors into a tightly coordinated network. Inside each individual ClearPath-SC—in a package about the size of a normal motor—is a rare-earth brushless motor, a powerful servo drive, a motion trajectory generator, and a high-resolution optical encoder. ClearPath-SC's high performance, all-in-one convenience, and low cost makes it practical to use multi-axis servo control in any automated machinery application.



*ClearPath-SC all-in-one servo motor*

**ClearPath-SC is a rugged, industrial-grade product.** The motor subsystem is based on Teknic's Hudson family of brushless servo motors, with similar instrument grade bearings, stainless steel shaft, windings, rare earth magnets, and encoder technology. The servo drive electronics and motion control firmware employ the same state-of-the-art technology and advanced motion control algorithms as our high-end, non-integrated servo control products.

OR



Original MKS SERVO42C PCBA 32bit ARM Servo Closed Loop Stepper Motor SMT32 Controller For Nema 17 Servomotor 3D Printer Parts

Extra 2% off

5.0 · 1 Review 20 Sold

US $26.99 ~~US $44.98~~ 40% off

Color: with motor

Quantity: 1 Additional 3% off (10 Pieces or more) 886 Pieces available

Ships to United States

Free Shipping

Estimated delivery on Jun 30

15-day delivery on orders over $5.00

Get a $1.00 coupon for late delivery

