

# Fly me to the moon ...

**Professor Mike Hinchey** 





Higher Education Authority An tÚdarás um Ard-Oideachas



THE IRISH SOFTWARE ENGINEERING RESEARCH CENTRE

Lero© 2010





Lero© 2010

THE IRISH SOFTWARE ENGINEERING RESEARCH CENTRE



66 Years Ago ....





- 650 instructions per second.
- 1024 17-bit words of memory in mercury ultrasonic delay lines.

**EDSAC** 

- Paper tape input and teleprinter output at 6 2/3 characters per second.
- 3000 valves, 12 kW power consumption, occupied a room 5m by 4m.
- "Operating system" occupied 31 words of read-only memory.
- Early use to solve problems in meteorology, genetics and X-ray crystallography.



#### Difference Engine





Errata, detected in Taylor's Logarithms. London: 4to, 1972 [sic]

Motivation

6 Kk Co-sine of 14.18.3 – 3398 – 3298

Nautical Almanac (1832)

In the list of ERRATA detected in Taylor's *Logarithms*, for cos. 4 18' 3" read cos. 14 18'2".

Nautical Almanac (1833)

ERRATUM of the ERRATUM of the ERRATA of TAYLOR'S *Logarithms.* For cos. 4 18'3", *read* 14 18' 3".

Nautical Almanac (1836)



#### First Programmer



Augusta Ada King, Countess of Lovelace

7



- Increases in demand for greater, more complex functionality;
- Stricter (required and desirable) constraints on performance and reaction times;
- Attempts to increase productivity and reduce costs while constantly pushing requirements to the limit;
- Requirement of regular change and evolving systems.



**Evolution** 

Any intelligent fool can make things bigger and more complex ...

It takes a touch of genius and a lot of courage to move in the opposite direction.

Albert Einstein

9



**Evolving Critical Systems** 

**Evolving** systems are software systems which exhibit change over time.

Software is supposed to change... otherwise it would be in the hardware!



- have evolved from legacy code and legacy systems, or
- result from a combination of existing component-based systems, possibly over significant periods of time, or
- evolve as a result of a focused and intentional change in organization and architecture to exploit newer techniques believed to be beneficial;
- they require that the system adapt and evolve at run-time in order to react to changes in the environment or to meet necessary constraints on the system that were not previously satisfied and possibly not previously known.



Critical systems are systems where

- failure or malfunction will lead to significant negative consequences;
- these systems may have strict requirements for security and safety, to protect the user or others;
- alternatively, these systems may be critical to the organization's mission, product base, profitability or competitive advantage.



An ECS Research Agenda addresses several core research topics in the evolving critical systems field.

The central research topic is building software that
(a) is highly reliable, and
(b) retains this reliability as it evolves, without incurring prohibitive costs.



#### **Evolving Critical Systems**

PEA+T







Peat





#### **Evolving Critical Systems**

PEA+T







Source: IBM, AC Blueprint 2003

the IRISH SOFTWARE ENGINEERING RESEARCH CENTRE



### Evolving

- Software is meant to change, both at design/revision time and at run-time
- Lero's research focuses on methods and tools for designing software that can be changed or that can change itself without degradation

Critical

- Much of today's software is mission-, safety- or business-critical
- Lero is researching methods and tools to improve the integrity of and confidence levels in critical software

Systems

- Expertise in software engineering needs to be coupled with domain knowledge
- Lero has existing partnerships & expertise in medical devices, space, future cities and financial services
- We will continue to seek domain-related partners for collaborative.



- A: Methods & Standards for High Integrity Systems
  - Lean, Agile & Global methods
  - Open Sourcing & Innovation
  - Standardised SW Development processes
  - Model-based approaches
  - Formal methods & safety use cases
  - B: Adaptive & Autonomous Systems
    - Systems that learn & respond to their environments
  - C: Software Performance
    - Large complex systems
    - Multicore embedded & massively parallel systems
  - D: Security & Privacy
    - New approaches to security and privacy and the trade-offs between them
    - Digital forensics



## Hub and Spoke Model



Lero© 2010

THE IRISH SOFTWARE ENGINEERING RESEARCH CENTRE 20



An ECS Scenario

- Space Exploration
  - Some of the most complex and expensive software applications to date.
  - High Levels of Autonomy.
  - Significant consequences for failure.

