Design Space Exploration for Secure Building Control

Martin Mansfield, Charles Morisset, Carl Gamble, **John C. Mace**
Ken Pierce and John Fitzgerald

School of Computing, Newcastle University

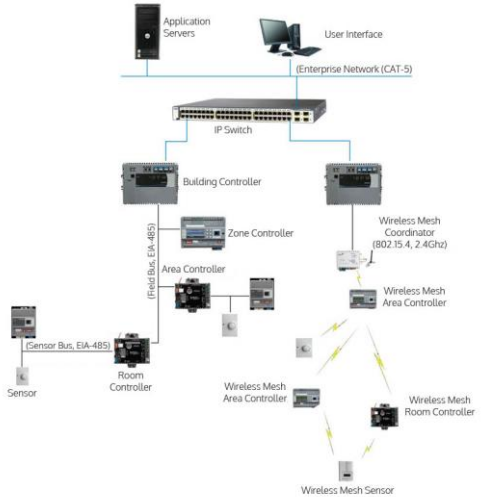
Building Control Systems

- Building services are largely controlled automatically
  - HVAC, lighting, water supplies, mobility, access control, security, etc.
- Automated building control offers many benefits
  - Improved operational efficiency, productivity, environmental sustainability, occupant health & safety, reduced energy consumption
- Building control systems integrate physical sensors & actuators, and software based cyber controllers
  - Building control systems are cyber-physical systems

Cyber Security Threats

- Building control system networks use Internet technologies (IP)
  - Open protocols for passing messages between devices (e.g. BACnet, KNX)
  - Many networks connected to Internet **[and Internet based cyber threats]**
  - More and more systems being integrated into single network

- Hostile reconnaissance
  - Control system properties, network layout, plan attack
- **Building control system attacks**
  - Turn systems on/off, **change sensor values**
- Network attacks
  - Re-route messages, break communications path
- Denial of Service (DoS) attacks
  - Flood network with messages, block sensors



Real-World Threat

Hackers Penetrate Google's Building Management System

The downside of smarter buildings: "If Google can fall victim, anyone can."

by Stephen Lacey
May 08, 2013

Smart Buildings, Dumb Security

March 9, 2016 | By Robert B. Razavi

Security 23

Building automation systems are so bad IBM hacked one for free

Tomorrow's Buildings: Help! My building has been hacked

By Jane Wakefield
Technology reporter

20 April 2016 | Technology

Austrian Hotel suffers Cyber Attack, Hackers are paid Ransom in Bitcoins

January 31, 2017 by Shipra Leave A Comment

12 APR 2013 NEWS

ICS-CERT reports two hacks on building management systems

Technology | CyberSecurity

Hackers leave Finnish residents cold after DDoS attack knocks out heating systems

The attack is believed to have lasted for a week, starting in late October and ending on 3 November.

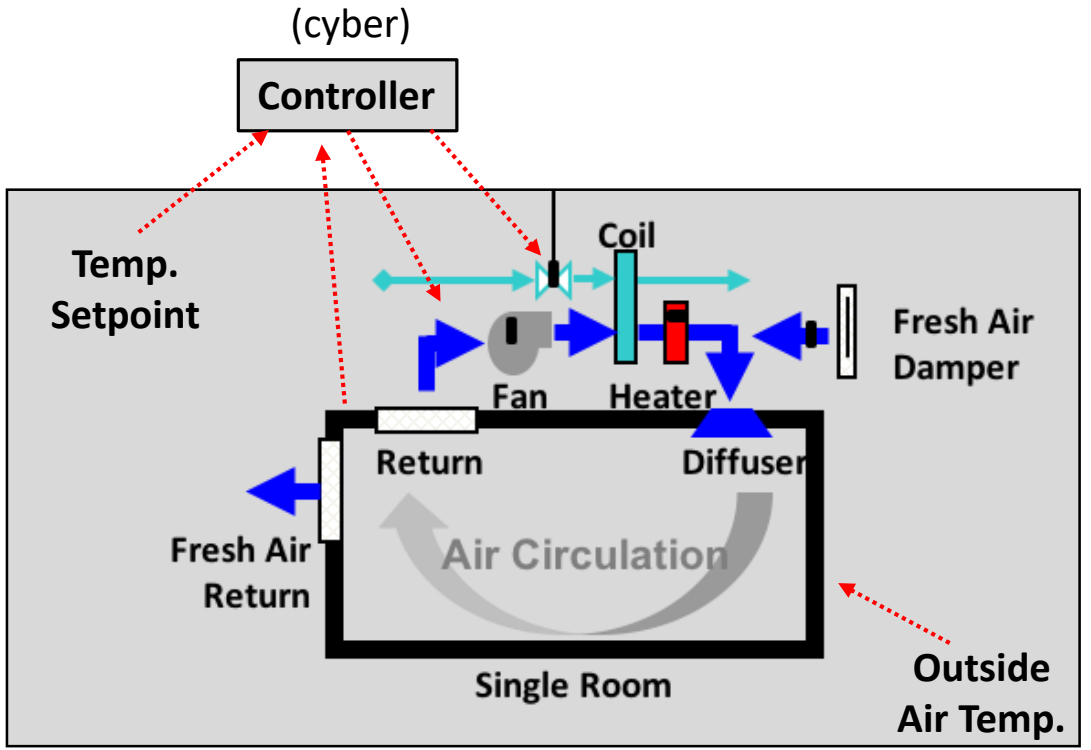
By India Ashok
November 9, 2016 10:51 GMT