From China to United States via AliExpress Standard Shipping

On-time guarantee

More options

Buy Now | Add to Cart | 98

75-Day Buyer Protection
Money back guarantee

Close-looped control = magical way to

convert

$$ and sub average linear motion hardware

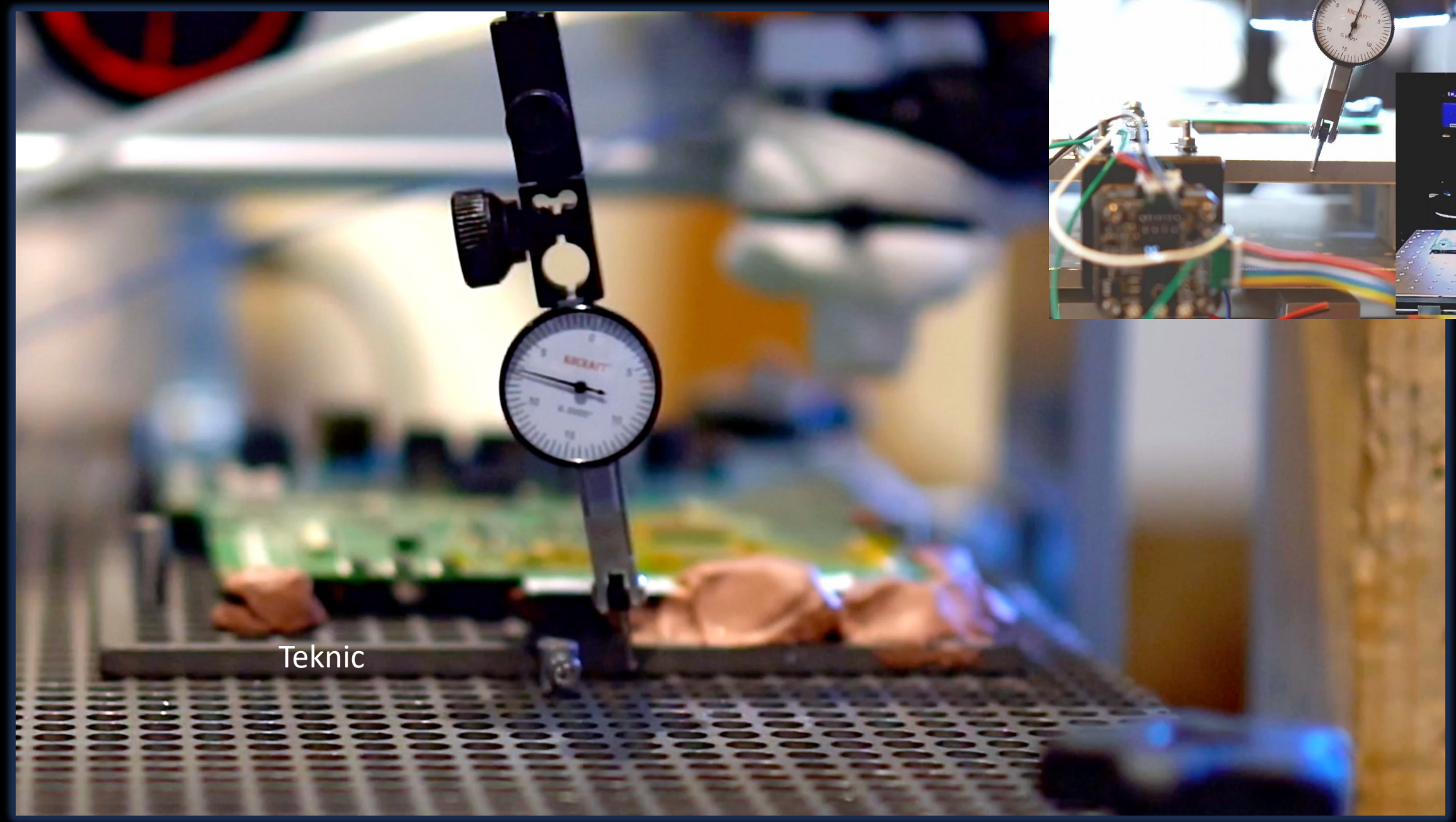
Alternatively,

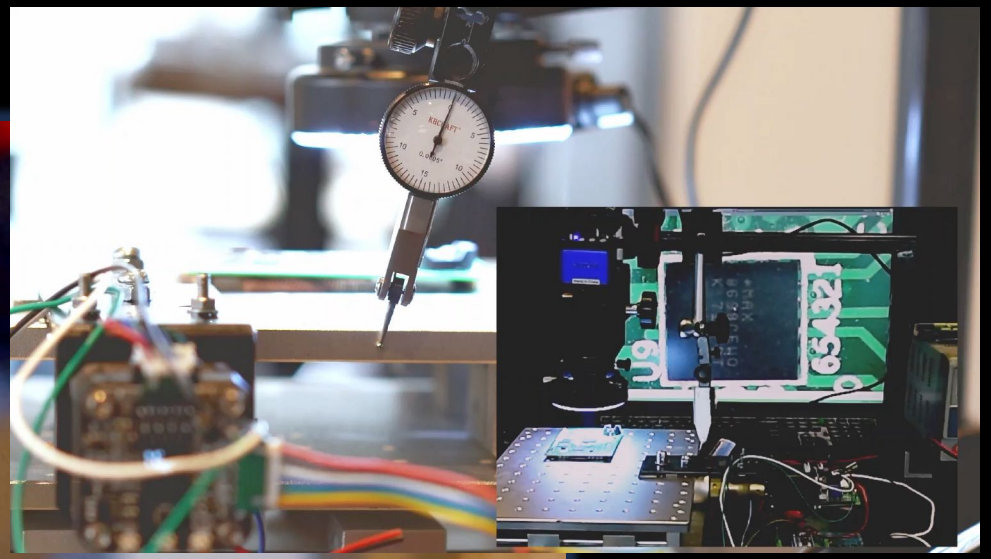
into

Fantastic precision motion machines

SC = Software Control
I'd get these over MCVP models

https://teknic.com/files/downloads/Clearpath-SC%20User%20Manual.pdf



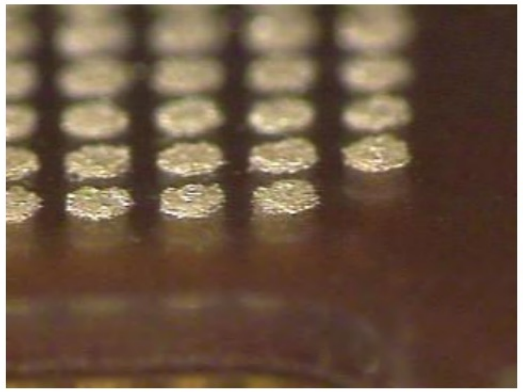
MKs Servo42

# Magical BGA RAM Socket

# Magical BGA RAM Socket

## Silver Ball Matrix Elastomer Socket

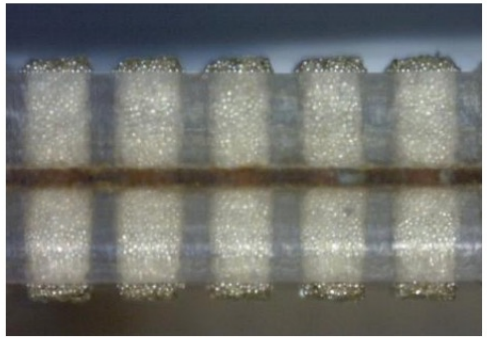
### SM Interposer



Array of Columns

Elastomer Matrix

Compliant Buttons



Cross Section

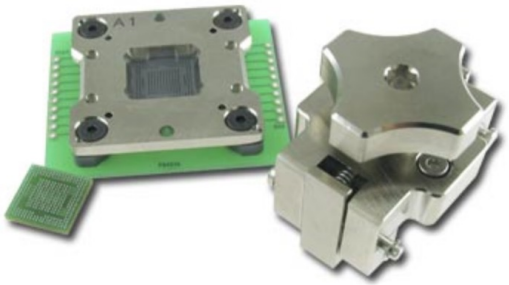
Silver Particles

Patented Core

Ironwood ELECTRONICS
www.ironwoodelectronics.com

ypical specifications for the SM/SMP contact technology include:

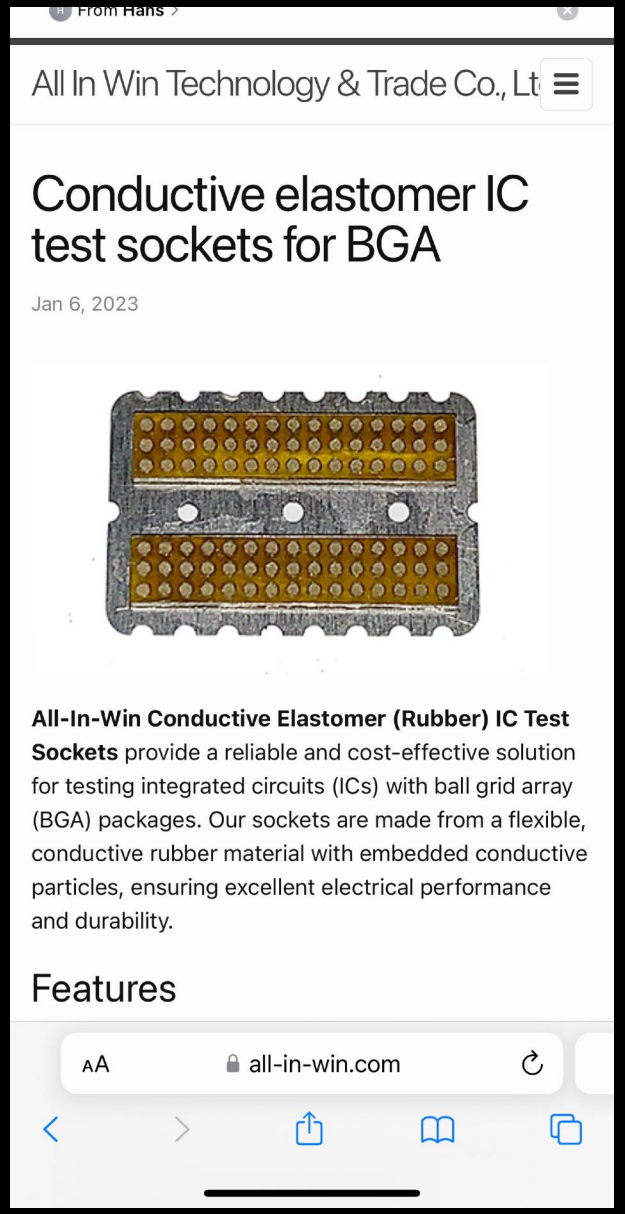
- Over 40GHz bandwidth @-1dB for edge pins
- Contact resistance under 15mOhms
- Self inductance under 0.21nH
- Capacitance under 0.15pF
- Operating temperature range -55C to +150C
- Insertion/Extraction life over 500, 000 cycles with protective plunger matrix
- Current rating at 14C temperature rise is 4 Amps per pin



