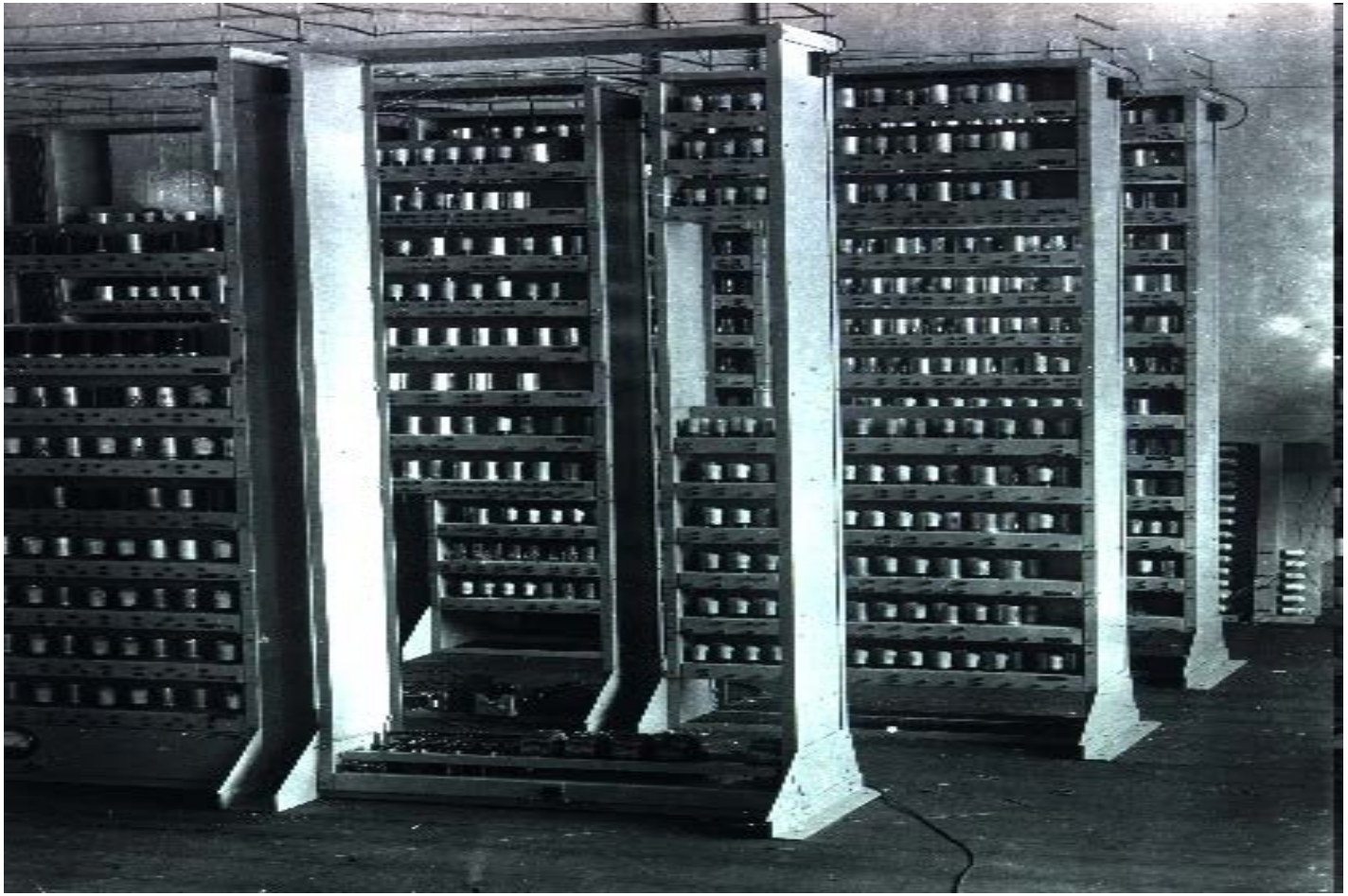
Lero THE IRISH SOFTWARE RESEARCH CENTRE

Building Resilient Space Exploration Missions

Prof. Mike Hinchey

University of Limerick Ollscoil Luimnigh
Trinity College Dublin
DCU
UCD Dublin
Ollscoil na Gaillimhe NUI Galway
Dundalk Institute of Technology
UCC University College Cork, Ireland Coláiste na hOllscoile Corcaigh
Maynooth University National University of Ireland Maynooth

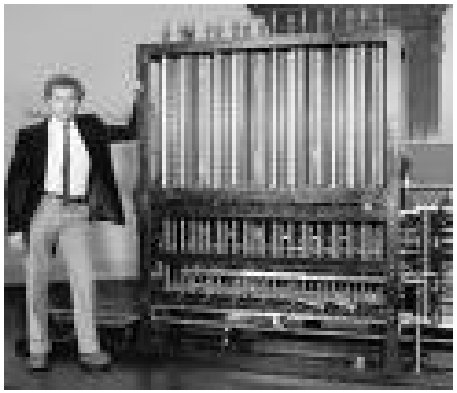
State of the Art (1949)

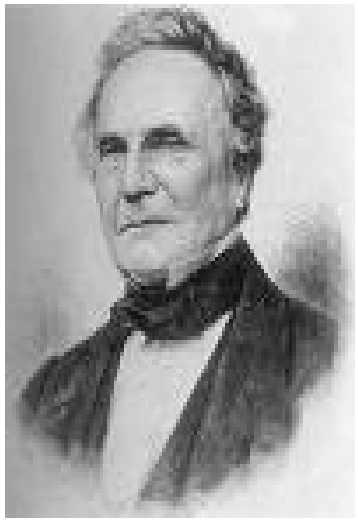


EDSAC

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





Motivation

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

...

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)

