Carleton UNIVERSITY

Artificially Intelligent Spacecraft as a Defence Strategy Against Hostile Cyber-Intervention

Prof Alex Ellery

Space Exploration Engineering Group (SEEG)

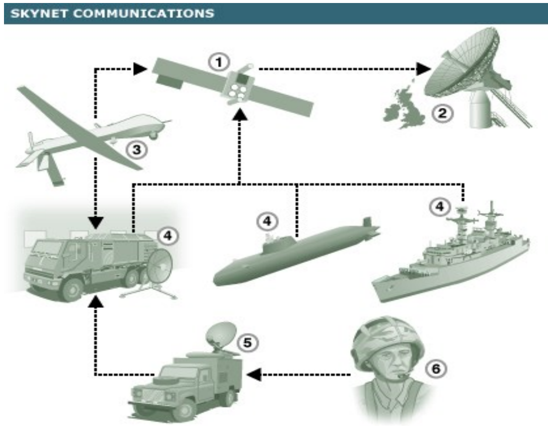
Carleton University, Ottawa, CANADA

12th Annual Conference on MILITARY SPACE SITUATIONAL AWARENESS London (26-27 Apr 2017)

Military Space Assets & Ground-Space Architecture

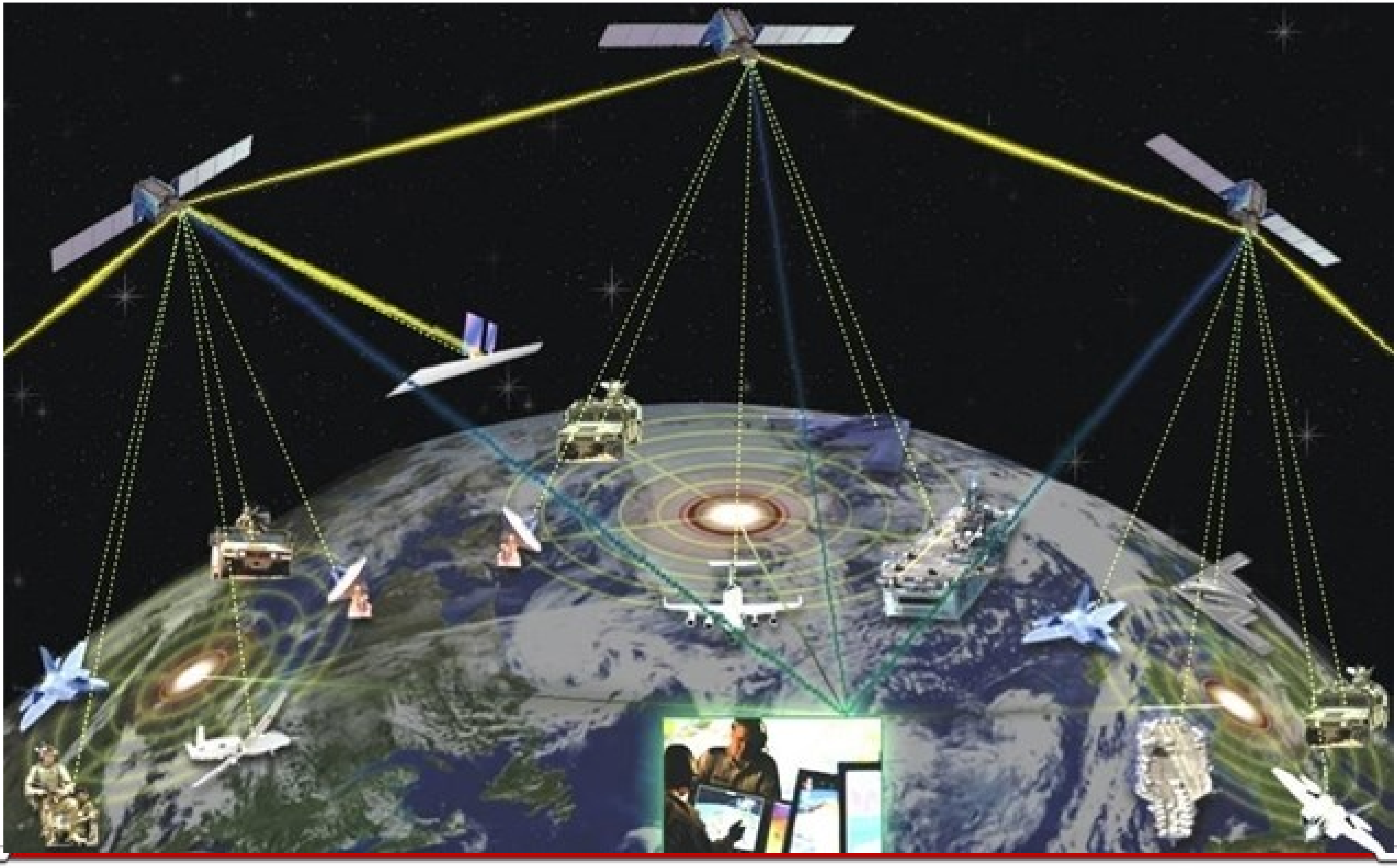
What military use is space?

