DEFENCE & DÉFENSE

Content

1. 15BA – An overview
2. S&T Thread #1 – The Poly-Tracing project
3. S&T Thread #2 – Redundancy and diversity in C2ISs architectures
4. S&T Thread #3 – Software resilience, self-adaptation and self-healing
5. Concluding remarks

15BA – Problematic and needs

Current situation

C2ISs are (& will continue to be) made of *increasingly Cx technologies* (software & hardware)

- Multi-proc., multi-core, multi-level (virtualization), geographically distributed, etc.

C2ISs are often utilized in *hostile and constrained environments*

- Network (Internet), rough & constrained physical spaces (mil. vehicles), etc.

Limitations

It is now *impossible to build* fully certified C2ISs (*we must learn to live with software defects*)

C2ISs are *harder to debug*, optimize and adapt in function of new demanding situations

C2ISs are *subject to serious cyber threats* (*current security frameworks are not sufficient*)

It is often very hard to detect and eliminate unwanted internal software behaviours during Ops

- They result from cyber attacks, design faults, operator errors and other kinds of threat

➔ **New complementary technologies are needed during operations for:**

The deep monitoring, tracing and fine analysis of C2ISs

The protection of C2ISs against unwanted software behaviours

To improve the awareness of the health of utilized systems

C2IS: Command and Control Information System

15BA – S&T Threads & participants

Main thread: Poly-Tracing project

Deep monitoring, tracing, analysis of n-core n-level distributed information systems
(3-to-1 leveraging project)
(15BA05)

Fin. Contr./participants:

1. DRDC (1/3)
2. NSERC (1/3)
3. Ericsson (1/3)
4. Eventually Red Hat

Acad. participants:

Polytechnique Mtl (sci. lead)
Ottawa Un.
Concordia Un.
Laval Un.

Complementary threads

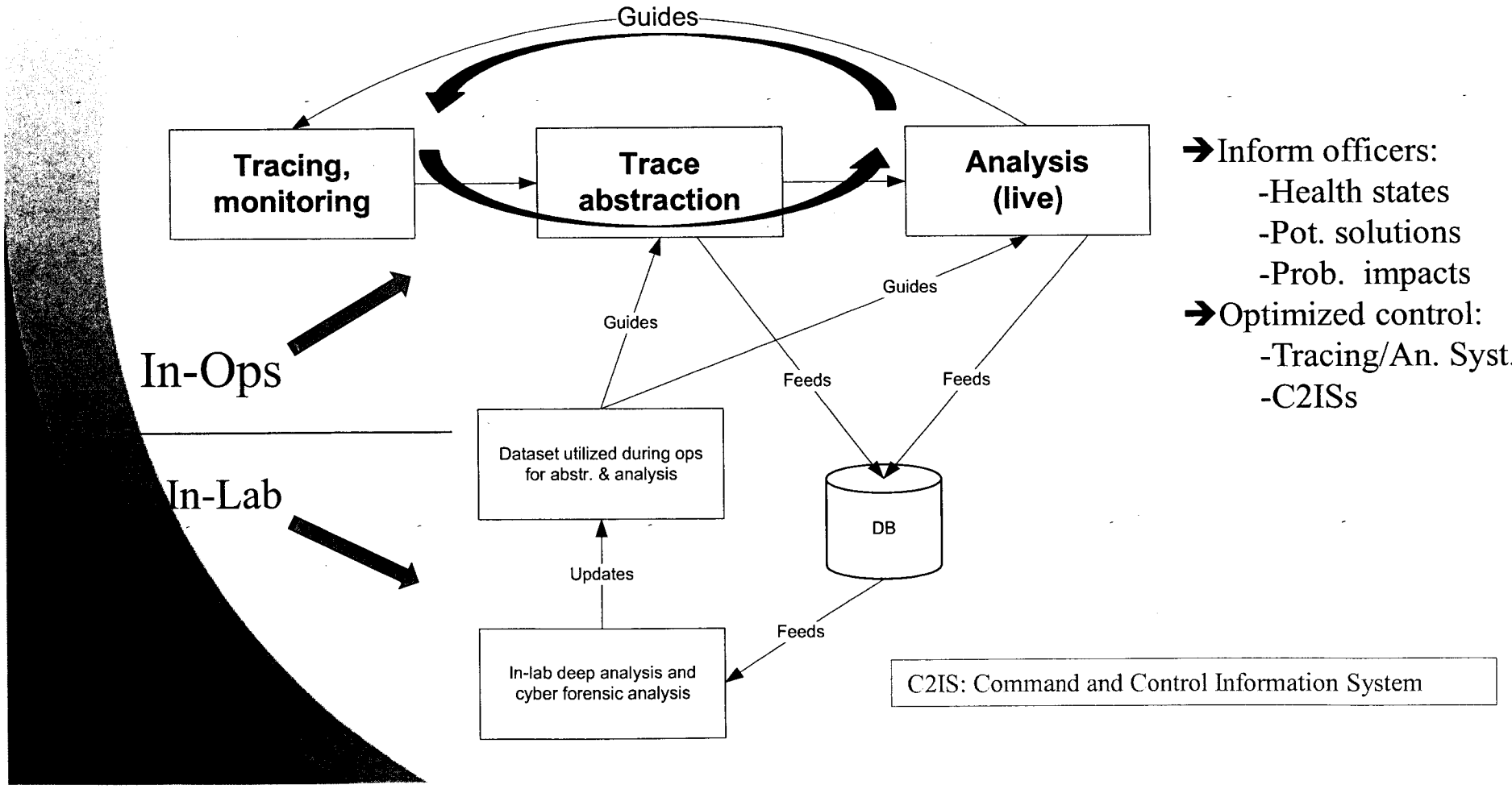
Software redundancy and diversity
(Post Doc)
(15BA02)