C9797and_C9798a_midsize

-55C!

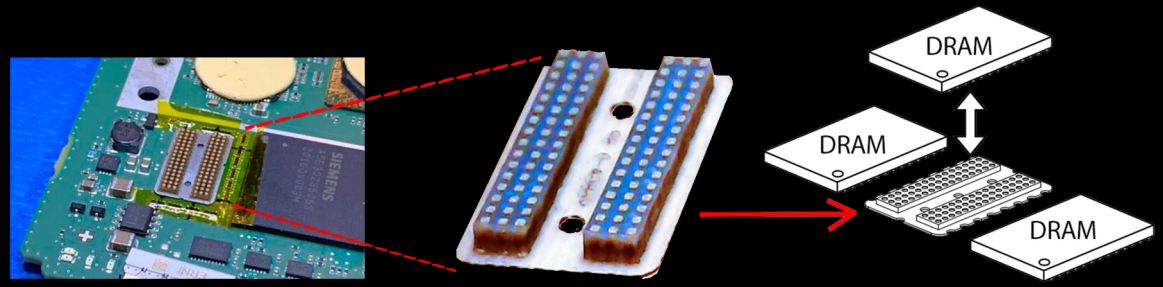
Get a lot of these





- For this many sockets

<- This much money

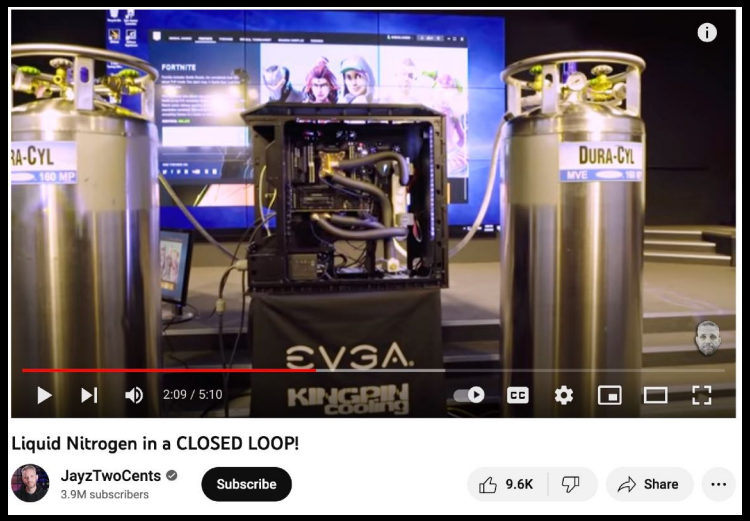


# Active, closed-loop, RAM cooling

# Active, closed-loop, RAM cooling



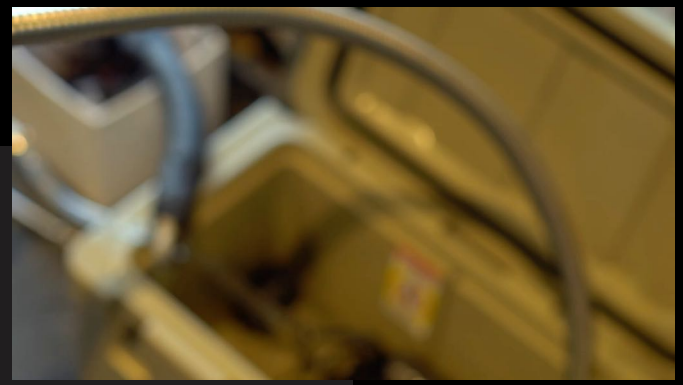
LOL?

