presented by

UEFI topics for the manufacturing efficiency

Spring 2019 UEFI Plugfest

April 8-12, 2019

Presented by Rafael R. Machado (Flex Inst. of Technology)

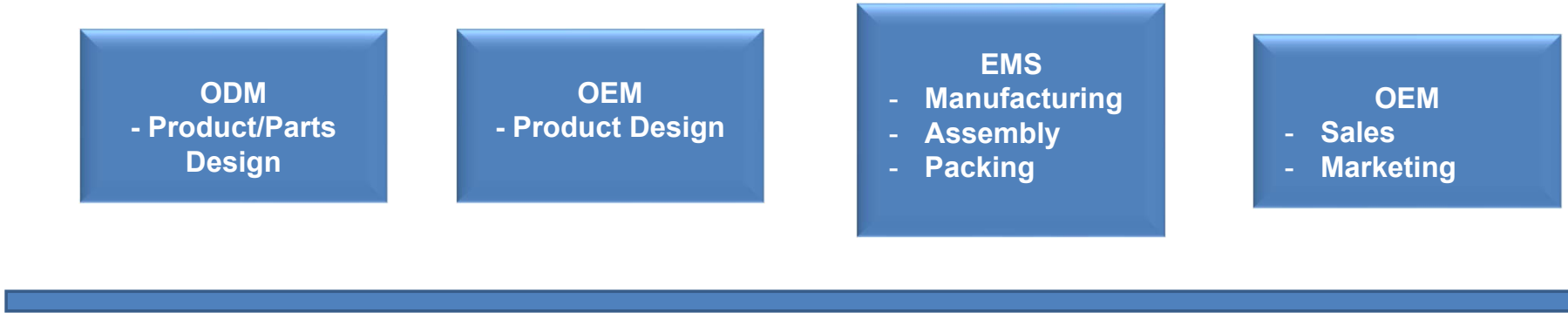
Agenda

- Introduction
- Manufacturing Process 101
- Hardware Diagnostics
- HW vs. FW Issues
- Manufacturing Needs
- Questions

Who am I ? Where I come from?

- Rafael R. Machado
- Computer Engineer
- MSc Computer Science
- Researcher at FIT
  - FIT is part of Flex (Flextronics) ecosystem
- Professor at FACENS