#### Requirements Effort vs. Cost Overrun



the IRISH SOFTWARE ENGINEERING RESEARCH CENTRE



- Inspired by swarms of bees and flocks of birds in nature;
- Many application areas:
  - drug discovery;
  - communication systems;
  - environmental monitoring;
  - exploration.



Coordinated swarms of smaller spacecraft will offer:

- More effective use of solar power;
- Access to areas where large craft could not go;
- Ability to perform more complex tasks;
- Greater accuracy and flexibility.



Autonomous NanoTechnology Swarm

Three concept sub-missions:

- 1. Lander Amorphous Rover Antenna (LARA)
- 2. Saturn Autonomous Ring Array (SARA)
- 3. Prospecting Asteroid Mission (PAM)





#### Tet Walkers





LARA Walkers





ANTS Concept Mission - PAM





**PAM** : the Movie





**ECS Contributions** 

- 1. Formal Methods
- 2. Autonomic Computing
- 3. Software Product Lines
- 4. Automatic Code Generation





the IRISH SOFTWARE ENGINEERING RESEARCH CENTRE

#### **ASSL Specification**

```
AEIP {
  MESSAGES { ... }
  CHANNELS { ... }
  FUNCTIONS { ... }
  MANAGED ELEMENTS {
    MANAGED ELEMENT worker {
       INTERFACE FUNCTION getDistanceToNearestObject { RETURNS { DECIMAL } }
} // AEIP
METRICS {
  METRIC distanceToNearestObject {
     METRIC TYPE { RESOURCE }
     METRIC SOURCE { AEIP.MANAGED ELEMENTS.worker.getDistanceToNearestObject }
     DESCRIPTION { "measures the distance to the nearest space object" }
    MEASURE UNIT { "KM" }
     VALUE { 100 }
     THRESHOLD CLASS { DECIMAL [0.001 ~ ) }
```

the IRISH SOFTWARE ENGINEERING RESEARCH CENTRE



**ECS Contributions** 

- 1. Formal Methods
- 2. Autonomic Computing
- 3. Software Product Lines
- 4. Automatic Code Generation



**Autonomic Computing** 

Inspiration from the human/mammalian autonomic nervous system.

Fight or Flight

**Rest and Digest** 



sympathetic (SyNS)



parasympathetic (PaNS)

#### The Autonomic Environment



THE IRISH SOFTWARE ENGINEERING RESEARCH CENTRE



**ECS Contributions** 

- 1. Formal Methods
- 2. Autonomic Computing
- 3. Software Product Lines
- 4. Automatic Code Generation

#### Feature Model



the IRISH SOFTWARE ENGINEERING RESEARCH CENTRE



**ECS Contributions** 

- 1. Formal Methods
- 2. Autonomic Computing
- 3. Software Product Lines
- 4. Automatic Code Generation



**Requirements to Design to Code (R2D2C)** 









- Automation of entire development process;
- Significant increase in quality;
- Ability to do formal proof on properties of implementations;
- Ability to do formal proof of correctness;
- Automated means for requirements analysis;
- Guaranteed correspondence between requirements and their implementation as code.



- End-to-end automatic code generation of provably correct systems;
- Automatic reimplementation after any requirements change;
- Exploiting re-use across platforms;
- Reverse engineering legacy systems to a mathematically sound model;
- Analysis and documentation of existing systems (e.g., expert systems);
- Re-engineering of legacy systems to a provably correct new implementation.



Domains (to date)

- Agent Based Systems;
- Wireless Sensor Networks ;
- ANTS;
- Verification of Robotic Procedures (cf. Hubble Space Telescope Robotic Servicing Mission).