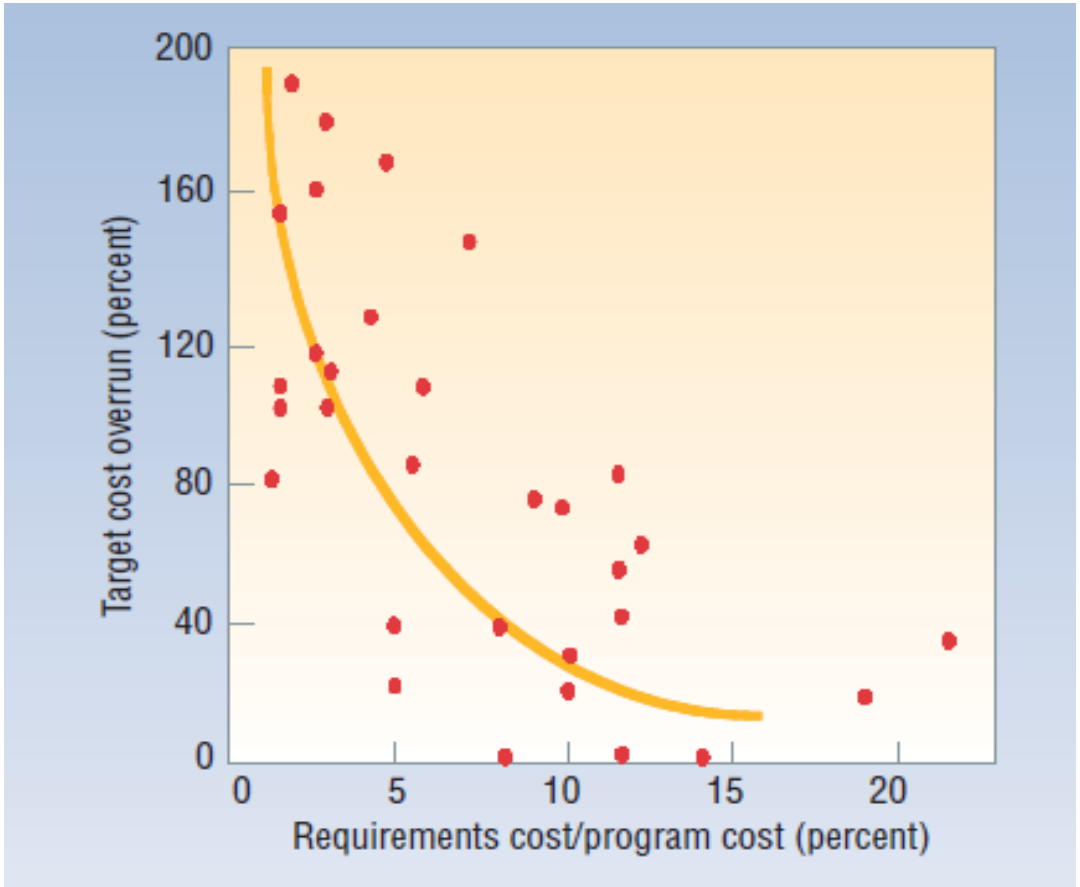
ERRATUM of the ERRATUM of the ERRATA of TAYLOR'S *Logarithms.* For cos. 4 18'3'', *read* 14 18' 3''.

Nautical Almanac (1836)

First Programmer

Augusta Ada King, Countess of Lovelace

Requirements Effort vs. Cost Overrun



Resilient Space Exploration Systems

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

Swarm Technologies

- Inspired by swarms of bees and flocks of birds in nature;

- Many application areas:
  - drug discovery;
  - communication systems;
  - environmental monitoring;
  - exploration.

Swarm Technologies

Coordinated swarms of smaller spacecraft will offer:

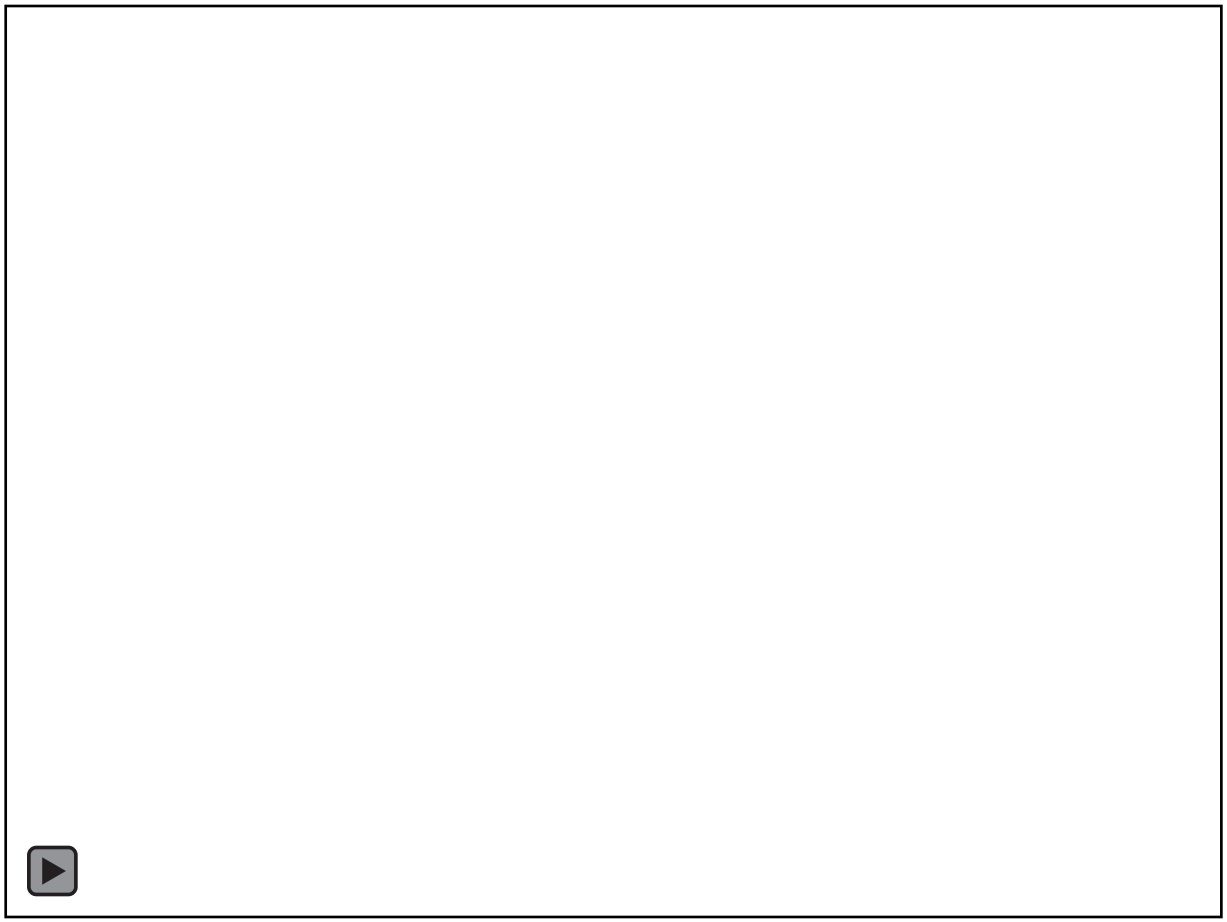
- More effective use of solar power;
- Access to areas where large craft could not go;
- Ability to perform more complex tasks;
- Greater accuracy and flexibility;
- RESILIENCE.