Manufacturing Process 101



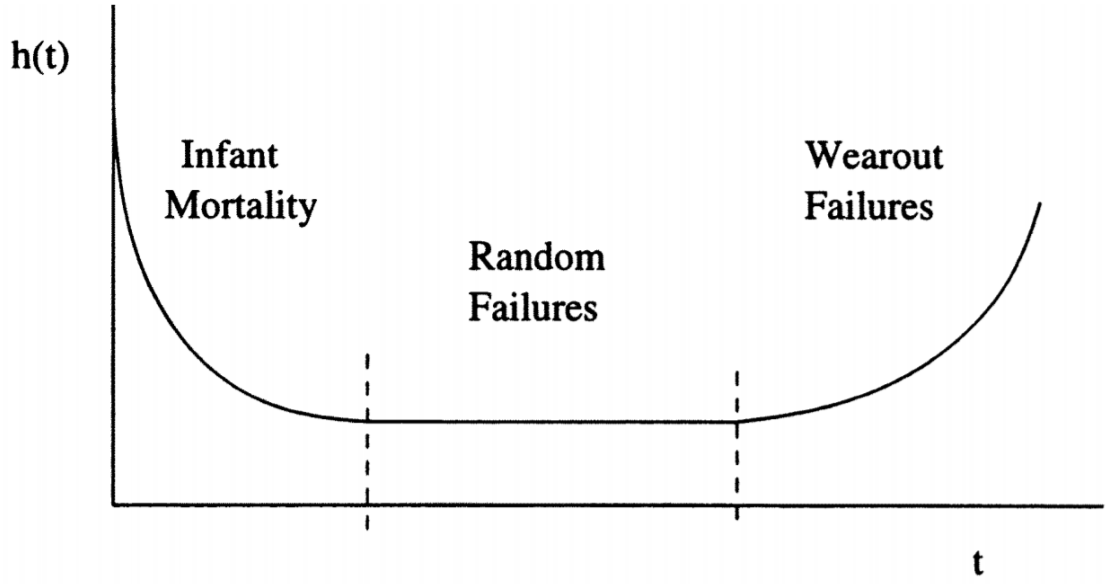
The Manufacturing Challenges

- Assemble a large number of devices
  - Make it fast
  - Make it with high quality
  - Make it with low cost
  - Zero Waste

Reliability Engineering

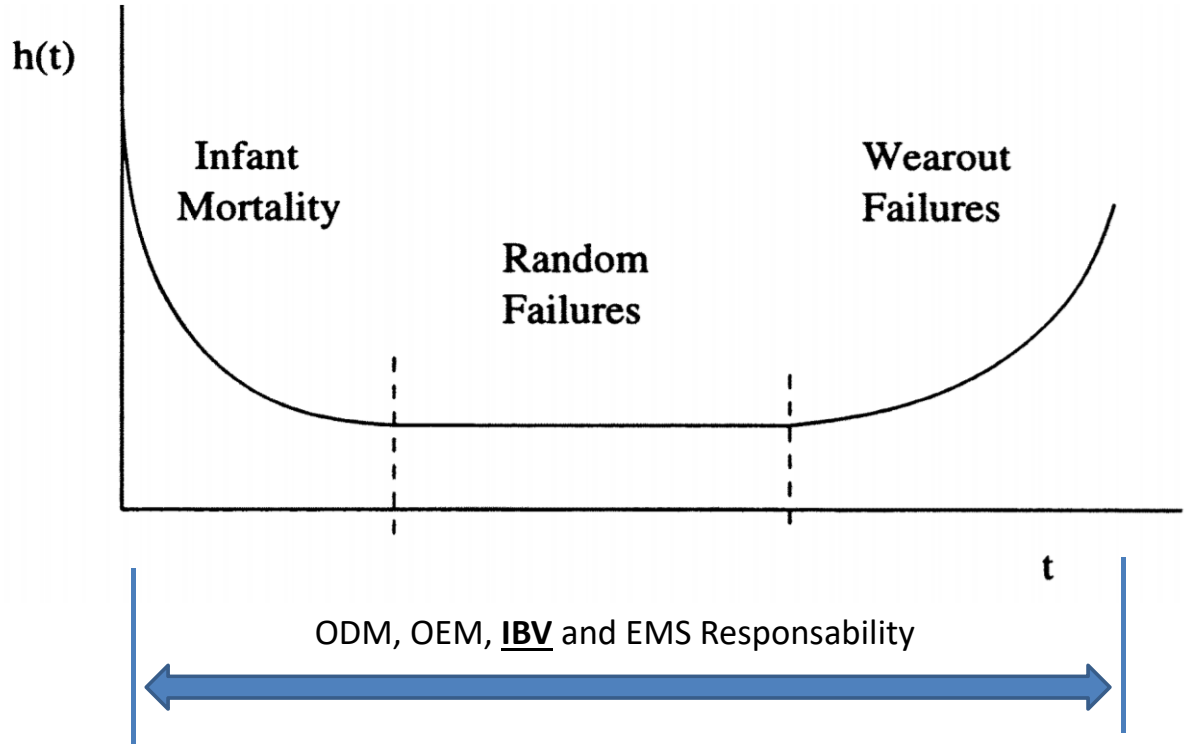
- **Infant Mortality**
  - **ICs problems**
  - **Failure by defects**
- **Random Failures**
  - **Stress exceeding strength**
  - **User fault**
- **Wearout**
  - **Common degradation due time usage**
  - **Corrosion / Oxidation**

Bathtub Curve [1][3]