## HRSM Procedures

WFC3_mod_01	21.doc - Microsoft Word		
jie <u>E</u> dit <u>V</u> iew	Insert Format Tools Table Window Help Add	be PDF Acrobat Comments	Type a question for help
	3. TA 149 64 IV. TA (A) - (A) - (A) - (A)	💶 100% 🕞 💿 📄 Read 🔤 💾 Normal + He	we - 8 - 1 = = = 1 =
	∃ R*I ∧ #*I № == #₹ ∧   → - 129 ⊞ [		
ù 📆 🖏 📘			
🕽 SnagIt [💇   Wir	dow 🗾 🚽		
<b>.</b>			7
	1		, , , , , , , , , , , , , , , , , , , ,
0	¤	¤	¤
1	<b>u</b>	WEC3-Installation#	п
TASK-*			-
DV/>HR>MIN*	GA¤	DR-2ª	DR-
	ECU-harness-connection-needs-to-be-     1-tool-caddy-[[     WFC3-Tool-Caddy-(Ground     WFC2-     WFC2-Interface-Platef[     WFPC2-     1-WFPC2-Interface-Platef[	nade after WFC3 installation (for thermal-protection)¶ ·Strap Tool, Connector Tool, Stabilization Tool (remains-in Interface Plate), Harness Tool (remains-on-ECU-harness	h HST FR27), Socket Extension Tool-I )))¶
	CUbarress connection needs to be 1     Or caddy: []     WFC3 Tool Caddy: []     WFC3 Tool Caddy: []     WFC3     WFC3     Tool Caddy: []     WFC3	nade after WFC3-installation-(for thermal-protection)¶ -Shap-Tool,-Connector-Tool, Stabilization-Tool (remains in Interface-Plate), Harness Tool (remains on ECU-harness avity, WFPC2, WFC3, and any-EM-open-bays¶ op=V1-avis¤	h HST-FR27), Socket-Extension-Tool ( 3))¶
×		nade after WFC3-installation-(for-thermal-protection)¶ Strap-Tool, Connector-Tool, Stabilization-Tool (remains-in Interface-Plate), Harness-Tool (remains-on-ECU-harness avity, WFPC2, WFC3, and any-EM-open-bays¶ ig—V1-axis¤   ≖	n HST-FR27), Socket Extension Tool ( ))¶ 
X	→ ECU harness connection needs to be r     1-tool caddy: ¶     → 1-tool caddy: ¶     → WFC3 Tool Caddy: (Ground     → → → WFC2     → 1-WFPC2-Interface Plate¶     → Sun-Protection-required for HST-WF-cc     → HST-\$A\$ positioned at 0° and sun-alor     ¤     ×	nade after WFC3-installation-(for-thermal-protection)¶ Strap Tool, Connector Tool, Stabilization-Tool (remains in Interface Plate), Harness-Tool (remains on ECU-harness avity, WFPC2, WFC3, and any-EM open bays¶ g=\/1 avis¤ ¤	h HST-FR27), Socket Extension Tool- ))¶ x x
n N N	→ ECU harness connection needs to be r     → 1 tool caddy. []     → ↓ VFC3 Tool Caddy. (Ground     → ↓ ↓ VFC3 Tool Caddy. (Ground     → ↓ ↓ ↓ VFC2     → ↓ VFC2 Interface Plate[]     → ↓ ↓ SUP. Protection required for HST-WF-cc     → HST-SAs positioned at 0° and sun alor     ×     ×     ×     ×     ×     ×     ×     ×     ×     ×     ×	nade after WFC3-installation (for thermal-protection)¶ Strap Tool, Connector Tool, Stabilization Tool (remains in Interface-Plate), Harness Tool (remains on ECU-harness avity, WFPC2, WFC3, and any EM-open bays¶ g=V1-axis¤ x x x x Start-of-Day-1¤	n HST-FR27), Socket Extension Tooli ))¶ 
и и и	→ ECU harress connection needs to be → 1 tool caddy: ¶     → → WFC3 Tool Caddy: @Ground     → → WFC3 Tool Caddy: @WFC2     → → ↓ WFC2	nade after WFC3-installation (for thermal-protection)¶ Strap: Tool,:Connector: Tool, Stabilization: Tool/remains in Interface Plate), Harness Tool (remains on ECU-harness avity,:WFPC2,:WFC3; and any-EM-open-bays¶ g=_V1-avis× x Start-of-Day-1¤ x	n HST-FR27), Socket Extension Tool (