1. GPS navigation is a core capability for military ground forces – broadcast downlink – TTC uplink only – no user uplink
2. Comsats for global communications in fixed orbits – TTC uplink - user uplink downlink via transponder relay, e.g. Skynet



3. Strategic/tactical reconn by EO – TTC uplink for orbit re-tasking – no direct user access
4. Meteorological monitoring and forecasting – TTC is same as for EO satellites
5. Internet-of-Things – military logistics (a la van Creveld)
6. Battlefield telemedicine

Backbone of the Future Battlefield



Example - Drones

- Drones operate through 3 radio links – aircraft transponder – GPS satellite – air-ground pilot control (via satellite)
- 1982: IDF Air Force deployed RPV squadrons against Syrian SAM air defence system in the Bekka Valley:

  (i) draw missile fire to deplete missiles

  (ii) recon missile radars and launch sites

  (iii) second wave manned air attack destroyed targets
- Aircraft losses: Syria - 80 Israel - 0
- Drones are the weapon system of choice for all kinds of political ailments

Satellite Vulnerability

- It was once assumed that high technological barrier rendered military satellites immune to attack
- US DoD used commercial services for 45% of its US-Gulf communications traffic during Desert Storm (first space war)
- However, there are 3 avenues of attack by state actors relevant to SSA

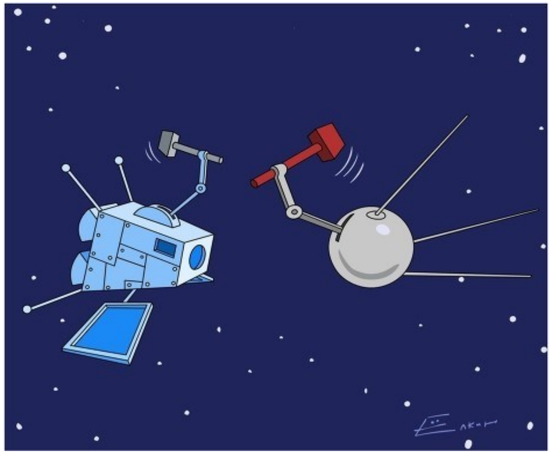
  (i) ASAT (anti-satellite) air-to-space missile

e.g. 2007: China fired missile at its Fengyun-1C mets increasing debris population by 30%

Satellite Vulnerability II

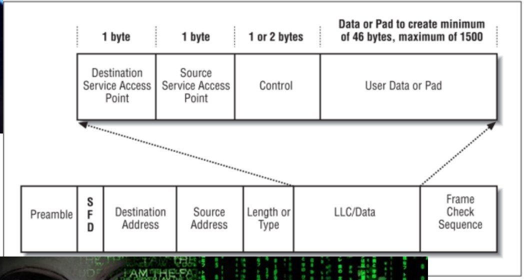
(ii) Micro-satellites introduce low-cost option for hunter-killer interceptors to observe, track and destroy satellites

- e.g. laser/particle/kinetic weapons for more selective attack to simulate debris
- e.g. Cubesats may be designed with low radar cross-setion for stealth



Stealth Attack

- Most insidious threat is that of which one is not aware until it happens – this is the ultimate challenge to SSA
- Cyber-threat is interference with satellite operations through its communications links (uplink)
- Virus appended data packets
- Example of asymmetric warfare waged by non-state aggressor against technological infrastructure



1 byte	1 byte	1 or 2 bytes	Data or Pad to create minimum of 46 bytes, maximum of 1500
Destination Service Access Point	Source Service Access Point	Control	User Data or Pad

Preamble	S F D	Destination Address	Source Address	Length or Type	LLC/Data	Frame Check Sequence