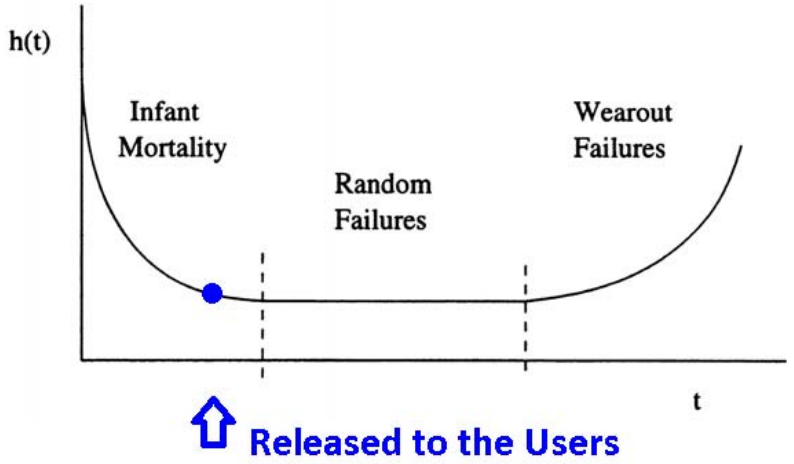
Reliability Engineering

Bathtub Curve

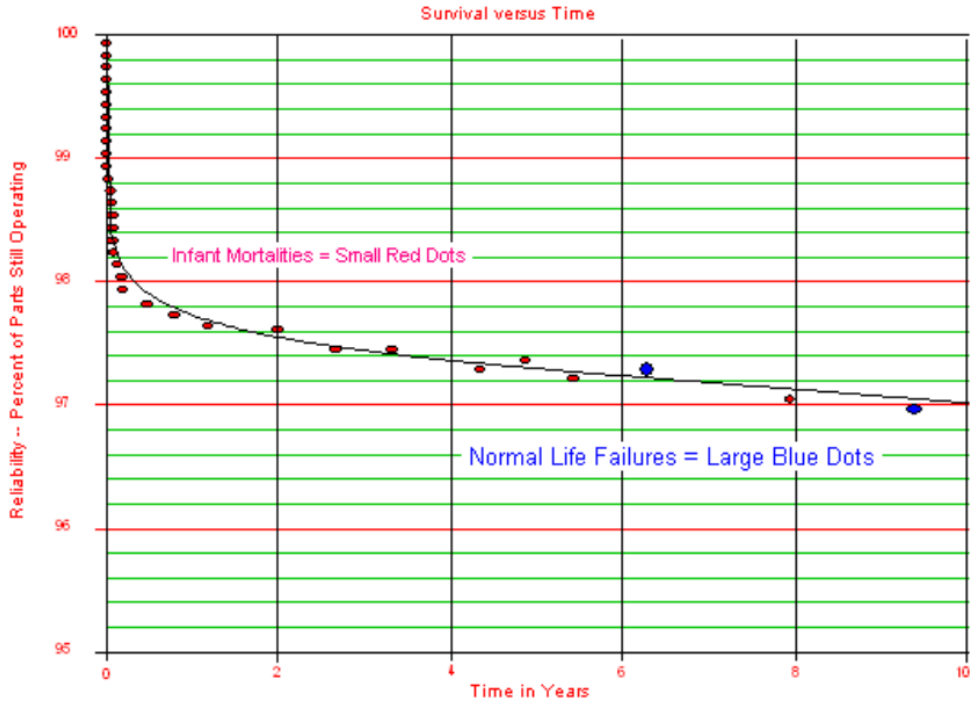


Stressing the Product

- **Design**
  - **Accelerated Life Testing (ALT)**
  - **Highly Accelerated Life Test (HALT)**
  - **Highly Accelerated Stress Test (HAST)**
  - **Highly Accelerated Stress Screen (HASS)**
- **Manufacturing**
  - **Highly Accelerated Stress Audit (HASA)**
  - **Burn-in**



Stressing the Product – Why?