Software resilience, self-adaptation, self-healing
(DRDC contracts)
(15BA05)

S&T Thread #1: – The Poly-Tracing Project

The vision:

➔Online *Feedback-directed semi-assisted diagnostic/corrective system* for C2ISs



➔Inform officers:
- -Health states
- -Pot. solutions
- -Prob. impacts

➔Optimized control:
- -Tracing/An. Syst.
- -C2ISs

C2IS: Command and Control Information System

S&T Thread #1: – The Poly-Tracing Project

1. **Adaptive fault probing**

   Activate/de-activate tracing probes at runtime (focus & resolution)

2. **Multi-level, multi-core distributed traces synchronisation**

   Synchronize trace events originating from different CPUs (different clocks)

3. **Trace abstraction, analysis and correlation**

   Build an understanding of internal behaviours from trace events & deep analysis

4. **Automated fault identification**

   Mechanisms for the identification of unwanted software behaviours (u.s. & k.s.)

5. **System health monitoring and corrective measure activation**

   Continual evaluation of the system health and on the fly adapted protection

6. **Trace directed modelling**

   Comparison of u.s. trace events with UML models of utilized software

u.s.: user space
k.s.: kernel space

S&T Thread #2: Redundancy and diversity in C2ISs architectures

This thread aims to study:

- Possible concurrent utilizations of *redundancy and diversity* in architectures (software & hardware) to improve their protection against unwanted software behaviours

➔A 2-year Post Doc effort (started last July): Dr Gherbi

1. *State of the art* (December 2009)
2. *Framework:* concurrent use of redundancy and diversity

Integrate with other S&T threads

S&T Thread #3: Software resilience, self-adaptation and self-healing

This thread aims to initiate preliminary studies on mechanisms allowing:

- *Software resilience, self-adaptation and self-healing*
  - Human is considered as "part of systems"

➔ A 6-month DRDC contract (started last August): Dr Hamou-Lhadj (Concordia Un.)

State of the art (February, 2010)

➔ Following feasibility studies will then investigate more in depth selected technological options (that were identified in the SOTA)

Integrate with other S&T threads

Concluding remarks

Expectations:

New technologies to be developed and utilized:

- Online: *during operations* (improve awareness & protection)
- Offline: for *deep in-lab software analyses* (debugging, cyber forensics)

➔ A *Feedback-directed semi-assisted diagnostic/corrective system* for C2ISs
➔ A framework for the concurrent utilization of *redundancy & diversity*
➔ New mechanisms: *software resilience, self-adaptation and self-healing*

They will complement the current security framework
They should be Open Source Software (distributed/supported by Red Hat)

C2ISs: Command and Control Information Systems