Types of Satellite Cyber-Attack

1. Direct communications (jamming) – denial-of-service (DOS)
2. Source of elint (malware)
3. Subversion of communications channel (misinformation)
4. Physical self-destruction
5. Subversion of satellite wholesale in pursuit of enemy`s goals

- Cyber-attack requires minimal technological investment
- Terrorism or even disaffected individuals
- Cyber-attack can be disguised as legitimate failure

History of Satellite Hacking

1. 1986: “Captain Midnight” disrupted uplink feed to Galaxy 1 TV broadcast satellite from Florida ground-station
2. 1995: Kurdish satellite channel jammed for broadcasting promotion of terrorism
3. 1997: Indonesian government imposed DOS attack on Tongan satellite regarding dispute over orbital slots
4. 2007: Sri Lankan Tamil Tigers hacked Intelsat to broadcast propaganda over TV and radio channels
5. 2009: hackers took control over NASA Terra EOS satellite (twice)
6. 2010: Dow Jones lost 9% die to flash (momentary) crash in GPS signals (accidental)

New Hacks

Non-satellite hacks can be implemented on satellites:

1. 2012: S Korean recon drone crashed into ground control station killing 3 people – N Korea jammed GPS signal
2. 2010: allegedly America-Israeli Stuxnet zero-day virus attacked Iranian nuclear processing plant centrifuges causing them to self-destruct

Stuxnet demonstrated that **computer viruses** can cause extensive physical damage to infrastructure facilities including satellites by manipulating control systems – a **version of munitions**

Satellite is a Hacker's Delight

- Orient solar arrays away from the sun to drain the batteries so on entering eclipse there is no power
- Feed constant current through solar array cells to encourage tin whisker growth short circuit
- Open louvres to heat sensitive batteries and optical surfaces to distort them
- Orient propellant tanks to deep space to freeze the propellant
- Induce mechanical resonant vibrations through reaction wheel motors or solar array motors
- Saturate reaction wheel drives to tumble the spacecraft
- Toggle thermal switches to re-distribute heat loads to sensitive components
- Dribble-leak propellant to shorten mission lifetime
- Overload CPU with DOS
- Spoof cameras by pointing them to the sun
- Switch open electronics/optics during SAA passage
- Overload diode protectors to breakdown voltage to generate power surges
- Intercept and re-direct communications traffic
- In all cases, ensure voltage/pressure/temperature sensors read nominal conditions
- In all cases, loss of functionality/failure may be attributable to random events

Multilayered Defence System

- **Isolate ground station from unauthorised users**

1. Firewalls cannot protect against password distribution across multiple users
2. Passwords – insecure due to multiple users – daily random letter/number generation are pseudorandom (unless quantum events exploited) and difficult to remember - easily remembered mnemonics with number substitution (Logica protocol) – resistance to change
3. Antivirus software (legacy only)

- **Isolate spacecraft from TTC uplink**

1. isolate spacecraft asset from ground by reducing TTC uplink sessions – last line of defence

AI – Raison D'Etre

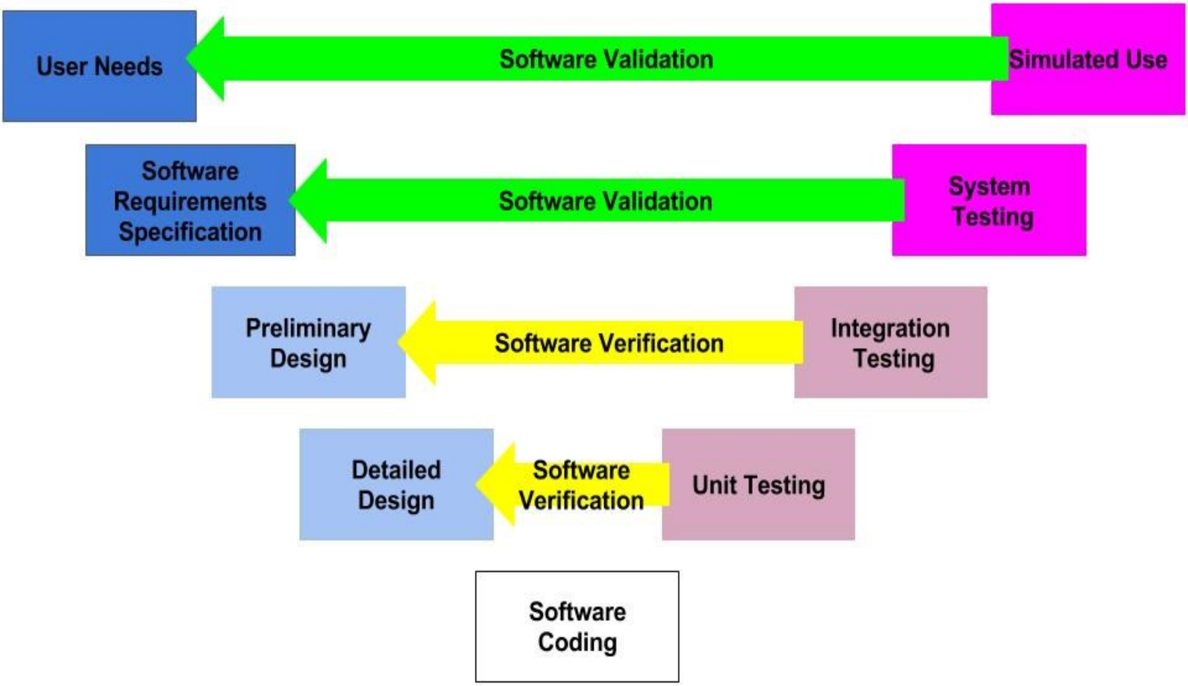
- Artificial intelligence methods permit autonomous satellite operations (launch-and-forget)
- Humans are poor decision-makers:

1. 1988: USS Vincennes in Persian Gulf shot down Iran Flight 655 Airbus killing 290 civilians – weapon crew authorised firing
2. 2009: human pilot of Air France airliner crashed into Atlantic during storm killing 228 passengers because ice formed in the pitot tubes measuring airspeed – pilot pitched up and stalled

- Autonomous operations are also desirable to reduce costs of ground station personnel
- PROBA (Project for On-Board Autonomy) focussed on fault detection, isolation and recovery (FDIR), autonomous navigation and mission planning
- I am proposing much more radical approach

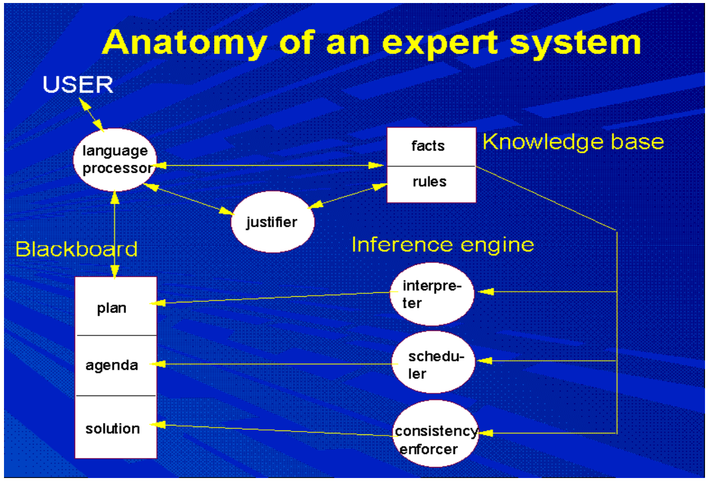
Verification & Validation

- Average released software has 11 bugs/1000 lines of code
- Space Agencies reduce this to 011 bugs/1000 lines of code through extensive V&V methods
- Program synthesis flow down is structured



Good Old Fashioned AI

- GOFAI is traditional approach to AI based on logical rules of inference – logic permits mathematical theorem proving techniques and program tracing
- Expert system comprises knowledge base of production rules of form: "IF (conditions) THEN (action)"
- GOFAI is structured – consistent with V&V required by space software
- Large expert systems suffer from large computational footprint, consistency maintenance and brittleness
- Non-monotonic logics (e.g. temporal logic of Remote Agent) weakens theorem proving validity