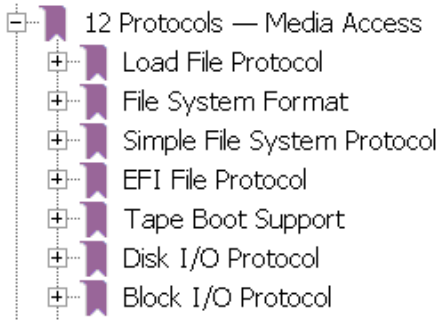


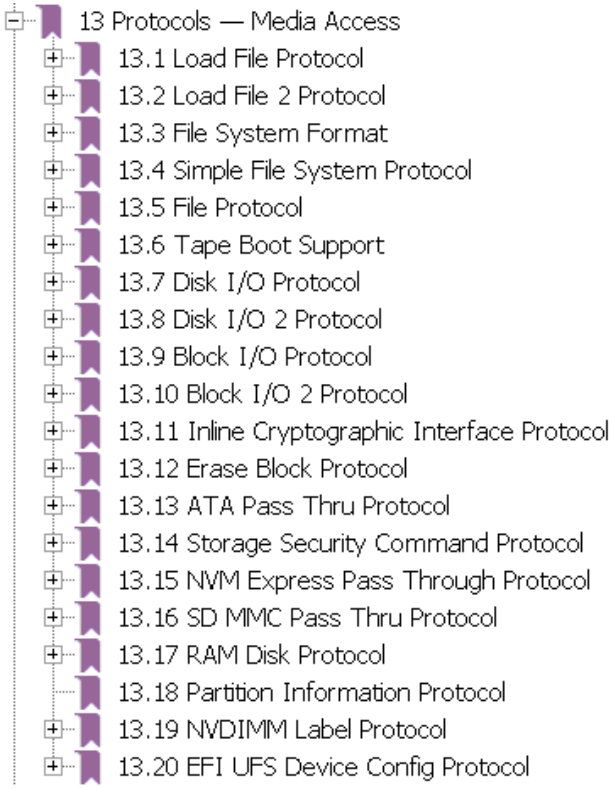
Most failures happen during the first year of usage [2]
(H)Accelerated Life Testing tries to find these devices

UEFI Tools and the Manufacturing

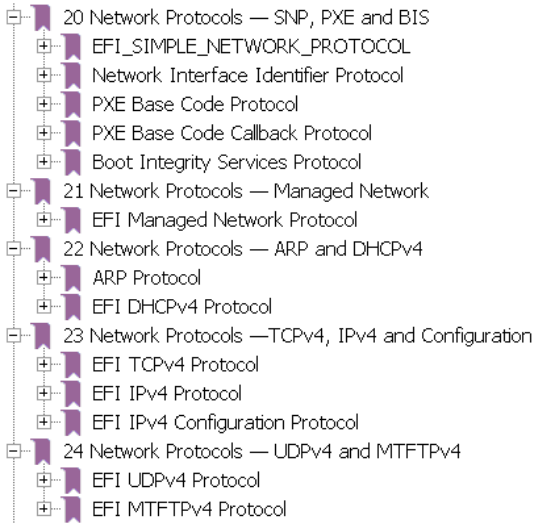
- More control of the hardware (User Space vs. Kernel Space)
- No OS overhead
- Cheaper (No OS license required)
- Faster to BOOT (as for today)

