



# UEFI topics for the manufacturing efficiency

Spring 2019 UEFI Plugfest

April 8-12, 2019

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

[www.uefi.org](http://www.uefi.org)

# 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



[www.uefi.org](http://www.uefi.org)

# Manufacturing Process 101



**ODM**  
- Product/Parts  
Design

**OEM**  
- Product Design

**EMS**  
- Manufacturing  
- Assembly  
- Packing

**OEM**  
- Sales  
- Marketing



# The Manufacturing Challenges

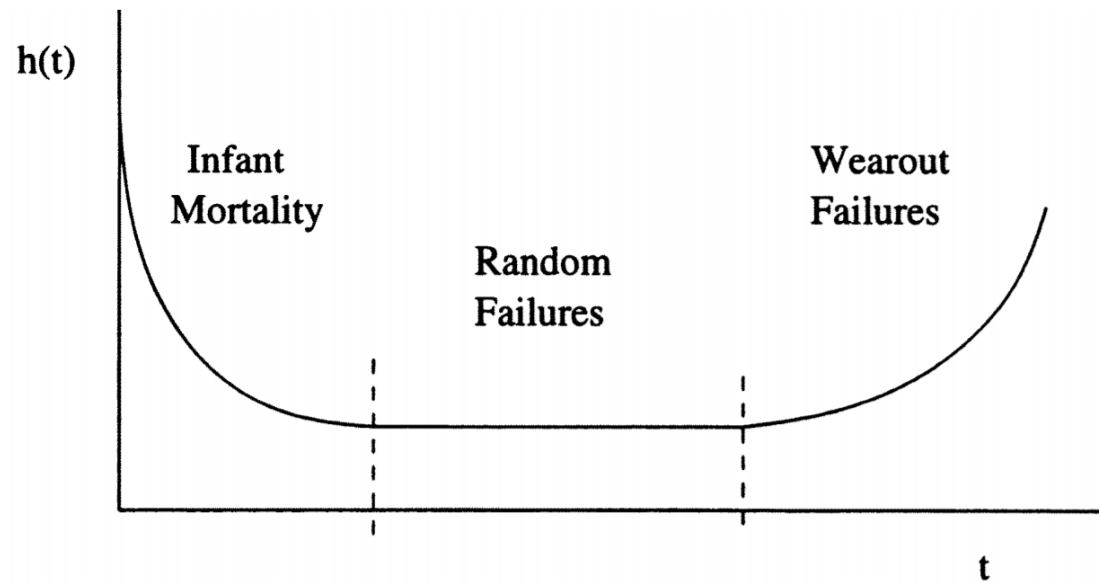
- Assemble a large number of devices
  - Make it fast
  - Make it with high quality
  - Make it with low cost
  - Zero Waste



# Reliability Engineering



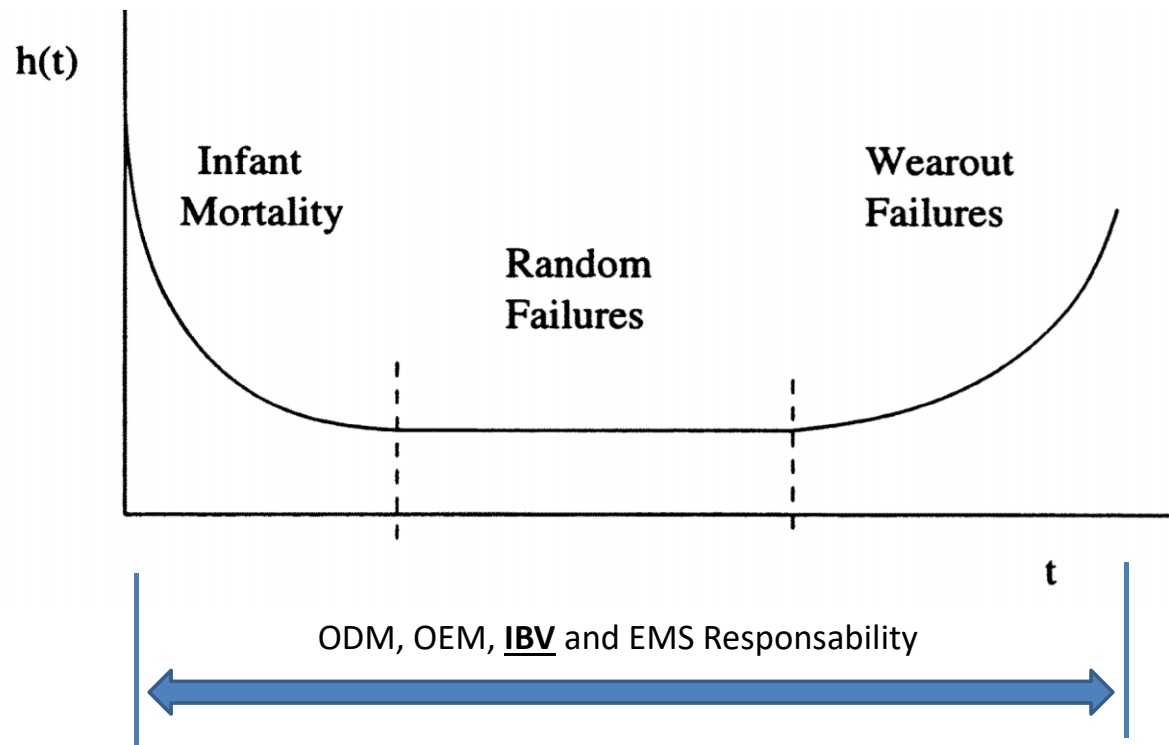
Bathtub Curve [1][3]