ж ж и 001:00:00ж	→ ECU harress connection needs to be r     → 1 tool caddy: {         1 → ↓ WFC3 Tool Caddy: (Ground         → ↓ WFC3 Tool Caddy: (Ground         → ↓ ↓ WFC2         1 WFC2 hierface Plate[         → ↓ WFC2         1 WFC2         + ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓	nade after WFC3 installation (for thermal-protection)¶ Strap Tool, Connector Tool, Stabilization Tool (remains in Interface Plate), Harness Tool (remains on ECU harness avity, WFPC2, WFC3, and any EM open bays¶ ig_V1 avits¤ x x Start-of-Day-1¤ x Daily GAJDE Power Up and Checkout - (00.15)¤	HST-FR27), Socket Extension Tool ( )))1  X X X X X X X X X X X X X X X X X
н н х 001:00:00म н	→ ECU harness connection needs to be r     → 1 tool caddy. []     → → VFC3 Tool Caddy. (Ground     → → → VFC3 Tool Caddy. (Ground     → → → → VFC2     → 1 VVFPC2-Interface Hate[]     → Sun-Protection required for HST-VF-cc     → HST-SAs positioned at 0° and sun alor     ×	nade after WFC3-installation-(for-thermal-protection)¶ Strap Tool, Connector-Tool, Stabilization-Tool (remains in Interface Plate), Harness Tool (remains on ECU-harness avity, WFPC2, WFC3, and any EM open bays¶ gV1 avis¤ x Start-of-Day-1¤ x Daily-GA/DR-Power-Up-and-Checkout~(00:15)¤ • → TBD tasks¤	n HST-FR27), Socket Extension Tool ( ))  X X X X X Daily-GA/DR Power Up- and Ch O → TBD-tasks×
ж ж и 001:00:00 ж и 00:00:15ж	→ ECU harress connection needs to be → 1 tool caddy: [1     → → WFC3 Tool Caddy. (Ground     → → WFC3 Tool Caddy. (Ground     → → → → → WFC3 Tool Caddy. (Ground     → → → → → → → → → → → → → → → → →	nade after WFC3 installation (for thermal-protection)¶ Strap: Tool, Connector: Tool, Stabilization: Tool (remains in Interface Plate), Harness: Tool (remains on ECU harness avity, WFPC2, WFC3; and any EM open-bays¶ ggV1-axisx           x           x           x           x           x           x           x           x           x           x           x           x           x           bally GADR: Power-Up and Checkout- (00:15)×           • TBD tasks×	n HST-FR27), Socket Extension Tool ( )))¶ x x x x x x x x x x x x x
х х х 001:00:00 х 001:00:15 х 001:00:15	→ ECU harress connection needs to be → 1 tool caddy: [1     → → WFC3 Tool Caddy: (Ground → → → WFC3 Tool Caddy: (Ground → → → WFC3 therface Hate] → → Sun-Protection required for HST WF cc → → Sun-Protection required for HST WF cc → → HST SAs positioned at 0° and sun alor × × × × × × Daily GADR: Power: Up and Checkout- (00:15) × → TBD tasks× × Refrieve WFC3 Tool Caddy: (01:33) × Command Ethool stowage door open×	nade after WFC3 installation (for thermal-protection)¶ Strap Tool, Connector Tool, Stabilization Tool (remains in Interface Plate), Harness Tool (remains on ECU harness avity, WFPC2, WFC3, and any-EM open bays¶ gV1-avits¤ x x Start-of-Day-1¤ x Daily GA/DR: Power Up and Checkout (00:15)¤ • → TBD tasks¤ x Refrice WFC3 Tool-Caddy (01:33)¤ x x x x x x x x x x x x x x x x x x x	h HST-FR27), Socket Extension Tool ( ))1 x x x <u>x</u> <u>x</u> <u>x</u> <u>x</u> <u>x</u> <u>x</u>