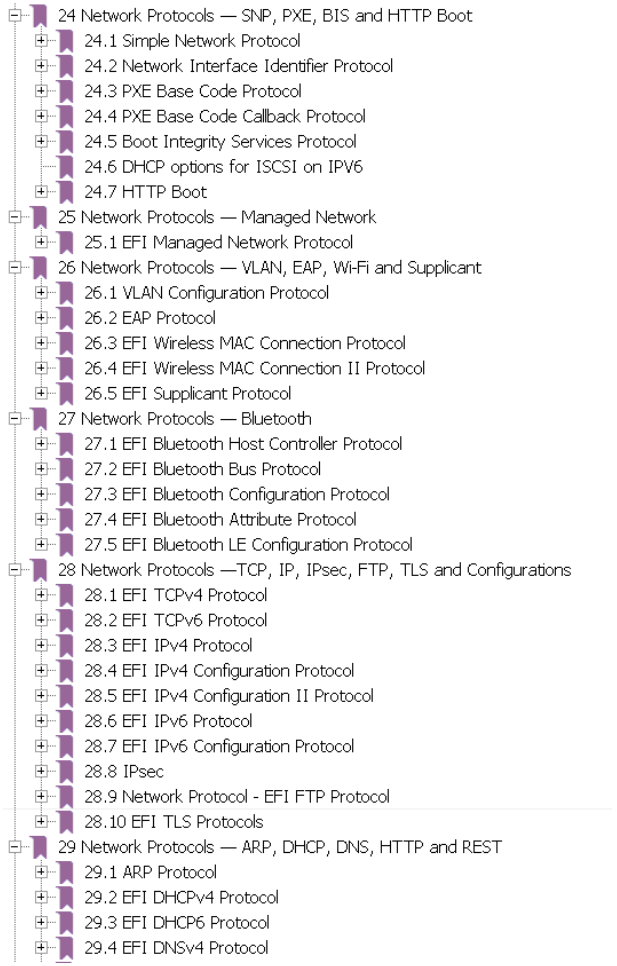
UEFI Spec Evolution for MFG – Media (2.0 vs 2.7)





UEFI Spec Evolution for MFG – Network (2.0 vs 2.7)

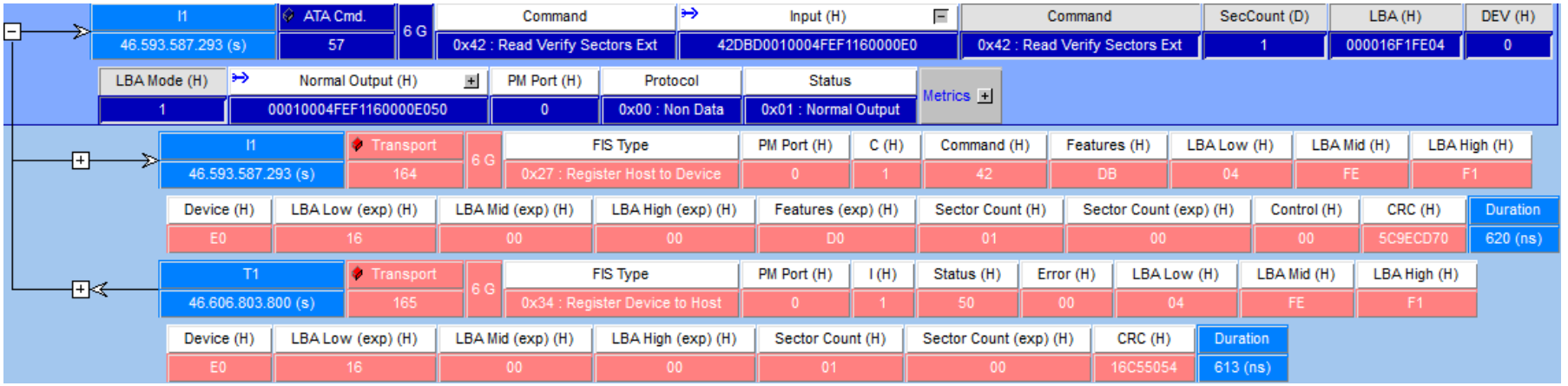




Is it a HW or FW issue?