Autonomous NanoTechnology Swarm

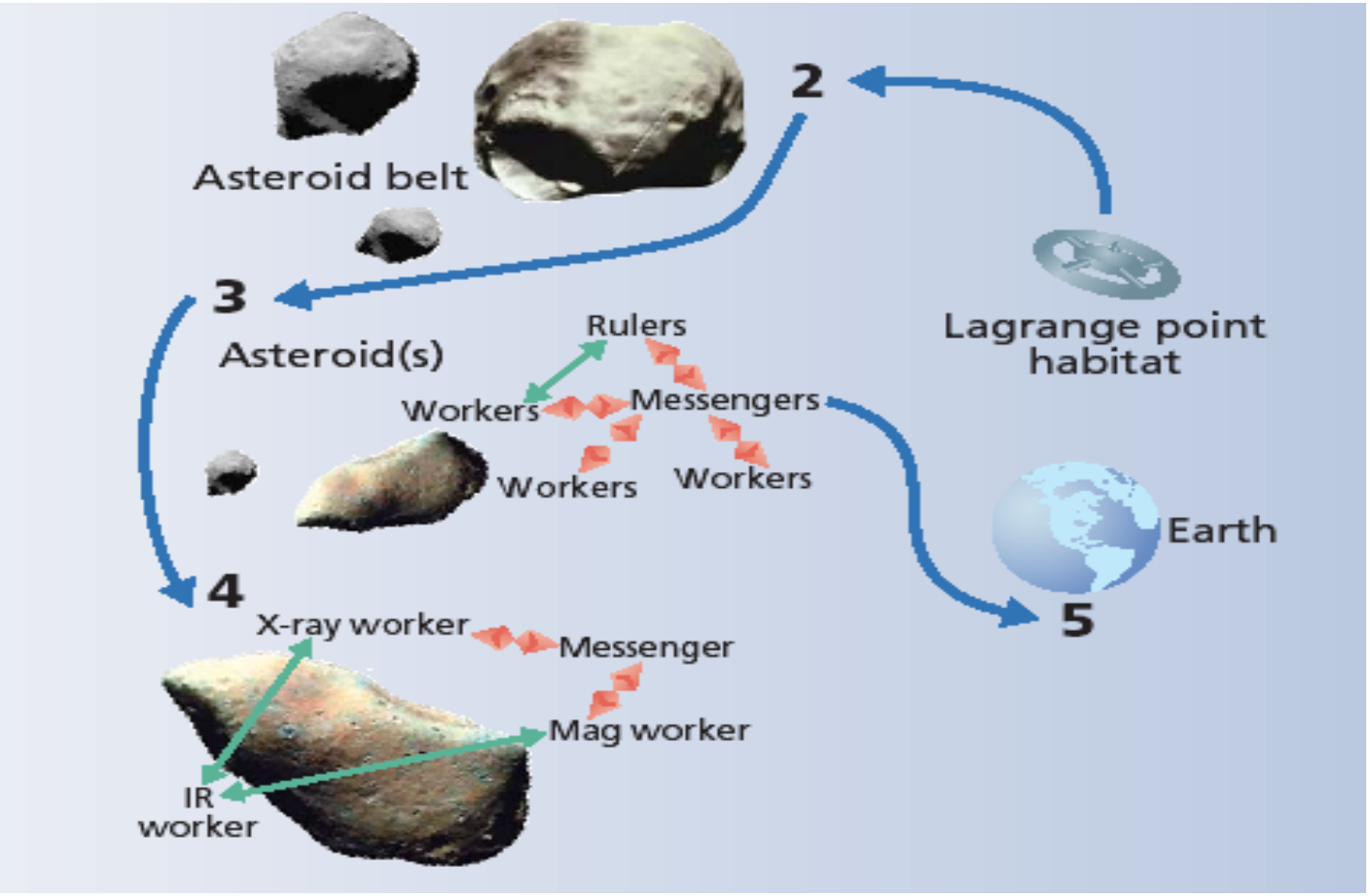
Using swarms of “intelligent”, autonomous spacecraft to explore

1. Lunar and Martian surface (Lander Amorphous Rover Antenna, LARA)
2. Saturn’s rings (Saturn Autonomous Ring Array, SARA)
3. Asteroid belt (Prospecting Asteroid Mission, PAM)

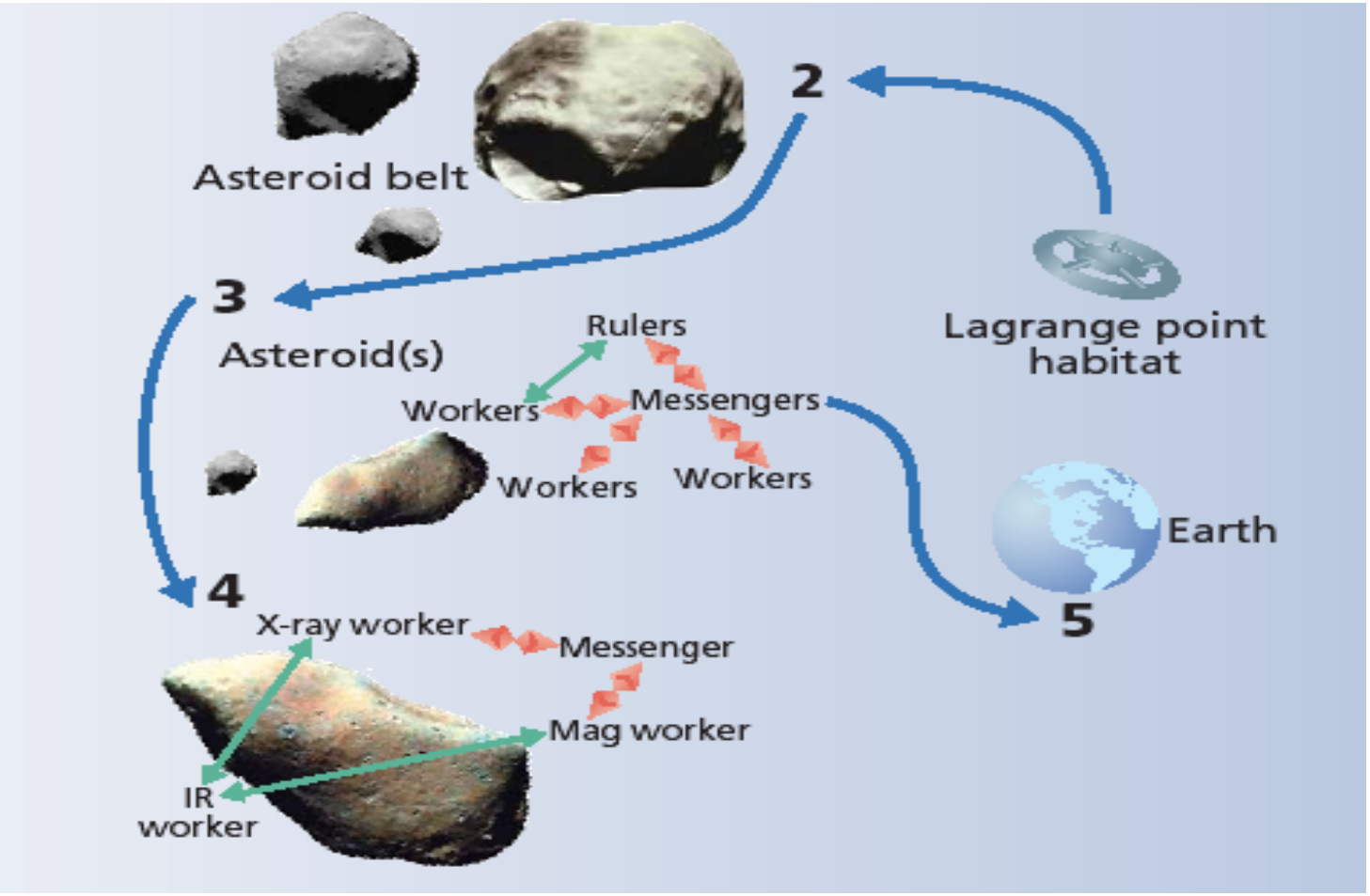
Walkers



ANTS Concept Mission - PAM



ANTS Concept Mission - PAM



Contributions

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

Model of Formal Method

V

Swarm Formal Method Model and Outline

$$LEADER\_COM_{i,com} = leader.in?\,msg \rightarrow$$
$$\text{case } LEADER\_MESSAGE_{i,com,msg}$$
$$\quad if\ sender(msg) = LEADER$$
$$MESSENGER\_MESSAGE_{i,com,msg}$$
$$\quad if\ sender(msg) = MESSENGER$$
$$WORKER\_MESSAGE_{i,com,msg}$$
$$\quad if\ sender(msg) = WORKER$$
$$EARTH\_MESSAGE_{i,com,msg}$$
$$\quad if\ sender(msg) = EARTH$$
$$ERROR\_MESSAGE_{i,com,msg}$$
$$\quad otherwise$$