ж ж 001:00:00 ж 001:00:015ж х 001:00:15ж ж	→ ECUP harness connection needs to be r     → 1 tool caddy, ¶     → → WFC3 Tool Caddy. (Ground     → → → WFC2-Interface Platef)     → → → → WFPC2-Interface Platef)     → → → → WFPC2-Interface Platef)     → → → → → WFPC2-Interface Platef)     → → → → → WFPC2-Interface Platef)     → → → → → → WFPC2-Interface Platef)     → → → → → → → WFPC2-Interface Platef)     → → → → → → → WFPC2-Interface Platef)     → → → → → → → → → → WFPC2-Interface Platef)     → → → → → → → → → WFPC2-Interface Platef)     → → → → → → → → → → → → → WFPC2-Interface Platef)     → → → → → → → → → → → → → → → → →	nade after WFC3 installation (for thermal-protection)¶ Strap Tool, Connector Tool, Stabilization Tool (remains in Interface Plate), Harness Tool (remains on ECU harness avity, WFPC2, WFC3, and any EM open bays¶ ig—V1 axis¤ x x Start-of-Day-1¤ x Daily GA/DR-Power-Up and Checkout~(00:15)¤ • → TBD tasks¤ x Retrieve WFC3 Tool-Caddy~(01:33)¤ x x	n HST-FR27), Socket Extension Tool ( NT x x x x x x x x x
ਸ ਸ ਸ 001:00:00 ਸ 001:00:15ਸ ਸ ਸ ਸ ਸ	→ ECUharness connection needs to be r     → 1 tool caddy: ¶     → → WFC3 Tool Caddy: (Ground     → → → WFC3 Tool Caddy: (Ground     → → → → WFC3     → → → → WFC2     → → → → WFC2     → → → → WFC2     → → → → → WFC2     → → → → → → WFC2     → → → → → → → WFC2     → → → → → → → → → WFC2     → → → → → → → → → → → WFC2     → → → → → → → → → → → → → → → → →	nade after WFC3-installation (for thermal-protection)¶ Strap-Tool, Connector Tool, Stabilization: Tool (remains in Interface Plate), Harness: Tool (remains on ECU harness avity, WFPC2, WFC3, and any EM open-bays¶ ga_V1:axisx x x x x Start-of-Day-1¤ x Daily GA/DR: Power-Up and Checkout-(00:15)× • → TED tasksx x Retrieve WFC3-Tool-Caddy-(01:33)× x x x	HST-FR27), Socket Extension Tool ( HST-FR27), Socket Extension Tool ( HX
メ メ メ 001:00:00 メ 001:00:15 メ メ メ メ メ 、 、 、 、 、 、 、 、 、 、 、 、 、	→ ECUharress connection needs to be → 1 tool caddy:¶     → → WFC3 Tool Caddy:(Ground     → → WFC3 Tool Caddy:(Ground     → → → WFC3 Tool Caddy:(Ground     → → → → WFC3     → → → WFC2     → → WFC2     → → → WFC2     → → → → WFC2     → → → → → → → WFC2     → → → → → → → → → → → → → → → → →	nade after WFC3 installation (for thermal-protection)¶ Strap: Tool, Connector: Tool, Stabilization: Tool (remains in Interface Plate), Harness Tool (remains on ECU-harness avity, WFPC2, WFC3, and any-EM open-bays¶ g=\/1-avisx           x           x           x           Daily GA/DR: Power: Up: and Checkout-(00:15)×           • - TBD tasks×           x           x           e - TBD tasks×           x           x	n HST-FR27), Socket-Extension Tool- × × × × × Daily-GA/DR-Power-Up-and-Ch × + × Retrieve-WFC3-Tool-Caddy-(0* × × × × × × × × × × × × × × × × × × ×
х х х х х о01:00:00х х 001:0015х х х х х х х х	→ ECU harress connection needs to be → 1 tool caddy: [1 → WFC3 Tool Caddy: (Ground → 1 WFC2 Interface Platef] → Set Sun-Protection-required for HST WF cc → Set Sun-Protection-required for HST WF cc → HST SAs positioned at 0° and sun alor × × × × × Daily GADR Power Up and Checkout- (00:15)¤ → HSD tasks¤ × × × Peterse Phrases (00:01)¤ → Set Brakes (00:01)¤ → Set Brakes (00:01)¤ ×	nade after WFC3 installation (for thermal-protection)¶ Strap Tool, Connector Tool, Stabilization Tool (remains in Interface Plate), Harness Tool (remains on ECU harness avity, WFPC2, WFC3, and any-EM open bays¶ ig→/1-axis¤           Image: A strate of the strate of th	n HST-FR27), Socket Extension Tool- × × × × × × × × × × × × × × × × × × ×
