

Dasharo Features

Dasharo User Group #1

Michał Żygowski

What is this presentation gonna be about?

Current status and feature plans for:

- Supermicro X11SSH (server)
- Dell OptiPlex 7010/9010 (desktop)
- Dell Precision T1650 (desktop/NAS)
- MSI Z690-A/Z790-P (desktop)

DASHARO COMMUNITY SUPPORT ROADMAP (*subject to change*)

		2023			
		Q1	Q2	Q3	Q4
Server	Supermicro	X11SSH-TF v0.1.0		X11SSH-TF v0.1.0	X11SSH-TF v0.1.0
		- Basic Dasharo System Features - UEFI Secure Boot improvements - IPMI Serial-over-LAN - iKVM keyboard		- Extend OSFV support over IPMI for BMC-based platforms - Debian 11 - XCP-ng 8.2 LTS	- coreboot 4.19 - iPXE 2022.01 - EDK II 202002

Discovery

Evaluation

Porting

Validation

Community Release

Supporters Release



v0.1.0 Community Release

Current status: **Porting**

- We have a working release candidate
- X11SSH-TF installed in the 3mdeb lab
- Basic Dasharo System Features and UEFI boot included
- iKVM keyboard does not want to work in the firmware, but does in OS (needs debugging)
- SOL works, Debian 11 checked and working
- **Sh*t tons** of ways of flashing with SUM, SMCIPICTool, flashrom, BMC GUI but **only BMC GUI** is working properly (and yet not always)...
- iKVM keyboard fix and some documentation is needed to switch to **Validation**



What's next? v0.2.0

Features ideas for next release:

- UEFI IPMI drivers for OOB management, SMBus ASF, BMC event logging?
- OpenBMC port? There are [Supermicro open-source packages](#) which resemble a BMC project (to be analyzed)





		DASHARO COMMUNITY SUPPORT ROADMAP (<i>subject to change</i>)				
		2023				
		Q1	Q2	Q3	Q4	
Desktops	Dell	OptiPlex 7010/9010 v0.1.0	OptiPlex 7010/9010 v0.1.0			
		- OSFV support for Dell desktop - XCP-ng 8.2 LTS	- coreboot 4.17 - iPXE 2022.01 - EDK II 202002			
		Precision T1650 v0.1.0	Precision T1650 v0.1.0	Precision T1650 v0.1.0		
		- Basic Dasharo System Features - UEFI Secure Boot improvements	- Add T1650 to Dasharo Lab Infrastructure - TrueNAS CORE 13.0 - ECC - SMBIOS UUID migration	- coreboot 4.19 - iPXE 2022.01 - EDK II 202002		
		Discovery				
		Evaluation				
		Porting				
		Validation				
		Community Release				
		Supporters Release				

Dasharo Community Support Roadmap | March 2023 (v0.1) | CC-BY-SA 4.0



v0.1.0 Community Release

Current status: **Validation**



- We have a working release candidate for quite some time
- Basic Dasharo System Features and UEFI boot included
- SMBIOS UUID and serial number migration
- Need to perform testing to finally switch to **Release** phase
- [GitHub v0.1.0 milestone](#)
- [GitHub Project](#)



What's next? v0.2.0

Feature ideas for next release:



- We don't know yet :)
- Ideas welcome
- Most likely inclusion of features developed for other platforms



v0.1.0 Community Release

Current status: **Porting**



- Board support available in upstream coreboot
- Nothing started yet so we need to prepare everything:
 - Whole documentation
 - Dasharo System Features enabling
 - installation in 3mdeb lab
- [GitHub v0.1.0 milestone](#)
- [GitHub Project](#)