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

# Reliability Engineering

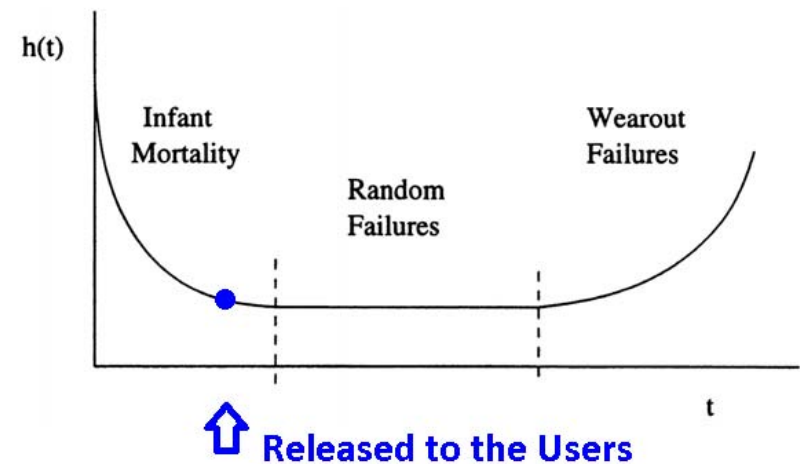
## Bathtub Curve



# Stressing the Product

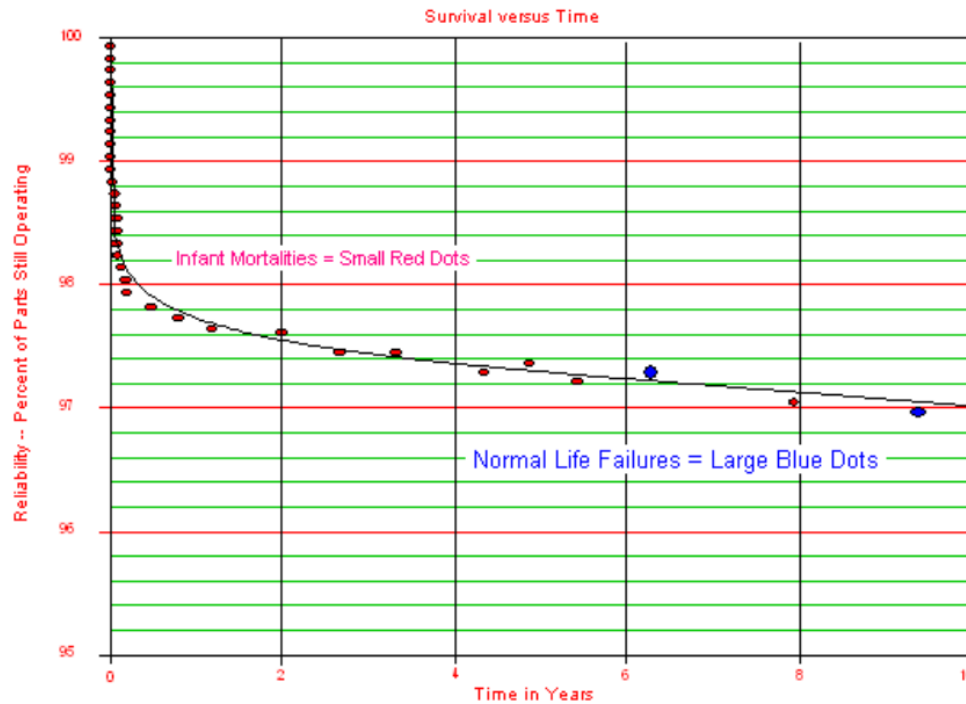


- **Design**
  - Accelerated Life Testing (ALT)
  - Highly Accelerated Life Test (HALT)
  - Highly Accelerated Stress Test (HAST)
  - Highly Accelerated Stress Screen (HASS)
- **Manufacturing**
  - Highly Accelerated Stress Audit (HASA)
  - Burn-in





# 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)

- 12 Protocols — Media Access
  - Load File Protocol
  - File System Format
  - Simple File System Protocol
  - EFI File Protocol
  - Tape Boot Support
  - Disk I/O Protocol
  - Block I/O Protocol

- 13 Protocols — Media Access
  - 13.1 Load File Protocol
  - 13.2 Load File 2 Protocol
  - 13.3 File System Format
  - 13.4 Simple File System Protocol
  - 13.5 File Protocol
  - 13.6 Tape Boot Support
  - 13.7 Disk I/O Protocol
  - 13.8 Disk I/O 2 Protocol
  - 13.9 Block I/O Protocol
  - 13.10 Block I/O 2 Protocol
  - 13.11 Inline Cryptographic Interface Protocol