# Active, closed-loop, RAM cooling

# Active, closed-loop, RAM cooling

# Active, closed-loop, RAM cooling

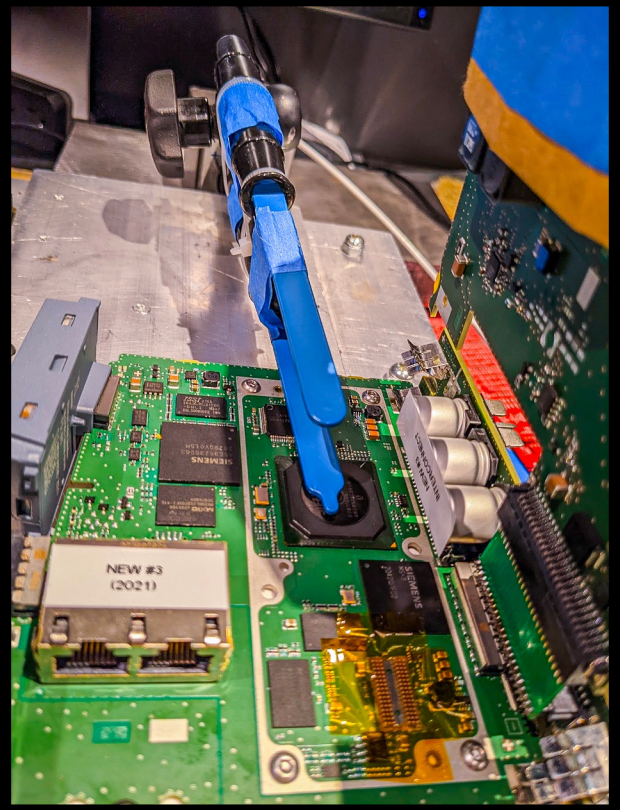


# Memory Extraction Timing

# Memory Extraction Timing

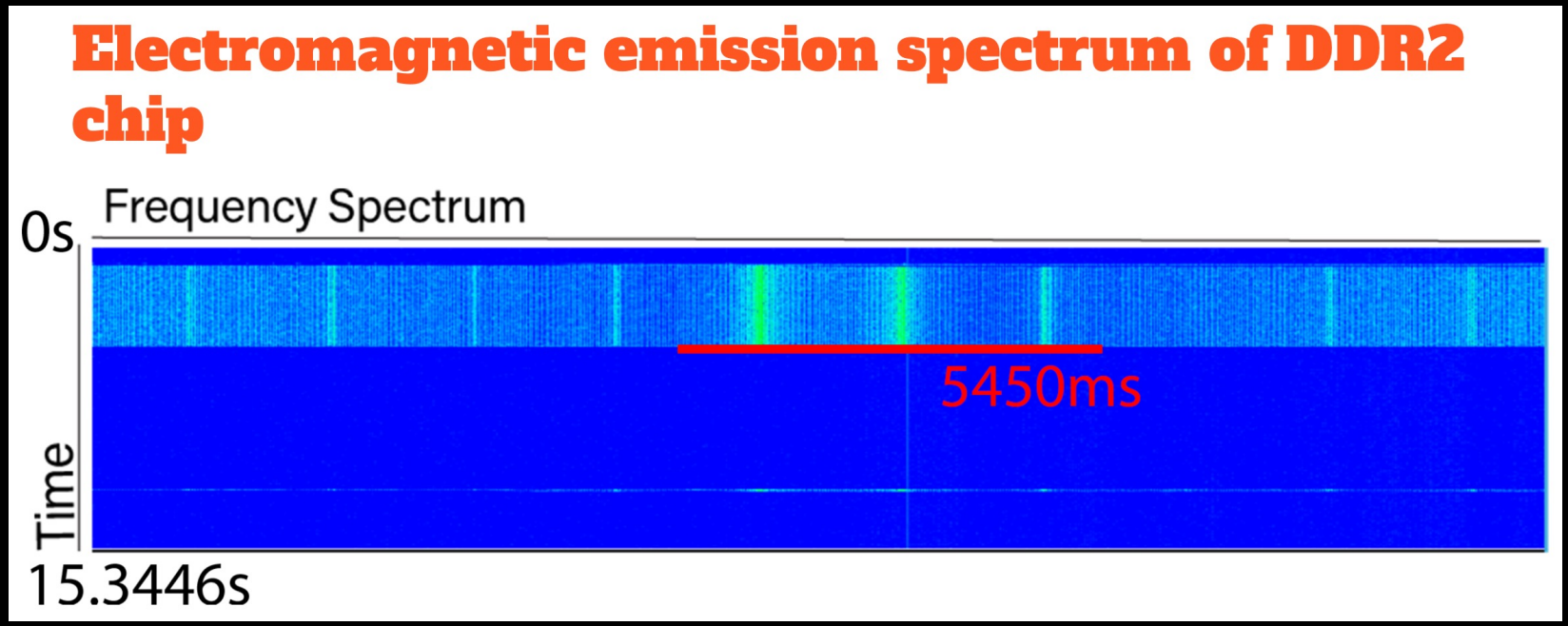
Pull memory 5 times at the same point in execution. Naïve approach timing precision ~100ns?

# Memory Extraction Timing

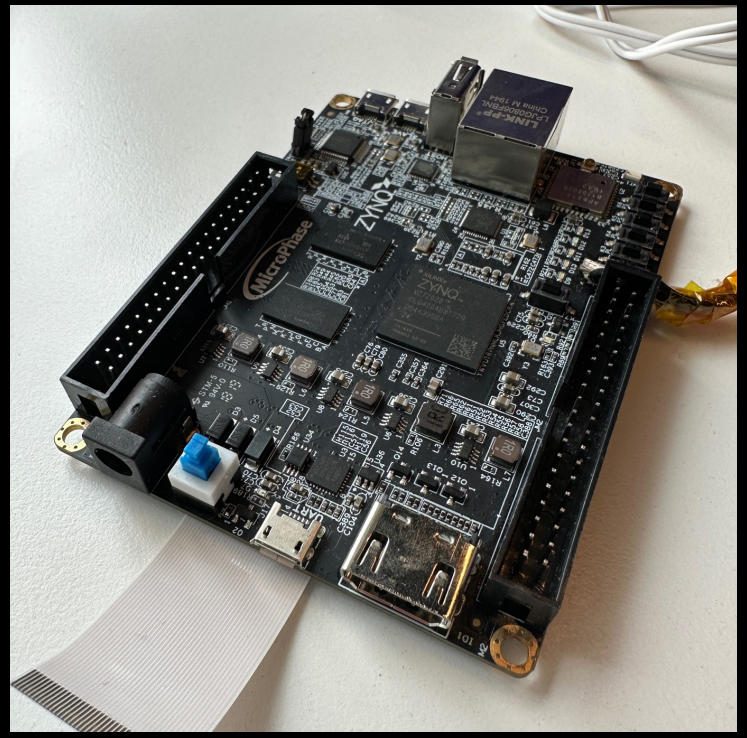


Pull memory 5 times at the same point in execution. Naïve approach timing precision ~100ns?