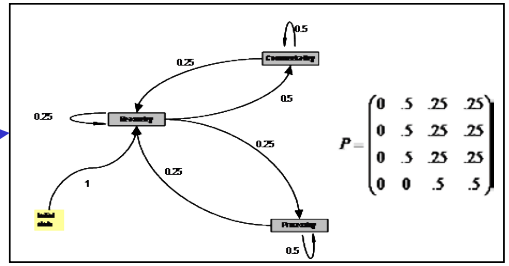
$$\Phi = \{SendMessage, ReceiveMessage, Reason, Process\}$$

is a set of (partial) transition functions where each transition function maps

$$Memory \times Input \rightarrow Output \times Memory$$

$$memory' = (Goals', Model', CommsTracking)$$

[Communicating]ReasoningDeliberatve(Leader)[Reasoning]
[Reasoning] SendMessage (Leader,Worker)[Communicating]
[Processing] SendMessage (Leader, Worker) [Communicating]



$$Communicating = 50\omega^2 : SendMessageWorker.Communicating$$
$$+ 50\omega^2 : SendMessageLeader.Communicating$$
$$+ 1\omega^1 : SendMessageError.Communicating$$
$$+ 50\omega^2 : ReceiveMessageWorker.Communicating$$
$$+ 50\omega^2 : ReceiveMessageLeader.Communicating$$
$$+ 1\omega^1 : ReceiveMessageError.Communicating$$
$$+ 50\omega^2 : ReasoningDeliberative.Reasoning$$
$$+ 50\omega^2 : ReasoningReactive.Reasoning$$
$$+ 17\omega^2 : ProcessingSortingAndStorage.Processing$$
$$+ 17\omega^2 : ProcessingGeneration.Processing$$
$$+ 17\omega^2 : ProcessingPrediction.Processing$$
$$+ 16\omega^2 : ProcessingDiagnosis.Processing$$
$$+ 16\omega^2 : ProcessingRecovery.Processing$$
$$+ 17\omega^2 : ProcessingRemediation.Processing$$

$$n\omega^{k+l} + m\omega^k = n\omega^{k+l} = m\omega^k + n\omega^{k+l}$$

$$n\omega^k + m\omega^k = (n+m)\omega^k = m\omega^k + n\omega^k$$

Agent State	Actions leading to the agent state	f	p
	Identity		
Communicating	SendMessageWorker	50	2
	SendMessageLeader	50	2
	SendMessageError	1	1
	ReceiveMessageWorker	50	2
	ReceiveMessageLeader	50	2
	ReceiveMessageError	1	1
Reasoning	ReasoningDeliberatve	50	2
	ReasoningReactive	50	2
Processing	ProcessingSortingAndStorage	17	2
	ProcessingGeneration	17	2
	ProcessingPrediction	17	2
	ProcessingDiagnosis	16	2
	ProcessingRecovery	16	2
	ProcessingRemediation	17	2