Anatomy of an expert system

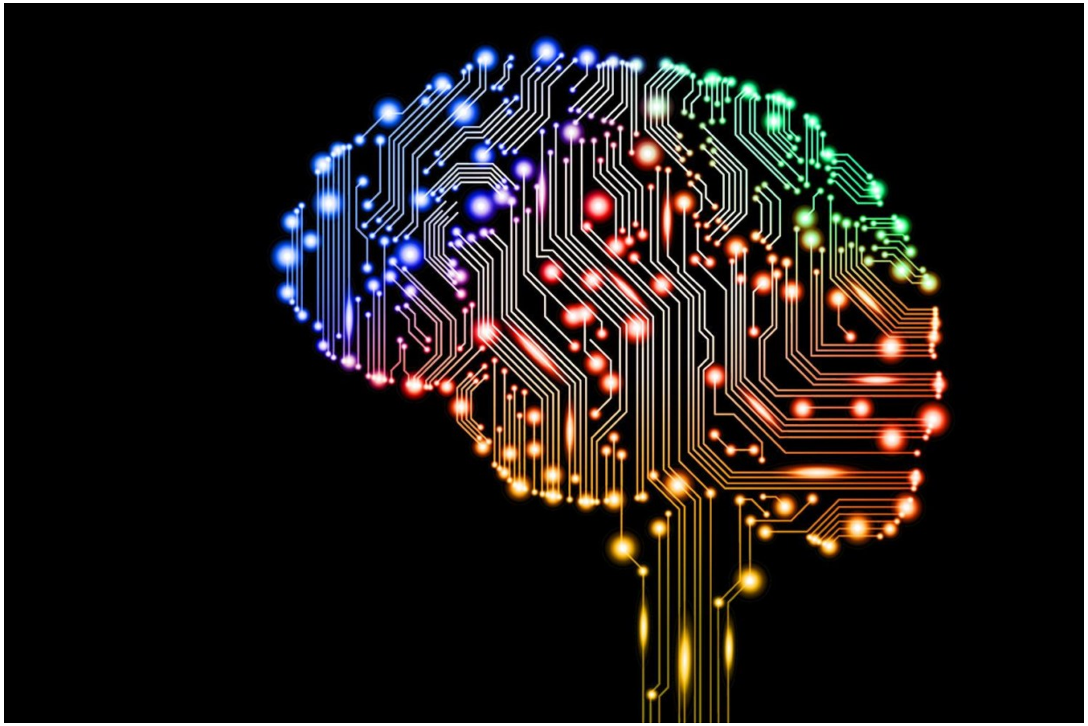
Fallibility of V & V

1. 1996: ESA’s Ariane 5 self-destructed within minutes of its maiden launch due to an error in its guidance system
2. 1999: NASA’s Mars Polar Lander experienced atmospheric vibrations which it interpreted as landing impact – it crashed from a great height
3. 1998: Mars Climate Observer received commands in units of lbf instead of N and inserted into too low a Mars orbit resulting in disintegration

Illusion of V & V has prevented adoption of soft computing methods of great power on spacecraft

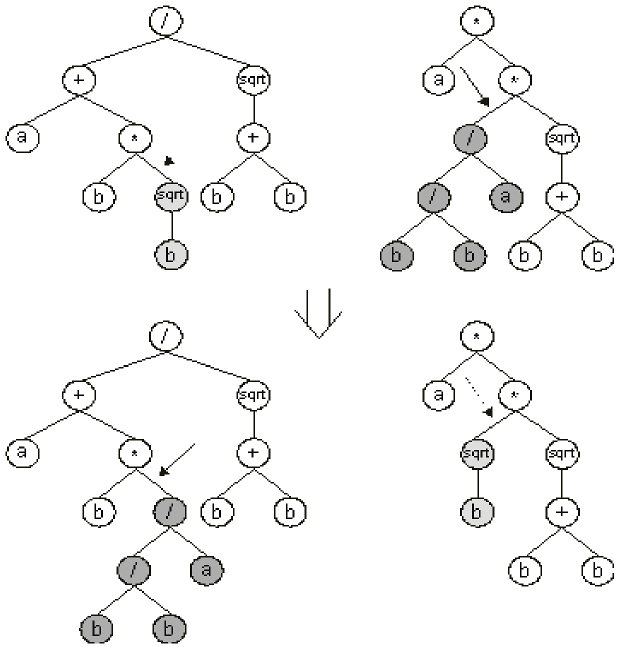
Proposed AI Architecture

- Genetic Program – Bayesian Network – Recursive Auto-Associative Memory – Recurrent Neural Network – FPGA hardware



Genetic Program

- Genetic program is high level programming language (Prolog) version of genetic algorithm
- Genetic program is inductive learning component
- Programs are subject a fitness function and evolved from generation to generation
- Cross-over of subtrees
- It learns Prolog condition-action rules



Bayesian Network

- Prolog rules form Bayesian network structured expert system with inheritance links
- Bayes rule gives a posterior probability of rule H given data D:

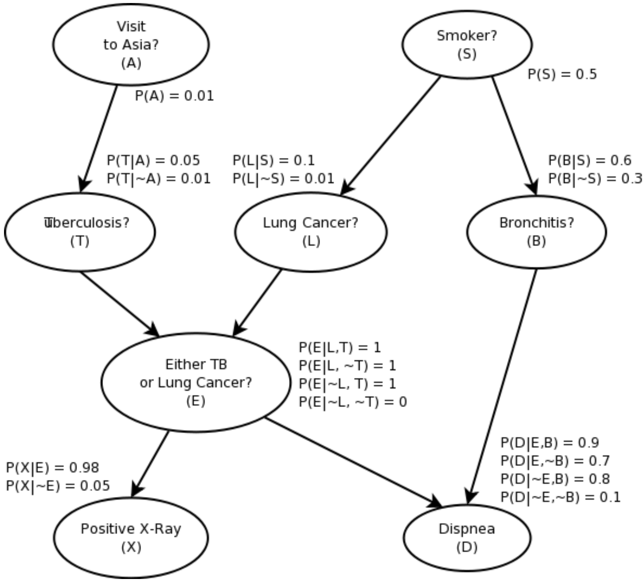
$$p(H \mid D) = \frac{p(D|H)\,p(H)}{p(D)}$$

- where p(H)=a priori probability of rule H

p(D)=probability of measuring data D,

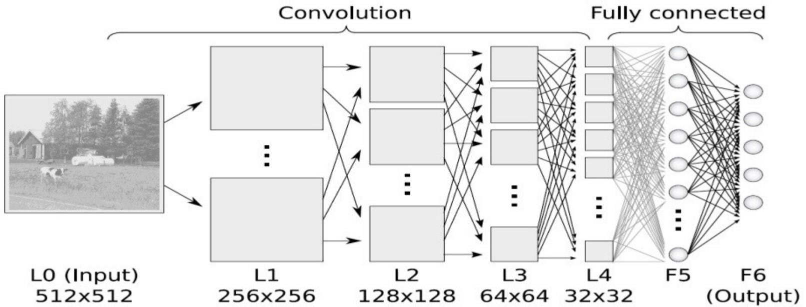
p(D|H)=probability of measuring data if

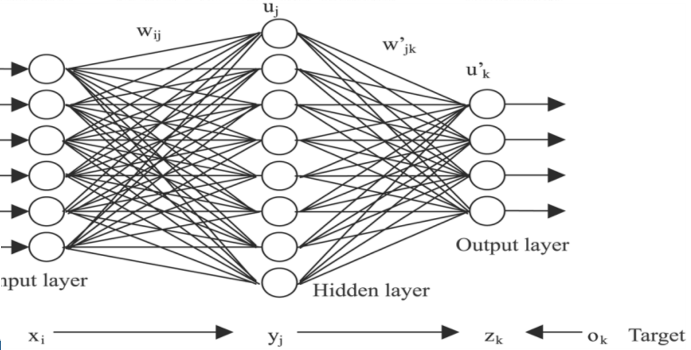
H is true

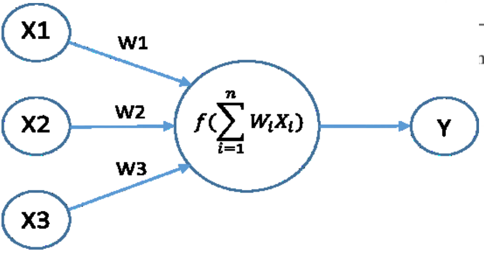


Deep Learning

- Deep learning involves unsupervised network followed by supervised network
- RAAM is preprocessor to encode rules compactly
- This is where magic happens.
- Multilayer NN is back-engine
- Neural net is layered network of thresholded switches







- Problem: neural network information is opaque to analysis

The Prestige!

- Weights w interpreted as a posteriori probabilities computing likelihood l(y|x,w) that training samples (x,y) are estimates of (y|x)
- Learning weights updated continuously using Kalman filter learning:

$$\hat{w}(t+1) = \hat{w}(t) + K(t)[y^{d}(t) - h(\hat{x}(t))]$$

- where $[y^{d}(t) - h(\hat{x}(t))]$ =error between estimated and measured output

$$K(t) = P(t)H(t)[(1/\eta)I + H(t)^{T}P(t)H(t)]^{-1}$$

$$\eta = [H(t)P(t)H(t)^{T} + R(t)]^{-1}P(t)$$

- Neural net compresses symbolic information around 100:1!
- Leaky integrate-and-fire neuron offers closer biological analogue with spiking output.