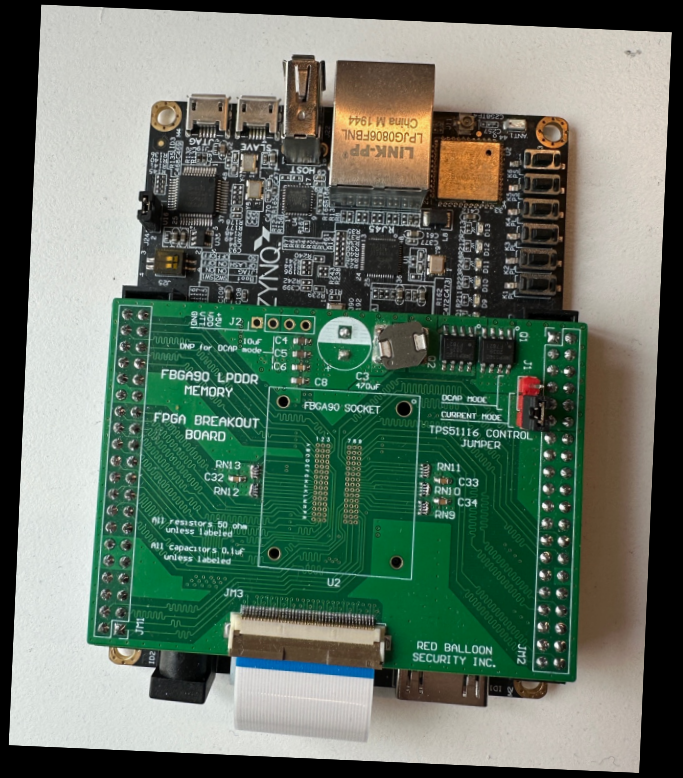
Find periods of CPU bound execution because..