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 ~ ) }
   }
}
```

Autonomic Computing

Inspiration from the human/mammalian autonomic nervous system.

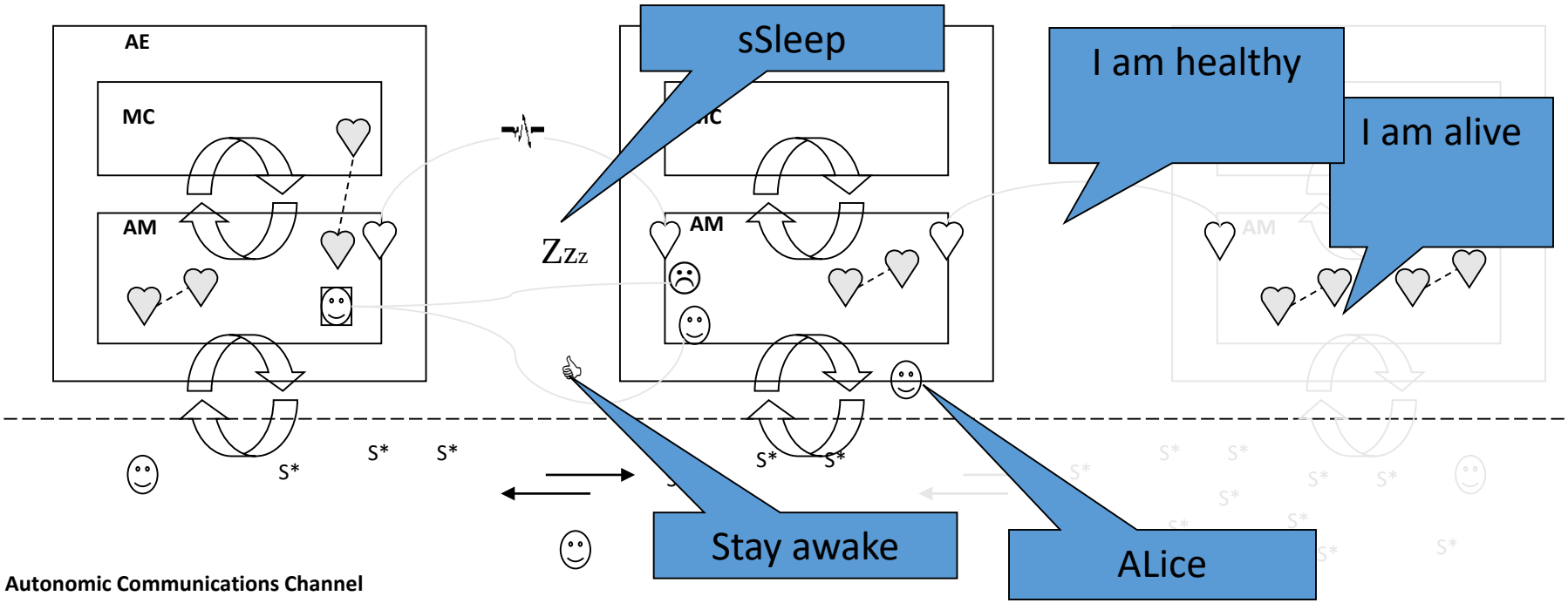
Fight or Flight

sympathetic
(SyNS)

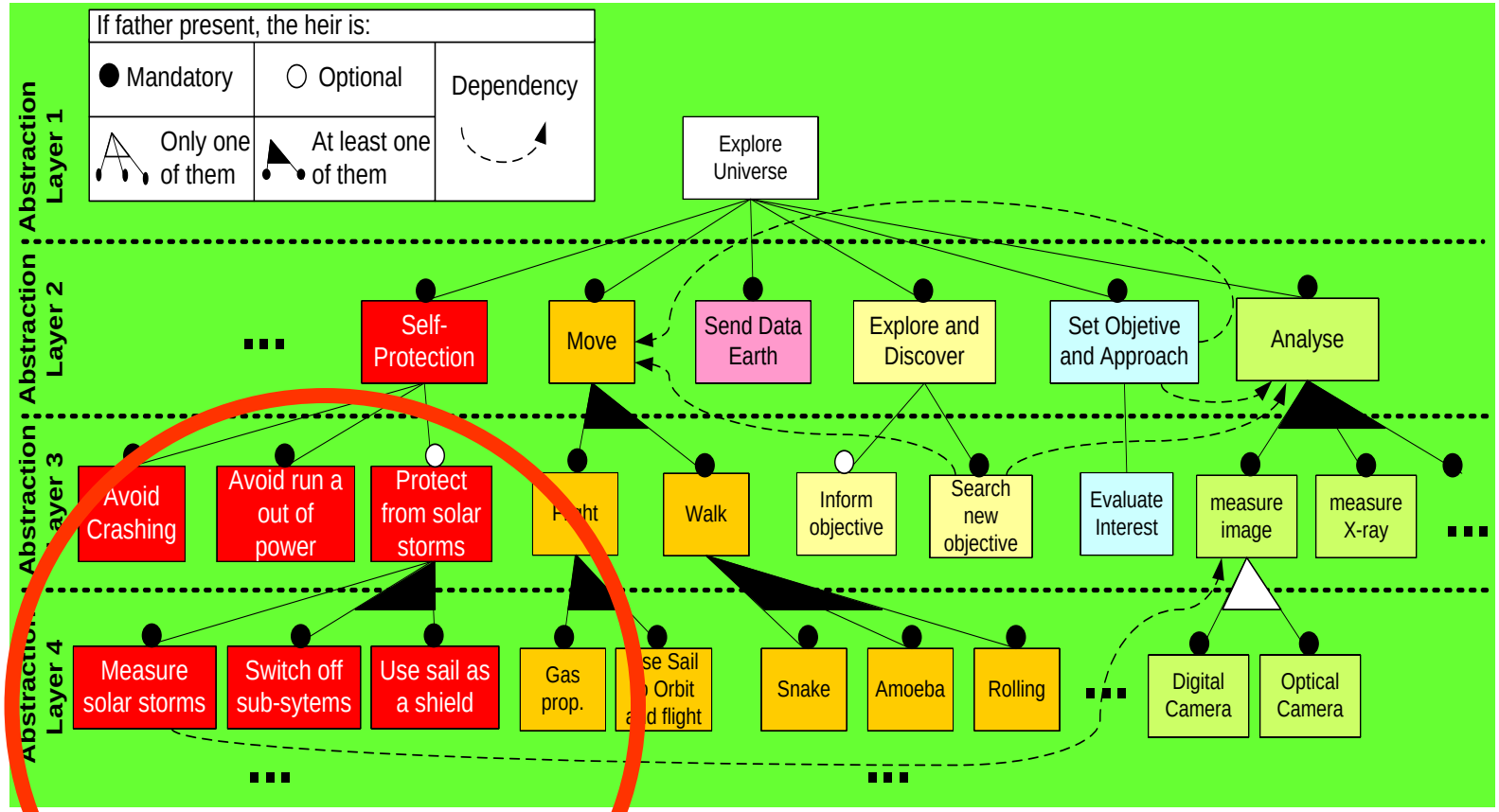
Rest and Digest

parasympathetic
(PaNS)

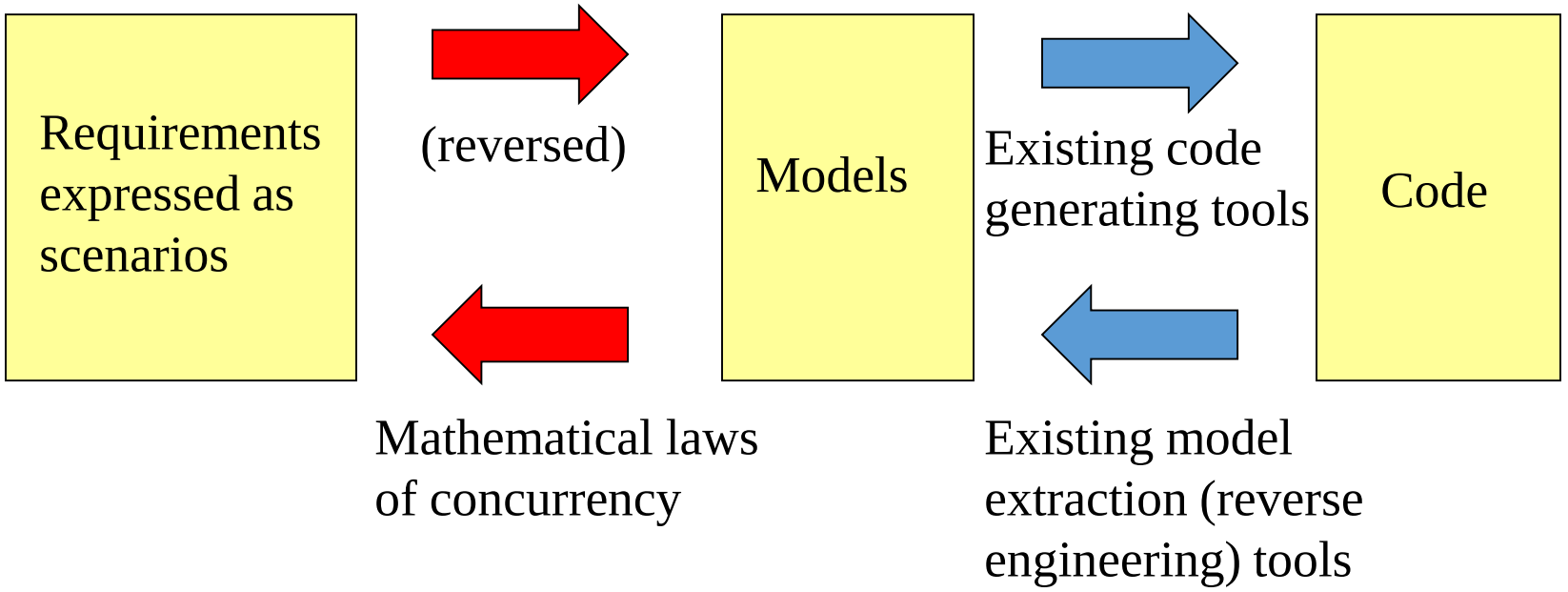
Autonomic Environment



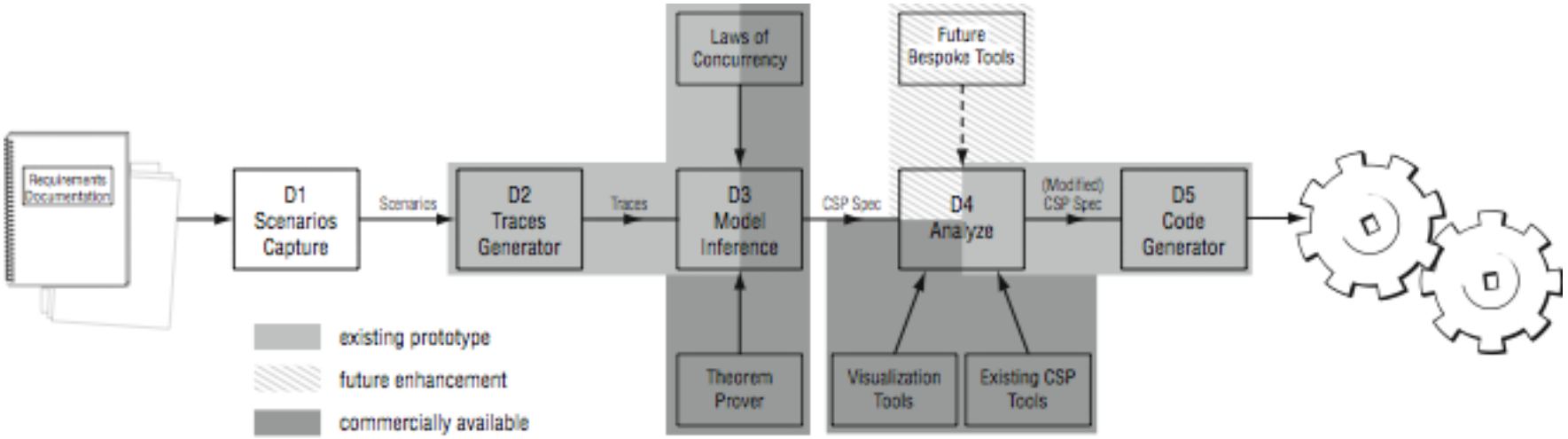
SPL / Feature Model



Requirements to Design to Code (R2D2C)



Current Status



Benefits of the Method

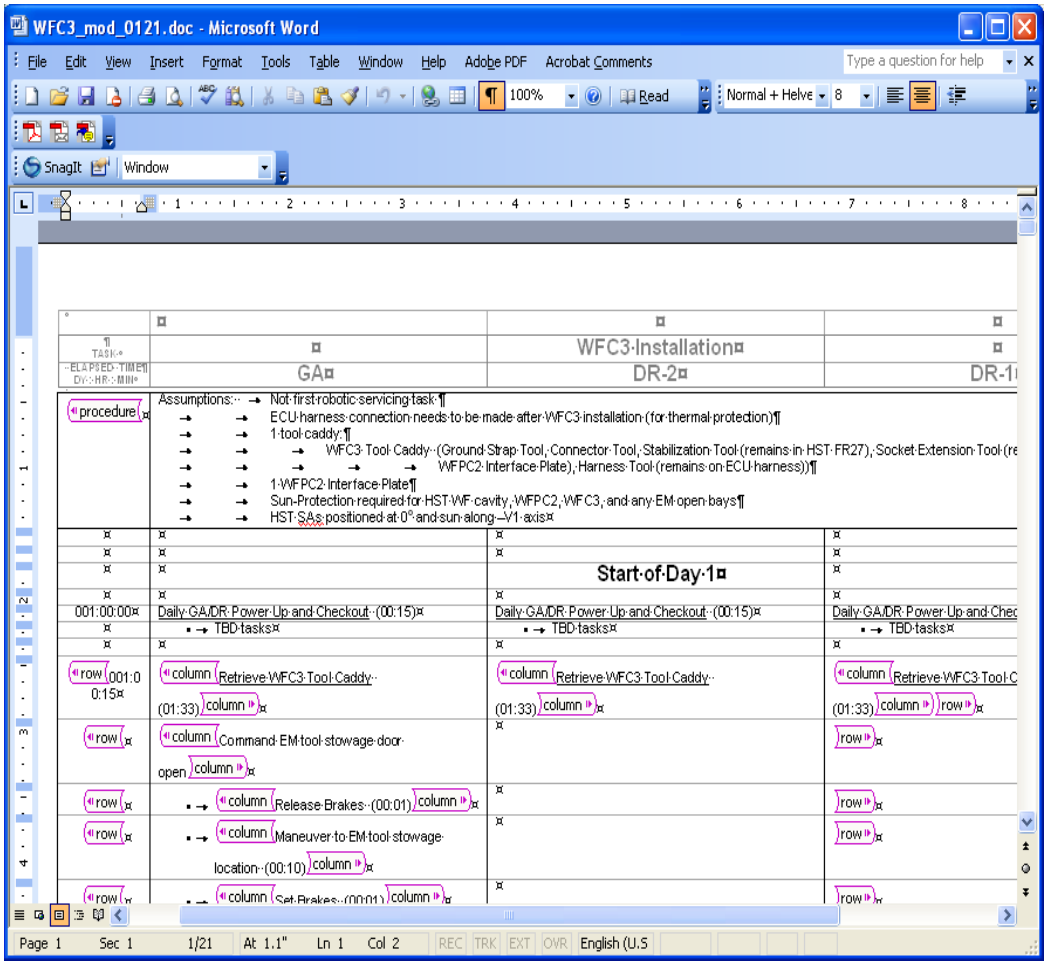
- Automation of entire development process;
- Significant increase in quality;
- Ability to do formal proof on properties of implementations;
- Ability to do formal proof of correctness;
- Automated means for requirements analysis;
- Guaranteed correspondence between requirements and their implementation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

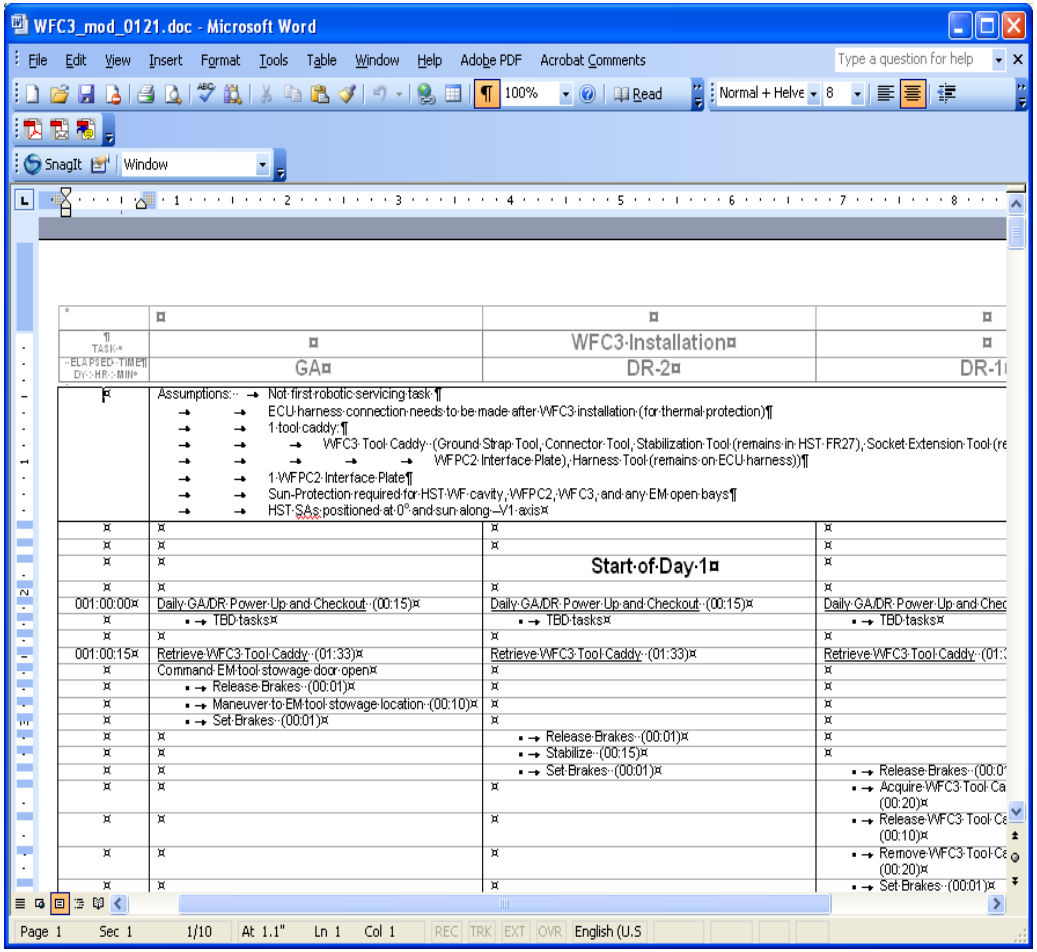
Applications

- 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.

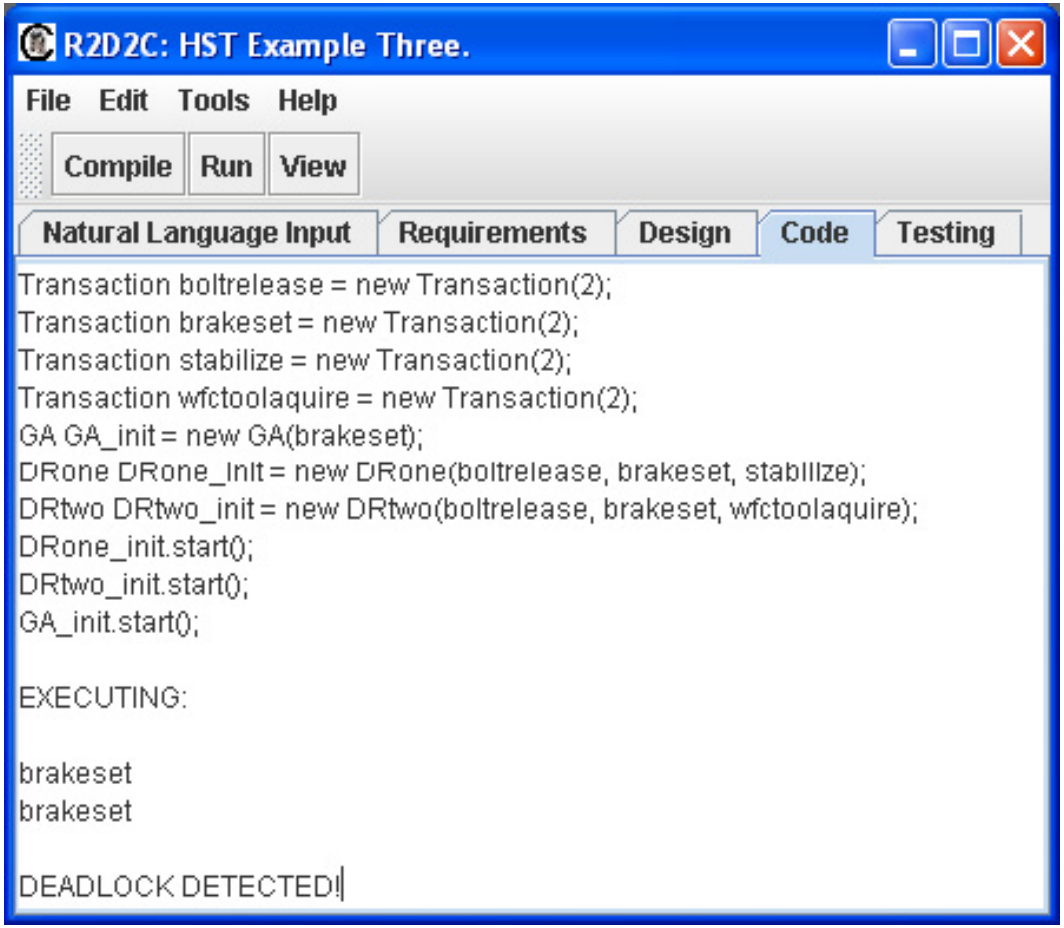
Domains (to date)

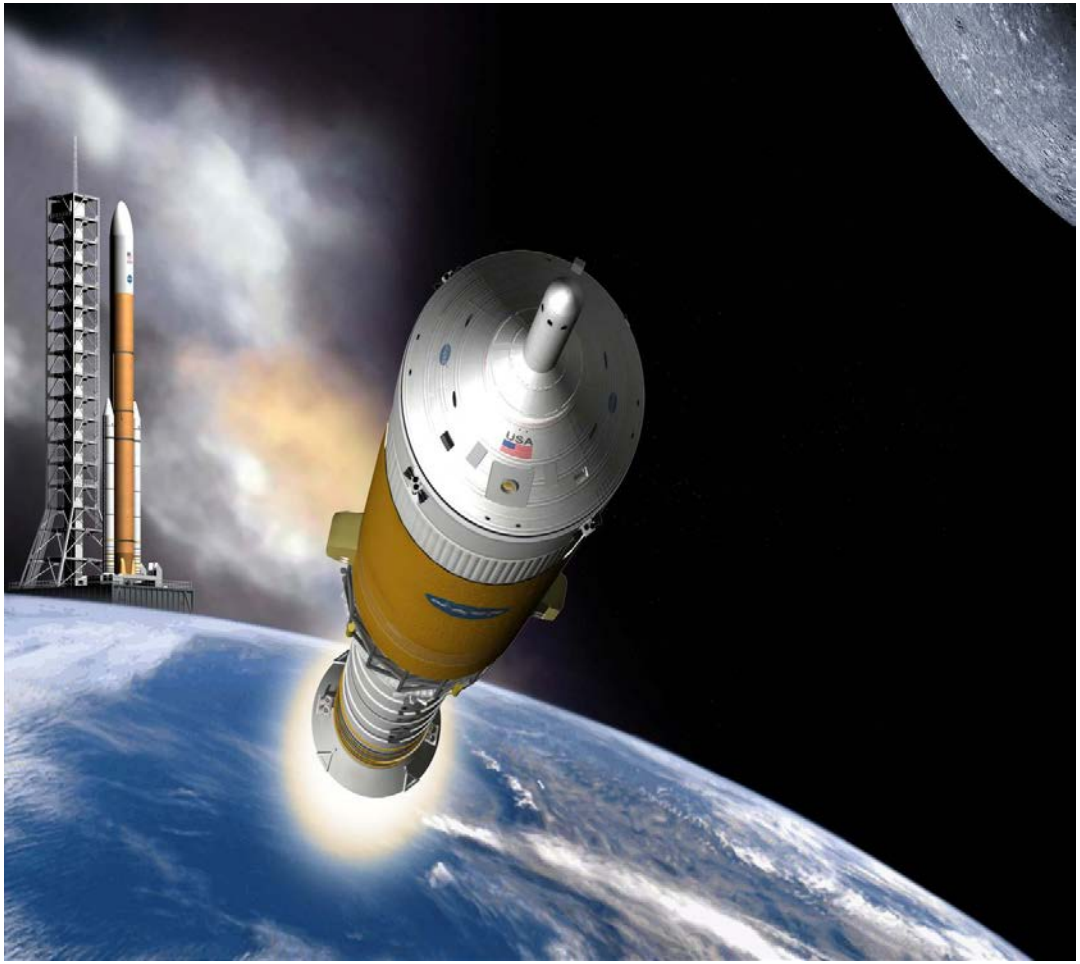
- Agent Based Systems;
- Wireless Sensor Networks ;
- ANTS;