Neural Immunity

- Information flow is one-way

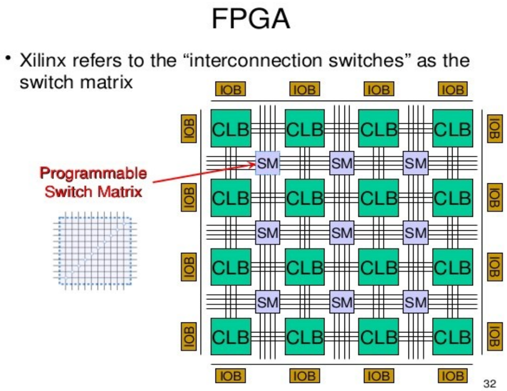
1. Learned networks downloaded to ground station
2. Rules extracted from neural net
3. V & V analysis performed on demand

- Neural net protects against Logic Bombs
- Logic Bombs must be installed in specific locations in software logic
- Stuxnet-like worms must be integrated into control software specifically to alter control parameters
- In neural net, logic is distributed throughout network in network matrix
- Hypothesis: neural controllers immune to worms
- However, neural net must be implemented in hardware

Field Programmable Gate Arrays

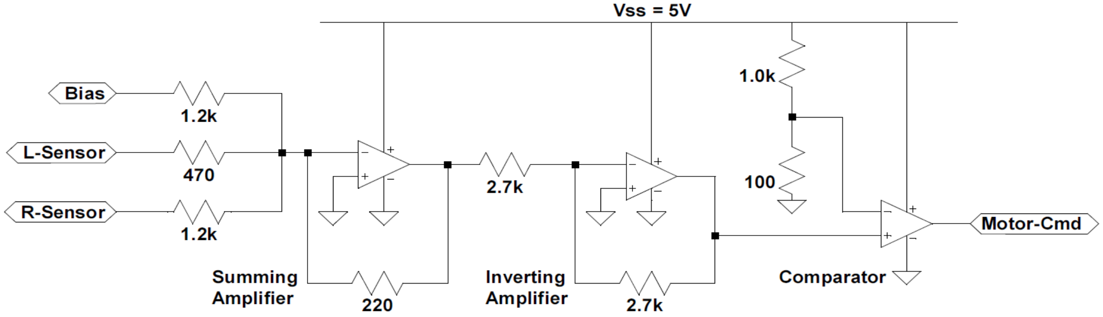
- Neural net may be implemented on FPGA for superior performance
- Neurons implemented as sub-blocks:

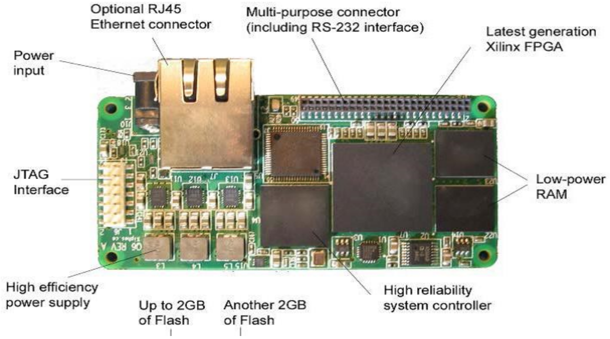
1. Multiplication of weighted inputs
2. Summation of weighted inputs
3. LUT implementation of sigmoid function
4. Control block to coordinate computations



FPGA

- Xilinx refers to the “interconnection switches” as the switch matrix



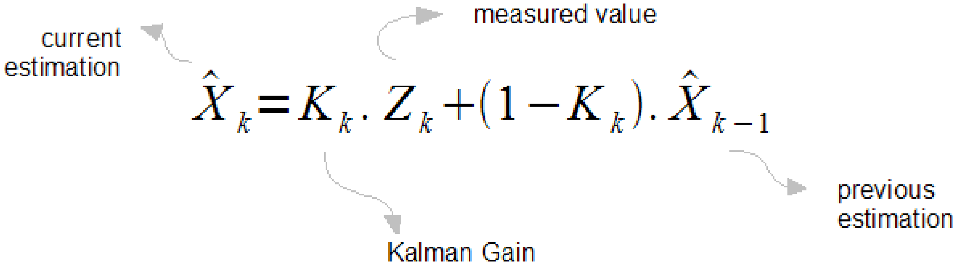


Optional RJ45 Ethernet connector
Multi-purpose connector (including RS-232 interface)
Latest generation Xilinx FPGA
Power input
JTAG Interface
Low-power RAM
High efficiency power supply
Up to 2GB of Flash
Another 2GB of Flash
High reliability system controller