# FPGA DDR{1|2|3} Dumper

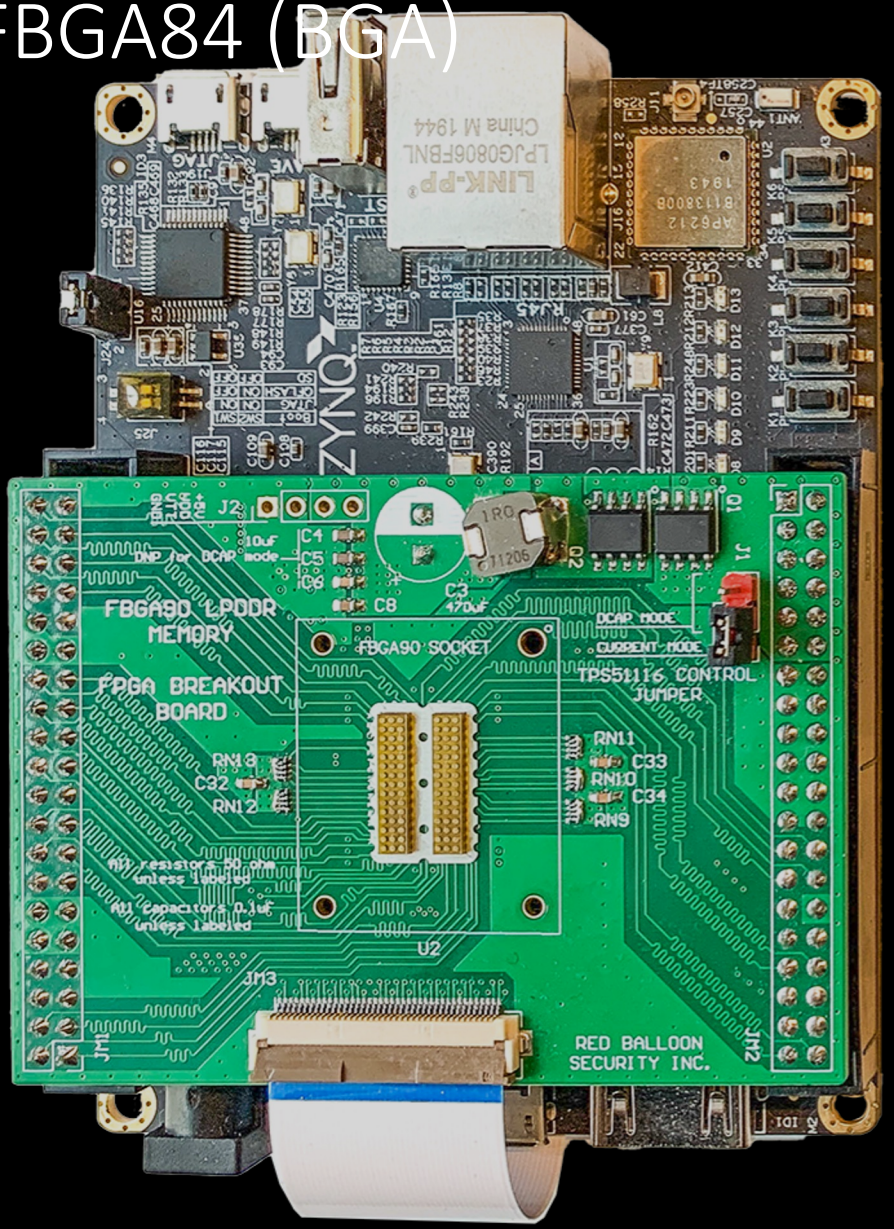


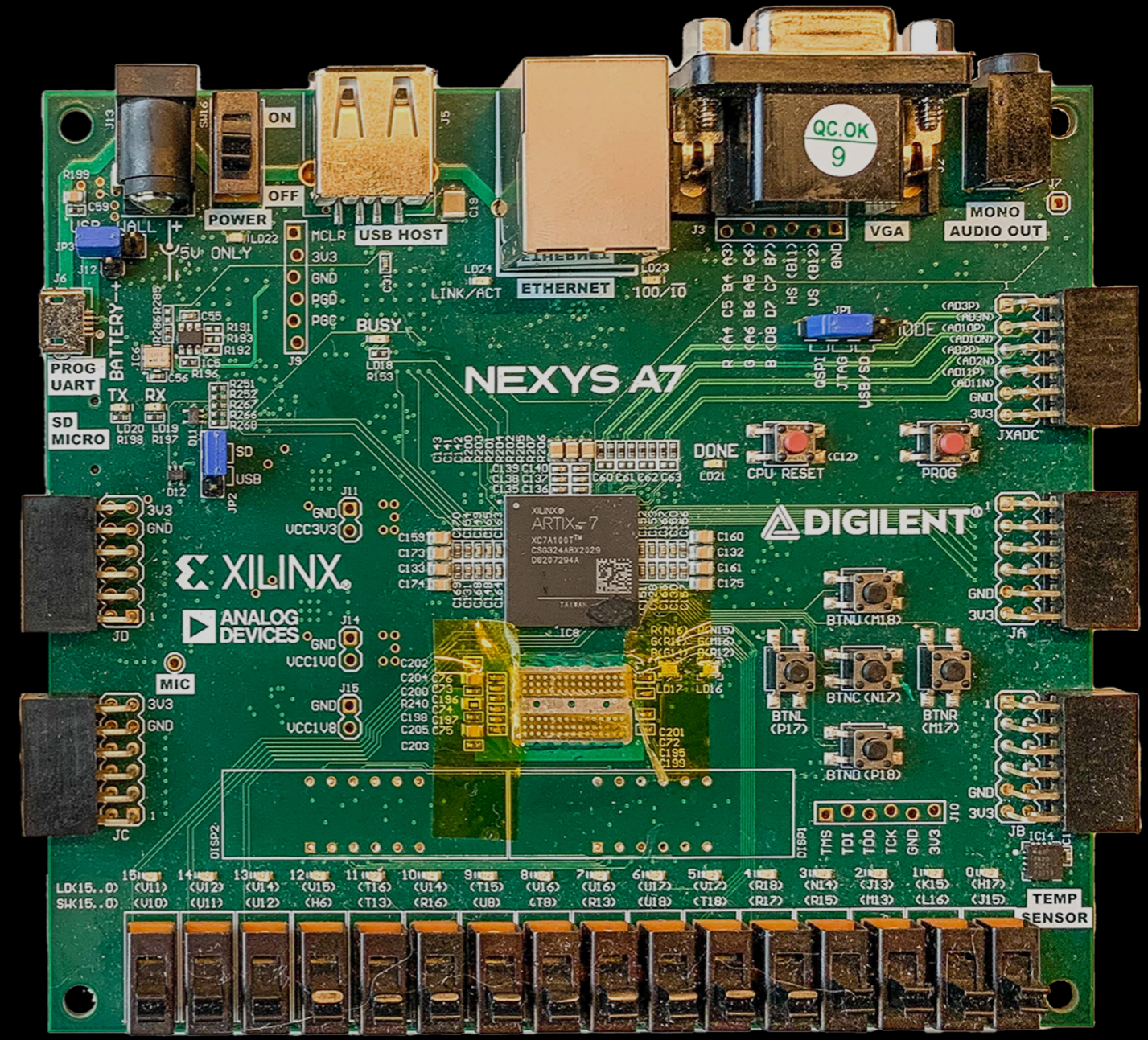

ZYNQ Base Board for DDR and LPDDR