- Verification of Robotic Procedures (cf. Hubble Space Telescope Robotic Servicing Mission).


WFC3_mod_0121.doc - Microsoft Word
File Edit View Insert Format Tools Table Window Help Adobe PDF Acrobat Comments
Type a question for help
Read
Normal + Helve
8
SnagIt
Window
TASK
ELAPSED TIME
DY:HR:MIN
GA
WFC3 Installation
DR-2
DR-1
procedure
Assumptions:
Not first robotic servicing task
ECU harness connection needs to be made after WFC3 installation (for thermal protection)
1 tool caddy:
WFC3 Tool Caddy (Ground Strap Tool, Connector Tool, Stabilization Tool (remains in HST FR27), Socket Extension Tool (re
WFPC2 Interface Plate), Harness Tool (remains on ECU harness))
1 WFPC2 Interface Plate
Sun Protection required for HST WF cavity, WFPC2, WFC3, and any EM open bays
HST SAs positioned at 0° and sun along –V1 axis
Start of Day 1
001:00:00
Daily GA/DR Power Up and Checkout (00:15)
TBD tasks
row
column
Retrieve WFC3 Tool Caddy
(01:33)
Command EM tool stowage door
open
Release Brakes (00:01)
Maneuver to EM tool stowage
location (00:10)
Page 1 Sec 1 1/21 At 1.1" Ln 1 Col 2 REC TRK EXT OVR English (U.S

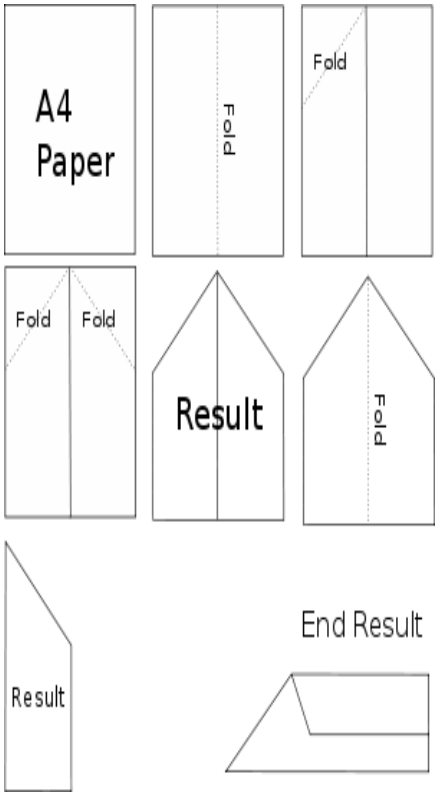

WFC3_mod_0121.doc - Microsoft Word
File Edit View Insert Format Tools Table Window Help Adobe PDF Acrobat Comments