  - 13.12 Erase Block Protocol
  - 13.13 ATA Pass Thru Protocol
  - 13.14 Storage Security Command Protocol
  - 13.15 NVM Express Pass Through Protocol
  - 13.16 SD MMC Pass Thru Protocol
  - 13.17 RAM Disk Protocol
  - 13.18 Partition Information Protocol
  - 13.19 NVDIMM Label Protocol
  - 13.20 EFI UFS Device Config Protocol

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



- [-] 20 Network Protocols — SNP, PXE and BIS
  - [+] EFI\_SIMPLE\_NETWORK\_PROTOCOL
  - [+] Network Interface Identifier Protocol
  - [+] PXE Base Code Protocol
  - [+] PXE Base Code Callback Protocol
  - [+] Boot Integrity Services Protocol
- [-] 21 Network Protocols — Managed Network
  - [+] EFI Managed Network Protocol
- [-] 22 Network Protocols — ARP and DHCPv4
  - [+] ARP Protocol
  - [+] EFI DHCPv4 Protocol
- [-] 23 Network Protocols —TCPv4, IPv4 and Configuration
  - [+] EFI TCPv4 Protocol
  - [+] EFI IPv4 Protocol
  - [+] EFI IPv4 Configuration Protocol
- [-] 24 Network Protocols — UDPv4 and MTFTPv4
  - [+] EFI UDPv4 Protocol
  - [+] EFI MTFTPv4 Protocol