- Manufacturing Nightmare
- FW issues can stop an entire manufacturing line
  - Normally happens with BIOS updates
- FW issues can brick a system (like a HW issue does)

FW x HW Issue – LBA Mode



I1	ATA Cmd.	6 G	Command	Input (H)	Command	SecCount (D)	LBA (H)	DEV (H)
46.593.587.293 (s)	57		0x42 : Read Verify Sectors Ext	42DBD0010004FEF1160000E0	0x42 : Read Verify Sectors Ext	1	000016F1FE04	0

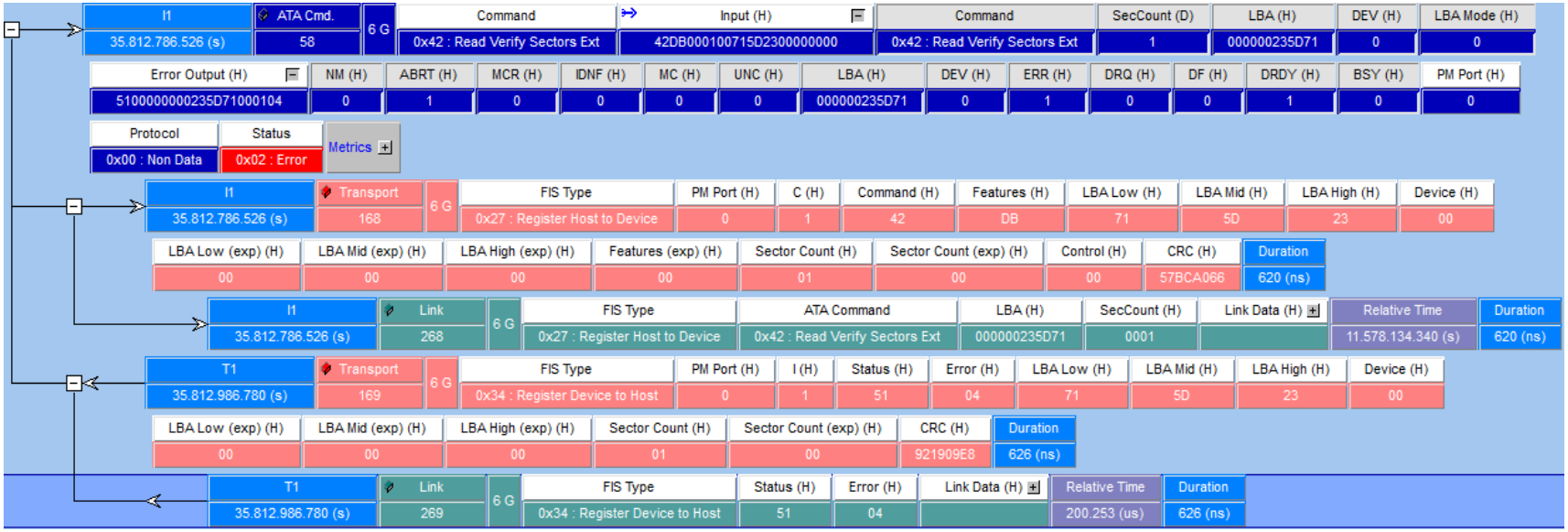
LBA Mode (H)	Normal Output (H)	PM Port (H)	Protocol	Status	Metrics
1	00010004FEF1160000E050	0	0x00 : Non Data	0x01 : Normal Output	

I1	Transport	6 G	FIS Type	PM Port (H)	C (H)	Command (H)	Features (H)	LBA Low (H)	LBA Mid (H)	LBA High (H)
46.593.587.293 (s)	164		0x27 : Register Host to Device	0	1	42	DB	04	FE	F1

Device (H)	LBA Low (exp) (H)	LBA Mid (exp) (H)	LBA High (exp) (H)	Features (exp) (H)	Sector Count (H)	Sector Count (exp) (H)	Control (H)	CRC (H)	Duration
E0	16	00	00	D0	01	00	00	5C9ECD70	620 (ns)

T1	Transport	6 G	FIS Type	PM Port (H)	I (H)	Status (H)	Error (H)	LBA Low (H)	LBA Mid (H)	LBA High (H)
46.606.803.800 (s)	165		0x34 : Register Device to Host	0	1	50	00	04	FE	F1