Type a question for help
100% Read
Normal + Helve 8
SnagIt Window
WFC3 Installation
GA
DR-2
DR-1
Assumptions:
Not first robotic servicing task
ECU harness connection needs to be made after WFC3 installation (for thermal protection)
1 tool caddy
WFC3 Tool Caddy (Ground Strap Tool, Connector Tool, Stabilization Tool (remains in HST FR27), Socket Extension Tool (re
WFPC2 Interface Plate), Harness Tool (remains on ECU harness))
1 WFPC2 Interface Plate
Sun Protection required for HST WF cavity, WFPC2, WFC3, and any EM open bays
HST SAs positioned at 0° and sun along –V1 axis
Start of Day 1
001:00:00
Daily GA/DR Power Up and Checkout (00:15)
TBD tasks
001:00:15
Retrieve WFC3 Tool Caddy (01:33)
Command EM tool stowage door open
Release Brakes (00:01)
Maneuver to EM tool stowage location (00:10)
Set Brakes (00:01)
Stabilize (00:15)
Acquire WFC3 Tool Ca (00:20)
Release WFC3 Tool Ca (00:10)
Remove WFC3 Tool Ca (00:20)
Page 1 Sec 1 1/10 At 1.1" Ln 1 Col 1 REC TRK EXT OVR English (U.S


R2D2C: HST Example One.
File Edit Tools Help
Compile Run View
Natural Language Input Requirements Design Code Testing
channel brakerelease, brakeset, stabilize, wfctoolaquire : T ;
GA = brakeset ! 0 -> GA ;