- Xiphos Q6 card is space qualified

Fault Diagnosis

- AI model to compute residuals (signatures) by comparing AI model with spacecraft measurements using Kalman filter



$$\hat{X}_k = K_k \,.\, Z_k + (1 - K_k) \,.\, \hat{X}_{k-1}$$

current estimation

measured value

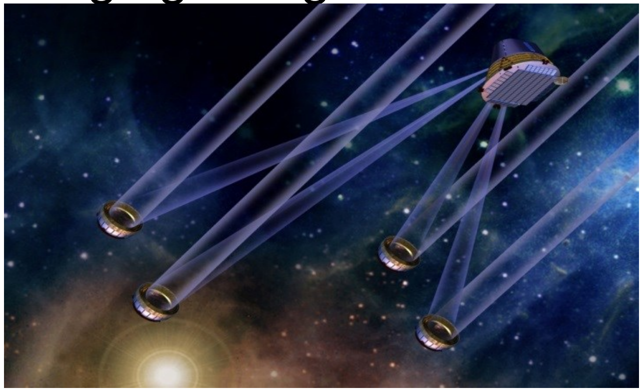
Kalman Gain

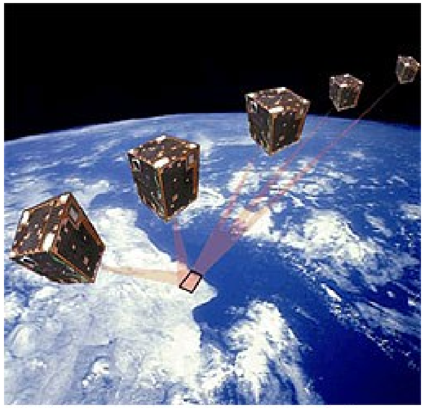
previous estimation

- Kalman filter balances noisy model-based prediction and noisy sensory measurements
- Changes in system dynamics indicate actuation failure
- Changes in measurement expectation indicate sensor failures

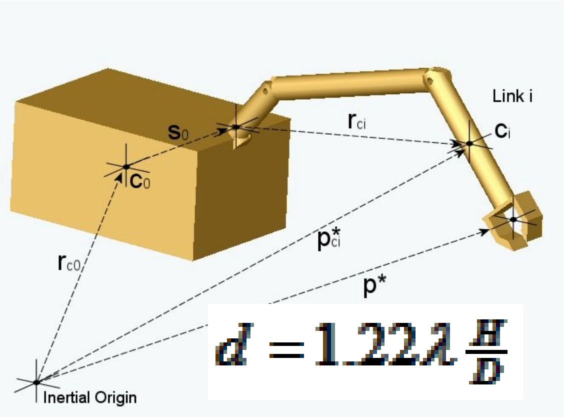
Earth Situational Awareness from Space

- We have been exploring a technique for extremely high resolution imaging using interferometry





Artist's concept of ESA's Proba-1 during an image capture run

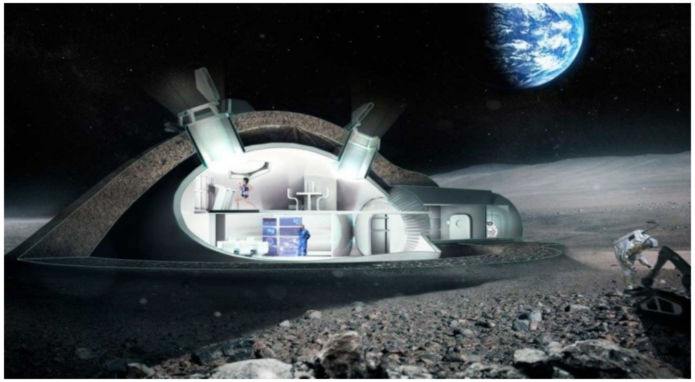


- 1m resolution imagery sufficient to identify ships, aircraft and armoured vehicles
- 0.5 m resolution imagery supply 50% of imagery requirements for the intelligence services
- D=1 km → d=0.5 mm!

srms_mov1.wmv

The Future is Here – Get Ready!

- Private sector is blazing a trail to the Moon and beyond



- This is happening
- Your citizens are expanding their domain
- Defence community needs to expand with them