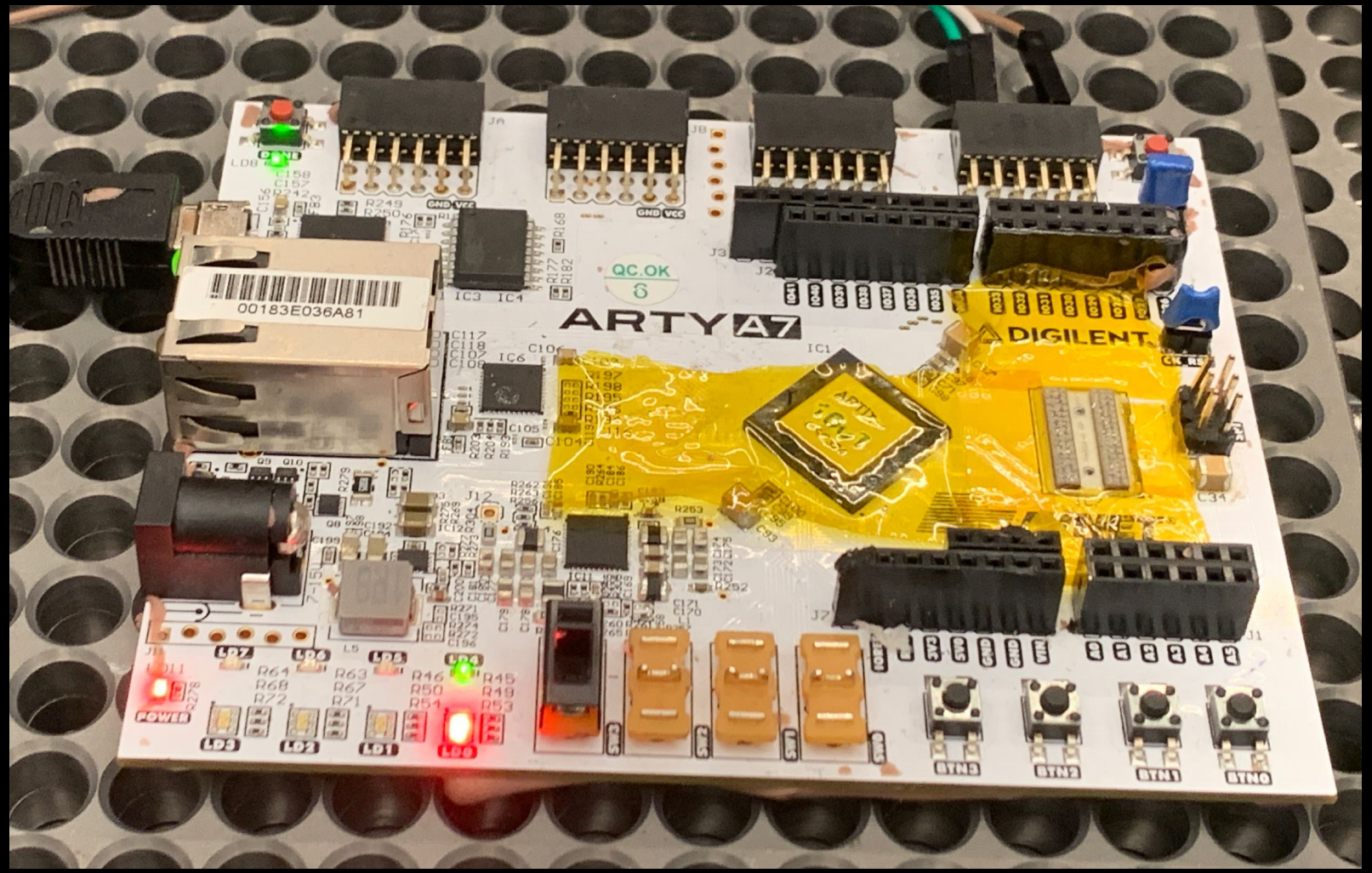



LPDDR1 Adaptor Board on FPGA

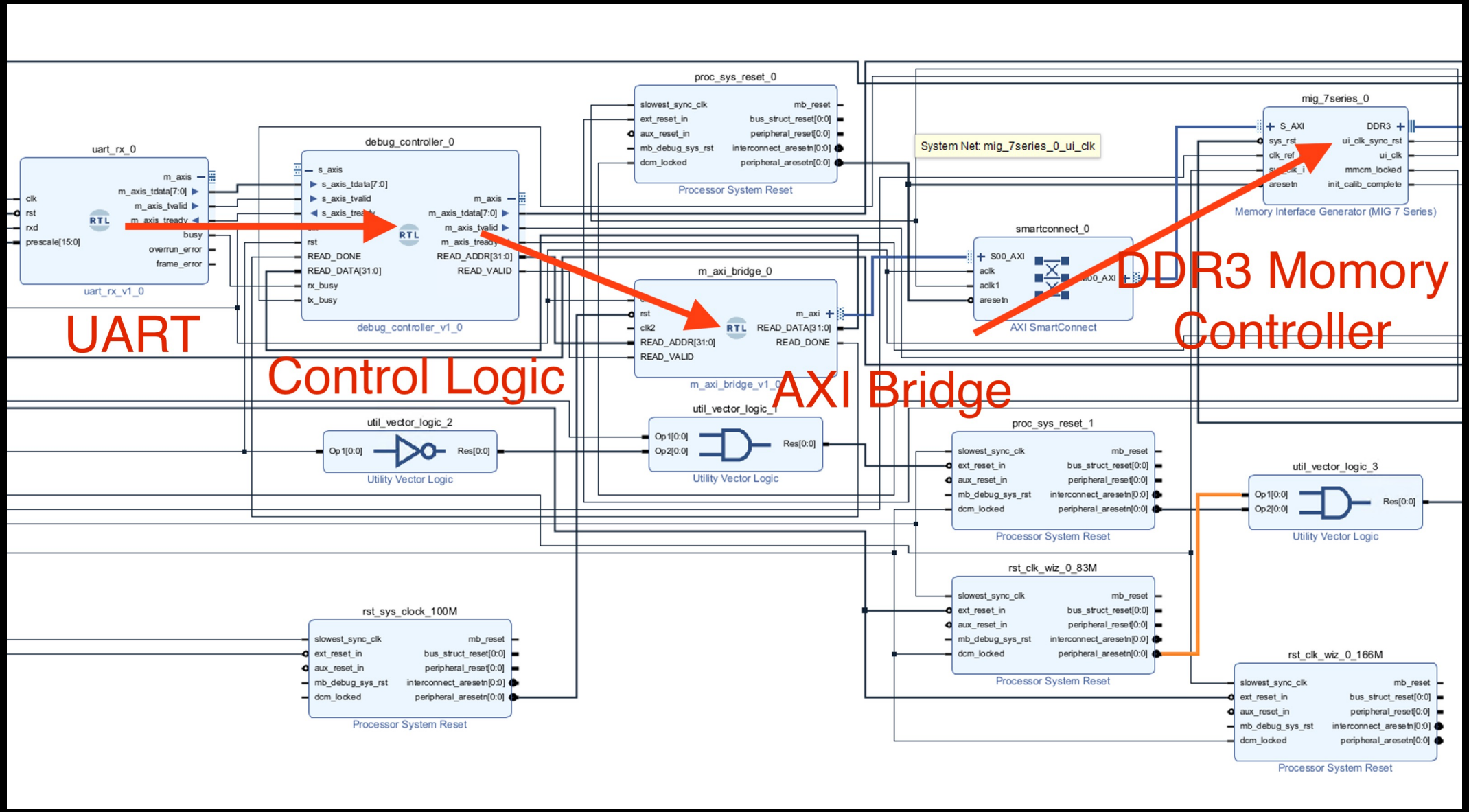
# LPDDR1 → DDR2
# FBGA84 (BGA)