DRone = brakeset ? x -> brakerelease ! 0 -> stabilize ! 0 -> brakeset ! 0 -> DRone ;
DRtwo = brakeset ? x -> wfctoolaquire ! 0 -> brakeset ! 0 -> DRtwo ;
System = DRone [| {| |} |] DRtwo [| {| |} |] GA ;


R2D2C: HST Example Three.
File Edit Tools Help
Compile Run View
Natural Language Input Requirements Design Code Testing
Transaction boltrelease = new Transaction(2);
Transaction brakeset = new Transaction(2);
Transaction stabilize = new Transaction(2);
Transaction wfctoolaquire = new Transaction(2);
GA GA_init = new GA(brakeset);
DRone DRone_init = new DRone(boltrelease, brakeset, stabilize);
DRtwo DRtwo_init = new DRtwo(boltrelease, brakeset, wfctoolaquire);
DRone_init.start();
DRtwo_init.start();
GA_init.start();
EXECUTING:
brakeset
brakeset
DEADLOCK DETECTED!


USA

Caveat



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

But that usually will create another problem.

David Wheeler

Lero THE IRISH SOFTWARE RESEARCH CENTRE

Go raibh maith agaibh!
Thank you!

SFI Science Foundation Ireland
Ireland's European Structural and Investment Funds Programmes 2014-2020
Co-funded by the Irish Government and the European Union
European Union
European Regional Development Fund
SOUTHERN Regional Assembly
Promoting our Region