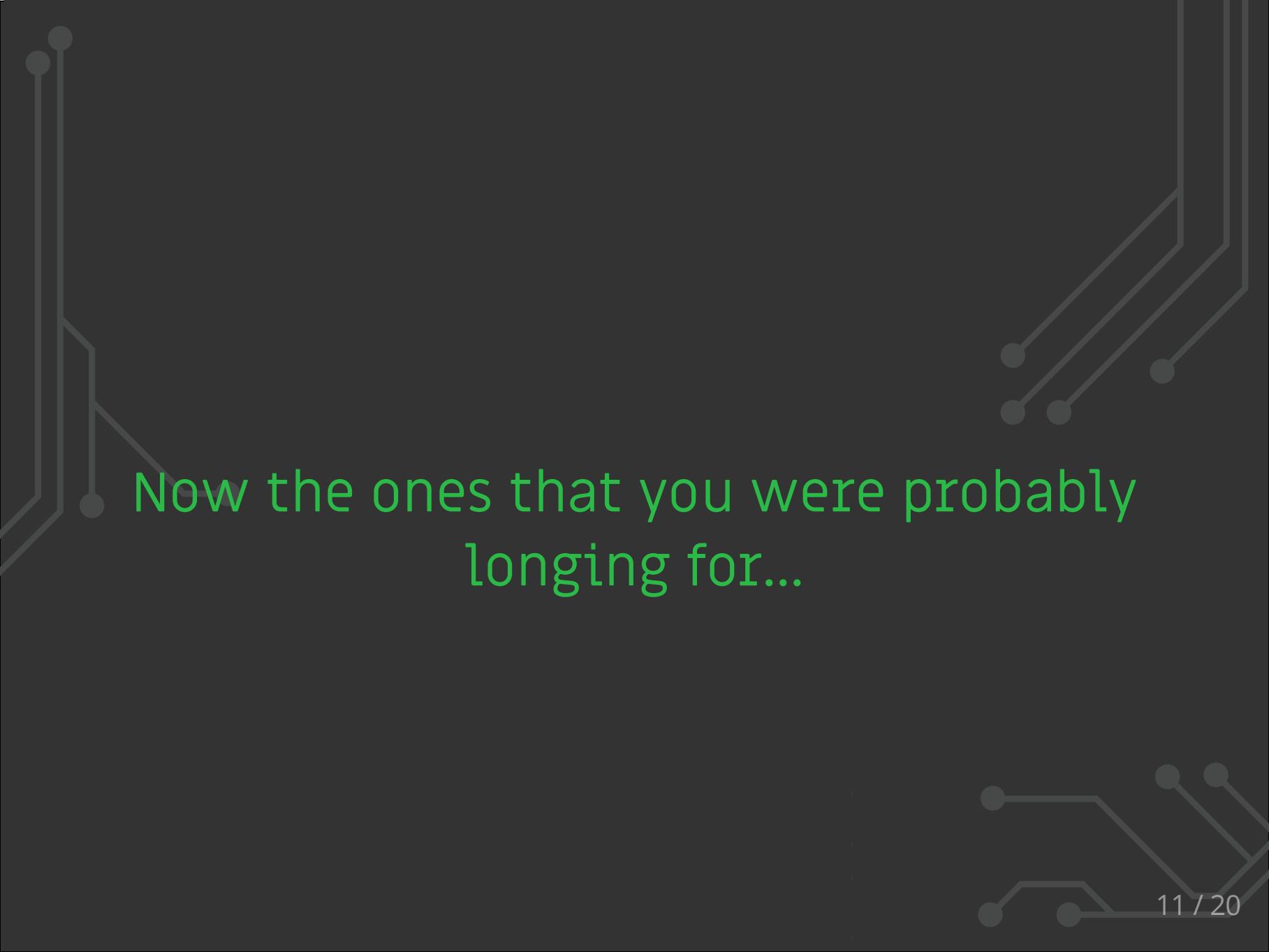


What's next? v0.2.0

Feature ideas for next release:



- Precision T1650 would be specifically intended for NAS use due to ECC RAM, so it needs a runtime option to configure platform behavior after power failure
- Most likely inclusion of features developed for other platforms



Now the ones that you were probably
longing for...

DASHARO COMMUNITY SUPPORT ROADMAP (*subject to change*)

		2023				2024			
		Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
Desktop	MSI	PRO Z690-A v1.1.1	PRO Z690-A v1.1.2	PRO Z690-A v1.1.2					
		- Qubes OS 4.1.2 - Early DMA protection - GPU HCL fixes - SATA hot-plug and more	- RPL-S CPU support - FlashBIOS button support - MSI Windows 11 SW and drivers support	- coreboot 4.18 - iPXE 2022.01 - EDK II 202002					
				PRO Z690-A v1.2.0	PRO Z690-A v1.2.0				
				- v1.1.2 feature parity	- v1.1.2 feature parity				
		PRO Z790-P v1.0.0		PRO Z790-P v1.0.0	PRO Z790-P v1.0.0	PRO Z790-P v1.0.0			
		- NLNet grant application		- feature parity with PRO Z690-A	- feature parity with PRO Z690-A	- coreboot 4.21 - iPXE 2022.01 - EDK II 202002			

Discovery
Evaluation
Porting
Validation
Community Release
Supporters Release



v1.1.2 - Supporters Release

Current status: Validation

- RPL-S CPU support in review upstream (not tested yet)
- MSI ACPI identification in Windows 11 to install MSI software and drivers automatically (done)
- ACPI interrupt routing fix (done) - my dual dGPU setup pays off...
- Fan control (almost finished) - few weekends gone, just like that...
- FlashBIOS button (in progress) - yessss...
- [GitHub v1.1.2 milestone](#)
- [GitHub Project](#)