ਸ ਸ ਸ 001:00:00 ਸ 001:00:15ਸ ਸ ਸ ਸ ਸ ਸ ਸ ਸ ਸ ਸ ਸ ਸ ਸ ਸ ਸ ਸ ਸ ਸ ਸ	→ ECU harness connection needs to be → 1 tool caddy, ¶     → WFC3 Tool Caddy. (Ground     → → WFC2 Tool Caddy. (Ground     → → → WFC2     → Sun-Protection required for HST-WF cc     → Sun-Protection required for HST-WF cc     → HST- <u>SAs</u> positioned at 0° and sun alor     ×	nade after WFC3-installation (for thermal-protection)¶ Strap-Tool, Connector Tool, Stabilization: Tool (remains in Interface Plate), Harness: Tool (remains on ECU harness avity, WFPC2, WFC3, and any EM open bays¶ gg=V1:avisx x x Start-of-Day-1¤ x Daily GA/DR-Power-Up-and-Checkout-(00:15)× • → TBD tasksX x x x x x x x x x	HST-FR27), Socket-Extension Tool- HST-FR27), Socket-Extension Tool- H H H H H H H H H H H H H
ж ж 001:00:00ж ж 001:00:15ж ж ж ж ж ж	→ ECU harress connection needs to be → 1 tool caddy: [1 → → WFC3 Tool Caddy: (Ground → → WFC3 Tool Caddy: (Ground → → → WFC3 Tool Caddy: (Ground → → → WFC3 → → WFC2 → → WFC2 → → WFC2 → → WFC2 → → → → → WFC2 → → → → → → → → WFC2 → → → → → → → → → → WFC2 → → → → → → → → → → → → → → → → →	nade after WFC3 installation (for thermal-protection)¶ Strap: Tool, Connector: Tool, Stabilization: Tool (remains in Interface Plate), Harness Tool (remains on ECU-harness avity, WFPC2, WFC3, and any-EM open-bays¶ g=_V1-axis¤           x           x           x           x           x           x           x           x           x           Daily CA/DR: Power Up and Checkout+(00:15)¤           • → TBD tasks¤           x	n HST-FR27), Socket Extension Tool ( )))¶ X X X X X X X X X X A Refrieve WFC3-Tool Caddy-(0' X X X X X X X X X X X X X
X X X 001:00:00# X 001:00:15# X X X X X X X X X X X X X	→ ECU harress connection needs to be → 1 tool caddy: [1     → → WFC3 Tool Caddy: (Ground → → → WFC3 Tool Caddy: (Ground → → → WFC3 therface Plate] → Sun-Protection required for HST WF cc → HST SAs positioned at 0° and sun alor ×	nade after WFC3 installation (for thermal-protection)¶ Strap Tool, Connector Tool, Stabilization Tool (remains in Interface Plate), Harness Tool (remains on ECU-harness avity, WFPC2, WFC3, and any-EM-open-bays¶ gV1-avisx x x x x x x x x x x x x x x x x x x	n HST-FR27), Socket Extension Tool ( )))¶ x x x Daily <u>GA/DR:Power Up and Ch</u> x -→ TBD-tasksx <u>Retrieve WFC3 Tool Caddy</u> (0' x x x x x x x x x x x x x
ж ж 001:00:00 ж 001:00:15ж ж ж ж ж ж ж ж ж ж ж ж	→ ECUP harness connection needs to be → 1 tool caddy: {{         1 → ↓ WFC3 Tool Caddy: (Ground + ↓ ↓ WFC3 Tool Caddy: (Ground + ↓ ↓ WFC2 + ↓ ↓ WFC2 + ↓ ↓ WFC2 + ↓ Sun-Protection required for HST WF cc + ↓ Sun-Protection required for HST WF cc × ↓ HST- <u>SAs</u> positioned at 0° and sun alor × × ↓ HST- <u>SAs</u> positioned at 0° and sun alor × × ↓ HST- <u>SAs</u> positioned at 0° and sun alor × × × ↓ HST- <u>SAs</u> positioned at 0° and sun alor × × ↓ HST- <u>SAs</u> positioned at 0° and sun alor × × ↓ HST- <u>SAs</u> positioned at 0° and sun alor × × ↓ HST- <u>SAs</u> positioned at 0° and sun alor × × ↓ HST- <u>SAs</u> positioned at 0° and sun alor × × × ↓ HST- <u>SAs</u> positioned at 0° and sun alor × × × ↓ HST- <u>SAs</u> positioned at 0° and sun alor × × × ↓ HST- <u>SAs</u> positioned at 0° and sun alor × × ↓ HST- <u>SAs</u> positioned at 0° and sun alor × × ×	nade after WFC3-installation (for thermal-protection)¶ Strap-Tool, Connector-Tool, Stabilization Tool (remains in Interface Plate), Harness Tool (remains on ECU harness avity, WFPC2, WFC3, and any-EM open bays¶ ig=\/1 varisx           x           x           x           baily GA/DR: Power-Up and Checkout - (00:15)×	n HST-FR27), Socket Extension Tool ( ))  X X X X Daily GA,DR Power Up and Ch • → TBD-tasks× X Retrieve WFC3 Tool Caddy: (0' X X X X X X X • → Release Brakes: (00' • → Acquire WFC3 Tool C (00:20)× • → Acquire WFC3 Tool C (00:20)× • → Release Drakes: (00' • → Release Drak
	→ ECU harress connection needs to be → 1 tool caddy: ¶     → → WFC3 Tool Caddy: (Ground     → → → WFC3 Tool Caddy: (Ground     → → → → WFC3 Tool Caddy: (Ground     → → → → → → → → → → → → → → → → →	nade after WFC3 installation (for thermal-protection)¶ Strap: Tool, Connector: Tool, Stabilization: Tool, remains in Interface Plate), Harness: Tool (remains on ECU-harness avity, WFPC2, WFC3, and any EM open-bays¶ g=_V1-axisx x Start-of-Day-1¤ x Daily GA/DR: Power-Up: and Checkout-(00:15)× • → TBD-tasks× x x x x x x x x x	HST-FR27), Socket Extension Tool ( M X X X X X X X X X X X X X
й           ж           й           001:00:00#           й           001:00:15%           ж           ж           ж           ж           ж           ж           ж           ж           ж           ж           ж           ж           ж           ж           ж           ж           ж           ж           ж	→ ECU harress connection needs to be → 1 tool caddy:¶     → → WFC3 Tool Caddy-(Ground     → → → WFC3 Tool Caddy-(Ground     → → → → WFC3 Tool Caddy-(Ground     → → → → → WFC2     → → → WFC2     → → → → → → → WFC2     → → → → → → → → → → → → → → → → →	nade after WFC3 installation (for thermal-protection)¶ Strap: Tool, Connector: Tool, Stabilization: Tool, remains in Interface Plate), Harness Tool (remains on ECU-harness avity, WFPC2, WFC3, and any-EM open-bays¶ g=\/1-avisx x Start-of-Day-1¤ x Daily GA/DR: Power-Up-and Checkout~(00:15)¤ • → TBD tasks¤ x Retrieve-WFC3 Tool-Caddy~(01:33)¤ x x x x x x x x x	h HST-FR27), Socket-Extension Tool ( )))¶ x x x Daily-GA/DR-Power-Up-and-Ch x x x Daily-GA/DR-Power-Up-and-Ch x x x x x x x x x x x x x x x x x x x
х х х 001:00:00ж х х х х х х х х х х х х х х х х х х	→ ECUParress connection needs to be → 1 tool caddy: [1     → → WFC3 Tool Caddy: (Ground → → → WFC3 Tool Caddy: (Ground → → → → WFC3 Tool Caddy: (Ground → → → → → WFC2 → → → → → → WFC2 → → Sun-Protection-required for HST WF cc → → HST SAs positioned at 0° and sun alor × × × × × × × Daily GA.DR: Power Up and Checkout- (00:15)¤ → TBO tasks ¤ × × × Tertireve WFC3 Tool Caddy: (01:33)¤ Command EM tool stowage door open¤ → Set Brakes· (00:01)¤ × × Set Brakes· (00:01)¤ ×	nade after WFC3 installation (for thermal-protection)¶ Strap Tool, Connector Tool, Stabilization Tool (remains in Interface Plate), Harness Tool (remains on ECU harness avity, WFPC2, WFC3, and any-EM open bays¶ g//1-avits¤ x <u>Start-of-Day-1¤ x Daily GA:DR:Power Up and Checkout</u> -(00:15)¤ •→ TBD tasks¤ x <u>Retrieve WFC3 Tool-Caddy</u> -(01:33)¤ x x x x x x x x x	HST-FR27), Socket-Extension Tool ( NHST-FR27), Socket-Extension Tool ( NHT × × × Daily GA/DR-Power-Up and Chr × × TED-tasks× × Retrieve-WFC3-Tool-Caddy-(01 × × × × × × × × × × × × ×