# DDR3 FBGA96 (BGA)

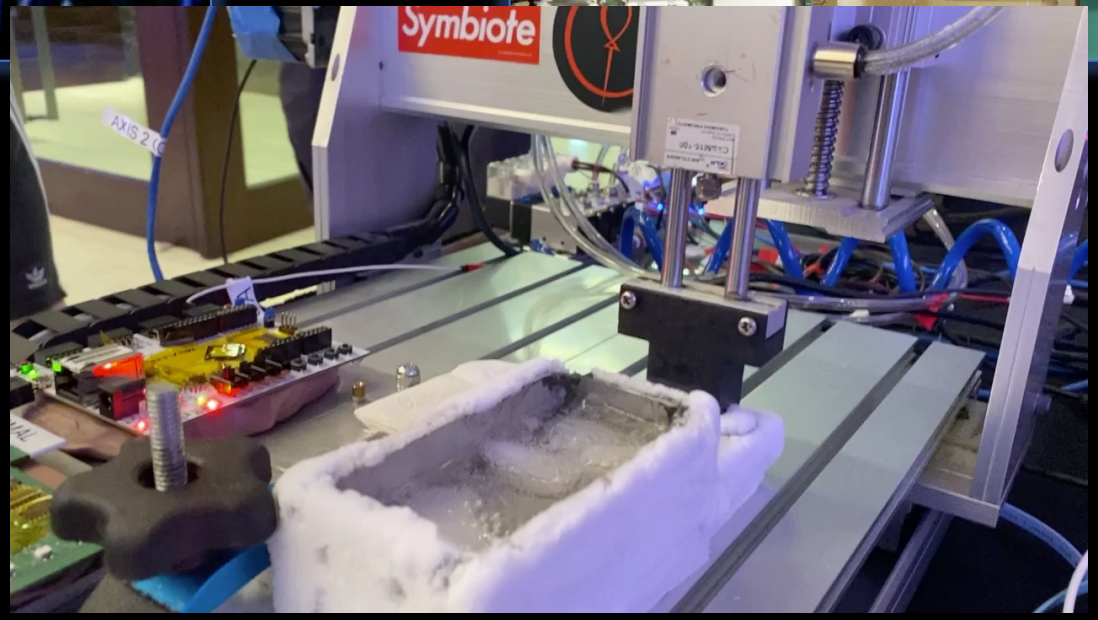



Xilinx FPGA Design

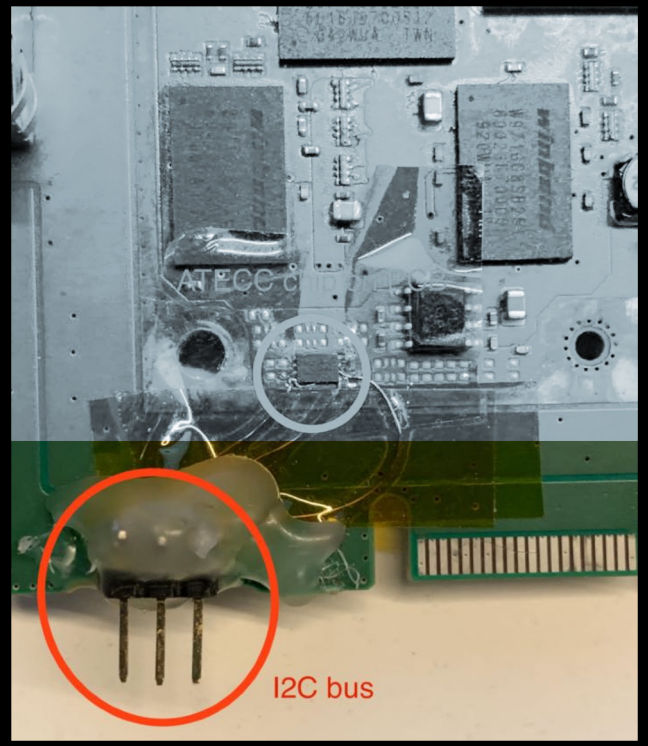
# Let’s review

| | |
|---|---|
| Build sufficiently precise linear actuation on a budget | Win |
| Find magical BGA RAM socket | Win |
| Active closed-loop RAM cooling | Win |
| Memory extraction timing | Win |
| FPGA DDR{1\|2\|3} RAM dumper | Win |

And with the magic of friendship, and after 7 months of failing



And the S7-1500…




Symmetric encryption instead of signature verification

ATECC i2c chip..