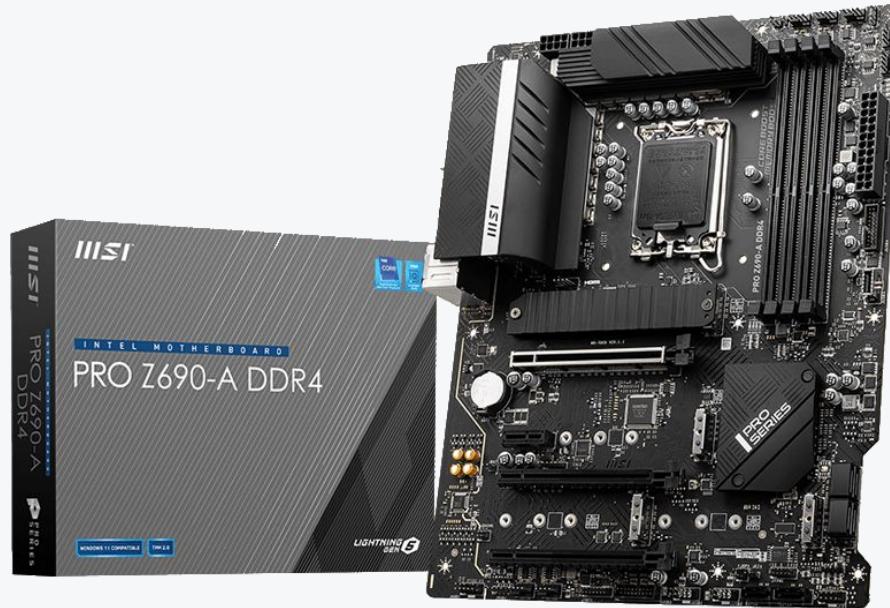
Features also planned for this release:

- Add option to skip PS/2 keyboard detection to make all pS/2 keyboard work hopefully (legacy stuff always problematic)
- Runtime options for: PL1/PL2, VR loadline, memory XMP profile selection



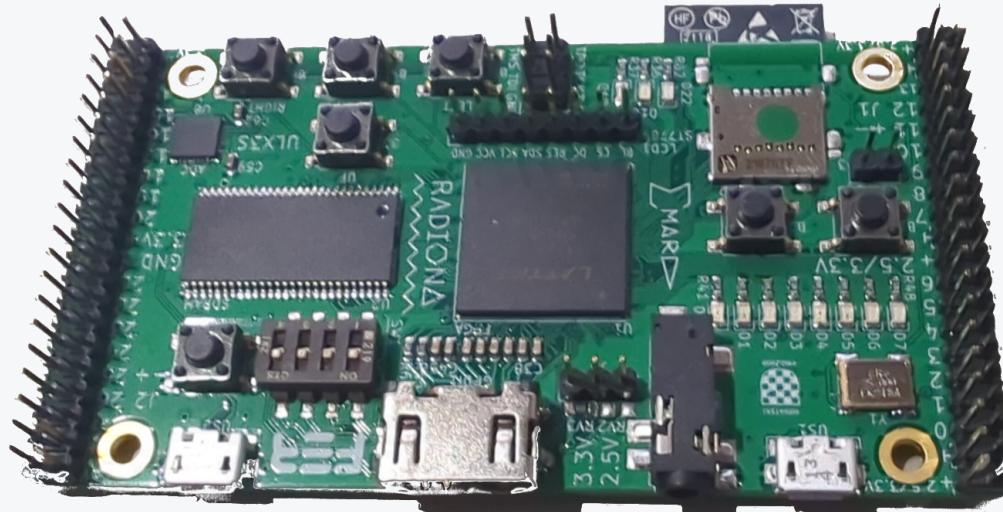
v1.2.0 - Community Release

- All features from v1.1.2 for everyone
- What else? We will see





- Decided to go with SpiSpy
- Inspired by the famous open-source activist, programmer , photographer and frequent hacker: Trammel Hudson
- <https://trmm.net/Spispy/>





- There is one interesting feature in SpiSpy - TOCTOU mode!
- It can hijack SPI cycles from the chipset and respond with data present on the SpiSpy SDRAM (programmed with our custom firmware binary)
- Nobody said it will not hijack SPI cycles coming from 3rdparty chip responsible for FlashBIOS functionality!
- Plan: gather a trace of the FlashBIOS recovery process and determine vendor firmware structures responsible for binary validation
- Goal: Make FlashBIOS feature work with Dasharo builds (v1.1.2 or v1.2.0?)



v1.0.0 - Community Release

Current status: Discovery (Waiting for funds to start Evaluation)

- Around 23'Q4 or 24'Q1!? I know.. I know... So frickin' late...
- The more supporters we have the quicker we may satisfy the community needs!



- Is MSI EZ LED debug support of any importance?
- What options do you see as most important to be implemented in near future?

Q&A

Thank you