the IRISH SOFTWARE ENGINEERING RESEARCH CENTRE

## HRSM Procedures

WFC3_mod_01	21.doc - Microsoft Word		
Eile Edit View	Insert Format Tools Table Window Help Add	o <u>b</u> e PDF Acrobat ⊆omments	Type a question for help 🛛 🗸 🗙
	3 🗅 🖤 🛍   X 🖻 🖪 🟈 19 - 1 😣 💷 [	¶ 100% 👻 🛞 📖 Read 🛛 💾 Normal + Helve	• 8 • <b>= = #</b>
Spagit 🛃 Wir	dow -		
	<b>y</b> • 1 • • • 1 • • • 2 • • • 1 • • • 3 • • • 1 •	4 1 5 1 6 1 .	,
0	¤	Ħ	<b>Z</b>
- 11 TASK-*	¤	WFC3·Installation¤	Π
- ELA PSED-TIME DY->HR->MIN*	GA¤	DR-2¤	DR-1
· · · · · · · · · · · · · · · · · · ·	→ → → WFC3-Tool Caddy-(Ground     → → → WFPC2     → → → WFPC2     → → 1/WFPC2-Interface-Plate¶     → Sun-Protection required for HST-WF-cc     → HST-SAs-positioned to <sup>0</sup> and sun alor	∙Shap Tool, Connector Tool, Stabilization Tool (remains in H Interface Plate), Harness Tool (remains on ECU harness))¶ avity, WFPC2, WFC3, and any EM open bays¶ ng –V1 axis¤	ST-FR27), Socket-Extension-Tool-(re [
<b>X</b>	X X	X	X X
	×	Start of Day 1¤	X
× 001:00:00×	X Daily-GA/DB-Power-Lip-and-Checkout(10:15)X	X Daily-GA/DR-Power-Lip and Checkout-(10:15)X	X Daily-GA/DR-Prover-Lip-and-Cher
- <u>x</u>	• → TBD-tasks×	• → TBD-tasks×	• → TBD-tasks¤
	(* column (Retrieve) AEC3. Tool: Carddy	("column (Retrieve) A/EC3. Tool. Cardy.	Column (Petrieve MEC3 Tool C
0:15×	(01-33) column ») a		
n (¶row(w	(* column (Command: EM:tool: strawage: door:	й	
- (•row(w	• (* column (Release Brakes (00:01))column *)	я	)row ),
• (•row(w	• • • • • • • • • • • • • • • • • • •	×	)row») <sub>e</sub>
4	location(00:10) column »)g		
· (*row(*	<pre>("column(Set.Brekes(nn-n1))column*);;</pre>	×	
= 6 🗉 3 🕸 🔇			
Page 1 Sec 1	1/21 At 1.1" Ln 1 Col 2 REC TI	RK EXT OVR English (U.S	

the IRISH SOFTWARE ENGINEERING RESEARCH CENTRE



💽 R2D2C: H	IST E	xample	Опв. 📃 🗆 🗙
File Edit T	ools	Help	
Compile	Run	View	
Natural Lan	iguag	e Input	Requirements Design Code Testing
channel brake GA = brakese DRone = brak DRtwo = brak System = DR	erelea t!0-> (eset 1 eset ? one []	se, bra GA ; ? x -> br ? x -> wf (   }  ] DI	keset, stabilize, wfctoolaquire : T ; ′akerelease ! 0 -> stabilize ! 0 -> brakeset ! 0 -> DRone ; ′ctoolaquire ! 0 -> brakeset ! 0 -> DRtwo ; Rtwo [  {   }  ] GA ;



🕼 R2D2C: HST Example	Three.			
File Edit Tools Help				
Compile Run View				
Natural Language Input	Requirements	Design	Code	Testing
Transaction boltrelease = n Transaction brakeset = new Transaction stabilize = new Transaction wfctoolaquire = GA GA_init = new GA(brakes DRone DRone_Init = new D DRtwo DRtwo_init = new DF DRone_init.start(); GA_init.start();	ew Transaction(2); / Transaction(2); Transaction(2); new Transaction(2 set); Rone(boltrelease, Rtwo(boltrelease, b	?); brakeset, s irakeset, w	stabilize); fctoolaqu	ire);
EXECUTING:				
brakeset brakeset				
DEADLOCK DETECTED!				





Lero© 2010







**Conclusions** 

- Software must evolve.
- There is a tension between reliability, predictability and cost and this need for evolution.
- There is a need for an Evolving Critical Systems research effort.
- Lero and others are driving that effort.



Any problem in computer science can be solved with another layer of indirection.

But that usually will create another problem.

David Wheeler





Edited by Mile Hinchey, Lowan Coyle, Bashar Nassibeh, and José Lais Findeire



**Essential Articles on Software Engineering** 



# Thank You

http://www.lero.ie/ecs/whitepaper





Higher Education Authority An tÚdarás um Ard-Oideachas



53