Device (H)	LBA Low (exp) (H)	LBA Mid (exp) (H)	LBA High (exp) (H)	Sector Count (H)	Sector Count (exp) (H)	CRC (H)	Duration
E0	16	00	00	01	00	16C55054	613 (ns)



I1	ATA Cmd.	6 G	Command	Input (H)	Command	SecCount (D)	LBA (H)	DEV (H)	LBA Mode (H)
35.812.786.526 (s)	58		0x42 : Read Verify Sectors Ext	42DB000100715D2300000000	0x42 : Read Verify Sectors Ext	1	000000235D71	0	0

Error Output (H)	NM (H)	ABRT (H)	MCR (H)	IDNF (H)	MC (H)	UNC (H)	LBA (H)	DEV (H)	ERR (H)	DRQ (H)	DF (H)	DRDY (H)	BSY (H)	PM Port (H)
5100000000235D71000104	0	1	0	0	0	0	000000235D71	0	1	0	0	1	0	0

Protocol	Status	Metrics
0x00 : Non Data	0x02 : Error	

I1	Transport	6 G	FIS Type	PM Port (H)	C (H)	Command (H)	Features (H)	LBA Low (H)	LBA Mid (H)	LBA High (H)	Device (H)
35.812.786.526 (s)	168		0x27 : Register Host to Device	0	1	42	DB	71	5D	23	00

LBA Low (exp) (H)	LBA Mid (exp) (H)	LBA High (exp) (H)	Features (exp) (H)	Sector Count (H)	Sector Count (exp) (H)	Control (H)	CRC (H)	Duration
00	00	00	00	01	00	00	57BCA066	620 (ns)

I1	Link	6 G	FIS Type	ATA Command	LBA (H)	SecCount (H)	Link Data (H)	Relative Time	Duration
35.812.786.526 (s)	268		0x27 : Register Host to Device	0x42 : Read Verify Sectors Ext	000000235D71	0001		11.578.134.340 (s)	620 (ns)

T1	Transport	6 G	FIS Type	PM Port (H)	I (H)	Status (H)	Error (H)	LBA Low (H)	LBA Mid (H)	LBA High (H)	Device (H)
35.812.986.780 (s)	169		0x34 : Register Device to Host	0	1	51	04	71	5D	23	00

LBA Low (exp) (H)	LBA Mid (exp) (H)	LBA High (exp) (H)	Sector Count (H)	Sector Count (exp) (H)	CRC (H)	Duration
00	00	00	01	00	921909E8	626 (ns)

T1	Link	6 G	FIS Type	Status (H)	Error (H)	Link Data (H)	Relative Time	Duration
35.812.986.780 (s)	269		0x34 : Register Device to Host	51	04		200.253 (us)	626 (ns)

FW vs HW Issue – LBA Mode

- Results
  - 32K HDD devices failing
  - Manufacturing delay
  - 32K possible calls to the support team

FW vs HW Issue – Touch Support

This is a desktop connected to a simple LCD monitor

```
Press ESC in 1 seconds to skip startup.nsh or any other key to continue.
Shell> dh -p absolutepointer
159: UnknownDevice AbsolutePointer SimplePointer UnknownDevice SimpleTextInEx SimpleTextIn Unknown
vice SimpleTextOut UnknownDevice
3AD: AbsolutePointer UnknownDevice DevicePath(x0)/Pci(0x14,0x0)/USB(0x6,0x1))
 USBIO
```

- No touch hardware is present
- User may think touch hardware is failing

FW vs HW Issue – Touch Support

- Results
  - User believes the hardware is not working
  - Additional checks needed at application level
  - New Product Introduction (NPI) delay due to BIOS update required

Other Problems

- Handles that point to nowhere
- Unnecessary Drivers at the BIOS
  - Consuming space that could be used by other tools like Diagnostic tools
  - It's also a problem related to manufacturing attacks
- Network Stack with problems
  - Specially PXE