- [-] 24 Network Protocols — SNP, PXE, BIS and HTTP Boot
  - [+] 24.1 Simple Network Protocol
  - [+] 24.2 Network Interface Identifier Protocol
  - [+] 24.3 PXE Base Code Protocol
  - [+] 24.4 PXE Base Code Callback Protocol
  - [+] 24.5 Boot Integrity Services Protocol
  - [+] 24.6 DHCP options for iSCSI on IPv6
  - [+] 24.7 HTTP Boot
- [-] 25 Network Protocols — Managed Network
  - [+] 25.1 EFI Managed Network Protocol
- [-] 26 Network Protocols — VLAN, EAP, Wi-Fi and Supplicant
  - [+] 26.1 VLAN Configuration Protocol
  - [+] 26.2 EAP Protocol
  - [+] 26.3 EFI Wireless MAC Connection Protocol
  - [+] 26.4 EFI Wireless MAC Connection II Protocol
  - [+] 26.5 EFI Supplicant Protocol
- [-] 27 Network Protocols — Bluetooth
  - [+] 27.1 EFI Bluetooth Host Controller Protocol
  - [+] 27.2 EFI Bluetooth Bus Protocol
  - [+] 27.3 EFI Bluetooth Configuration Protocol
  - [+] 27.4 EFI Bluetooth Attribute Protocol
  - [+] 27.5 EFI Bluetooth LE Configuration Protocol
- [-] 28 Network Protocols —TCP, IP, IPsec, FTP, TLS and Configurations
  - [+] 28.1 EFI TCPv4 Protocol
  - [+] 28.2 EFI TCPv6 Protocol
  - [+] 28.3 EFI IPv4 Protocol
  - [+] 28.4 EFI IPv4 Configuration Protocol
  - [+] 28.5 EFI IPv4 Configuration II Protocol
  - [+] 28.6 EFI IPv6 Protocol
  - [+] 28.7 EFI IPv6 Configuration Protocol
  - [+] 28.8 IPsec
  - [+] 28.9 Network Protocol - EFI FTP Protocol
  - [+] 28.10 EFI TLS Protocols
- [-] 29 Network Protocols — ARP, DHCP, DNS, HTTP and REST
  - [+] 29.1 ARP Protocol
  - [+] 29.2 EFI DHCPv4 Protocol
  - [+] 29.3 EFI DHCP6 Protocol
  - [+] 29.4 EFI DNSv4 Protocol



## 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  
Device SimpleTextOut UnknownDevice  
BAD: 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?

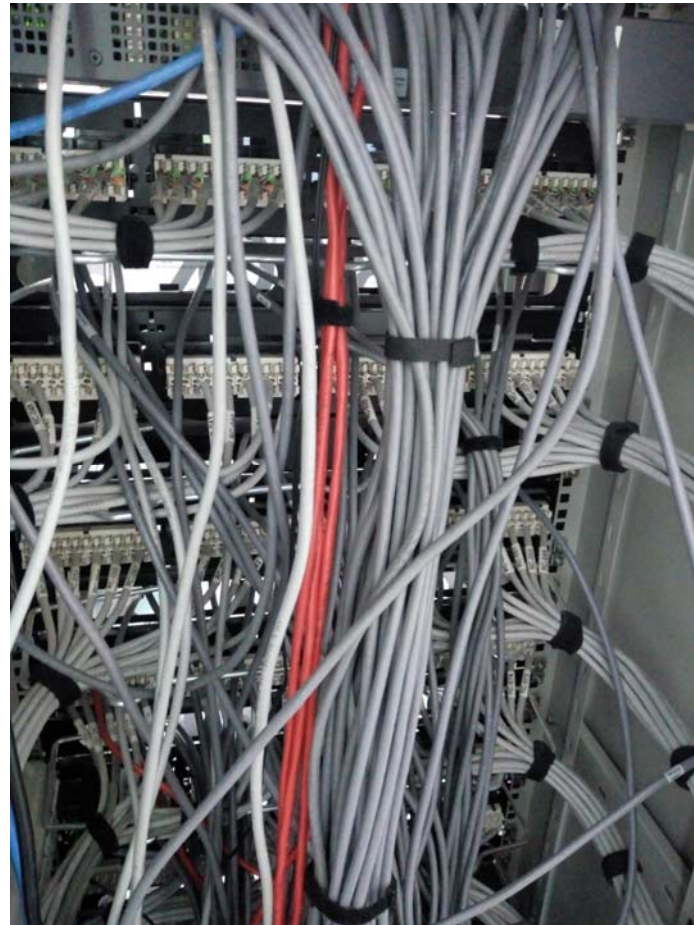


- GPU Protocol
- Battery Protocol
- Multi-touch Protocol
- Audio Protocol
  - [https://github.com/RafaelRMachado/Msc\\_UefiHda\\_PreOs\\_Accessibility](https://github.com/RafaelRMachado/Msc_UefiHda_PreOs_Accessibility)
- Fan Protocol

# What is the MFG dream?



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



[www.uefi.org](http://www.uefi.org)



# Questions ?

[www.uefi.org](http://www.uefi.org)



# Thanks!

Rafael Machado (FIT - Flex Inst. of Technology)

[rafaelr.machado@fit-tecnologia.org.br](mailto: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*



Instituto de Tecnologia

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

[www.uefi.org](http://www.uefi.org)