Check-list for Efficient Manufacturing

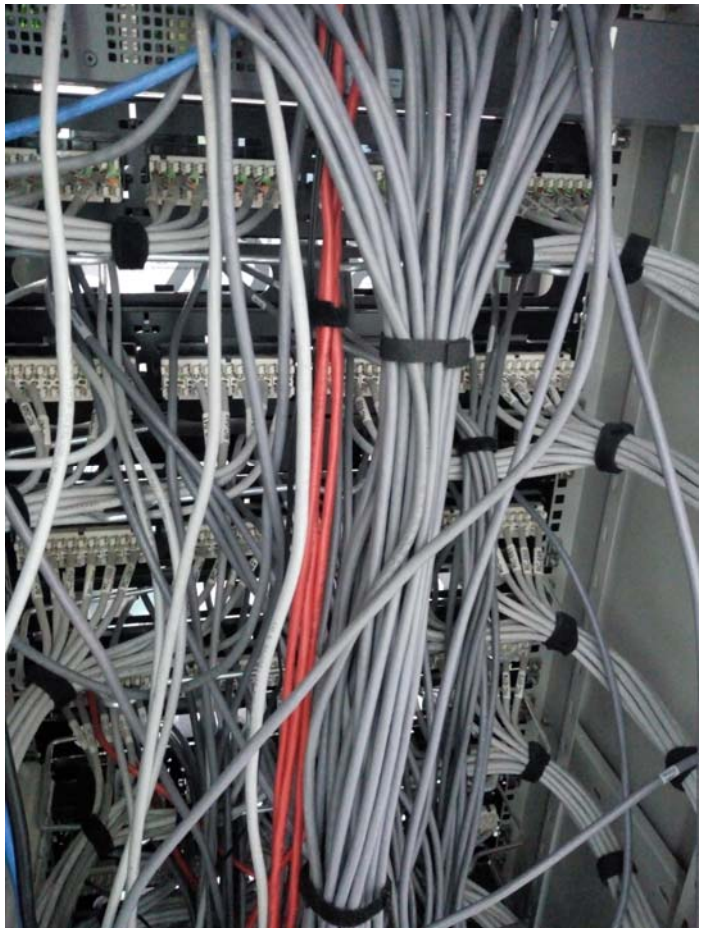
- Follow existing Specs (USB, PCIe, UEFI, ACPI, ...)
  - MFG and Diagnostic tools rely on the Specs
- Remove unnecessary binaries from BIOS image
  - Boot faster
  - BIOS update faster (download during MFG time)
- Network + UEFI is crucial for MFG!

What does MFG need at the UEFI Spec?

- GPU Protocol
- Battery Protocol
- Multi-touch Protocol
- Audio Protocol
  - https://github.com/RafaelRMachado/Msc_UefiHda_PreOs_Accessibility
- Fan Protocol

What is the MFG dream?

- Pxe/HTTP Boot over WiFi
  - Faster to create new manufacturing lines
  - Cheaper to create infrastructure



Questions ?

Thanks!

Rafael Machado (FIT - Flex Inst. of Technology)
rafaelr.machado@fit-tecnologia.org.br
https://linkedin.com/in/rafael-rodrigues-machado-br/

References

[1] Klutke, Georgia-Ann, Peter C. Kiessler, and Martin A. Wortman. "A critical look at the bathtub curve." IEEE Transactions on reliability 52.1 (2003): 125-129.

[2] https://www.weibull.com/hotwire/issue21/hottopics21.htm

[3] R. E. Barlow and F. Proschan, Statistical Theory of Reliability and Life Testing: Probability Models, 1975, p. 55.

[4] Halley, Edmond. "VI. An estimate of the degrees of the mortality of mankind; drawn from curious tables of the births and funerals at the city of Breslaw; with an attempt to ascertain the price of annuities upon lives." Philosophical transactions of the Royal Society of London 17.196 (1693): 596-610.

Thanks for attending the 2019 Spring UEFI Plugfest

For more information on UEFI Forum and UEFI Specifications, visit http://www.uefi.org

presented by

http://fit-tecnologia.org.br/en