Security Control Testing

- Testing on an operational building control is not practical
  - Launching different cyber attacks is risky and unethical
  - Hundreds of different systems in a single building
  - Systems have single purpose and are unadaptable
  - Expensive – both in terms of money and time
- Test beds are still expensive and may be incomplete
- Security should be considered at the building design stage
- Control system modelling and simulation is one solution

Example: Fan-Coil Unit

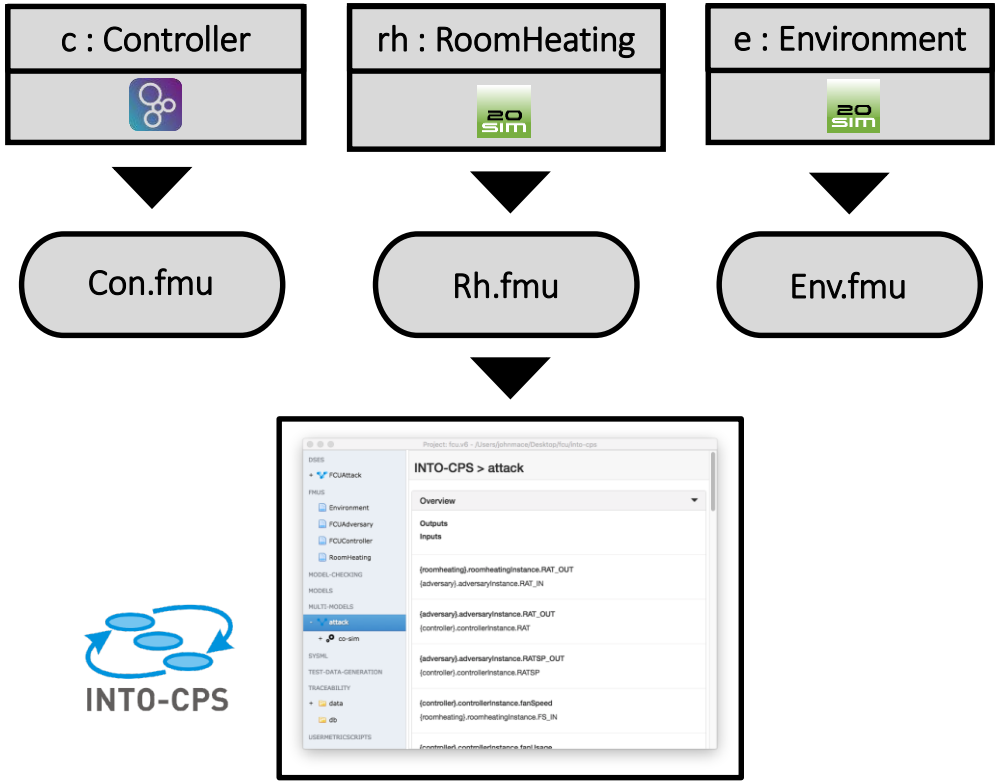
Fan Coil Units (FCUs) are heating systems commonly found in buildings

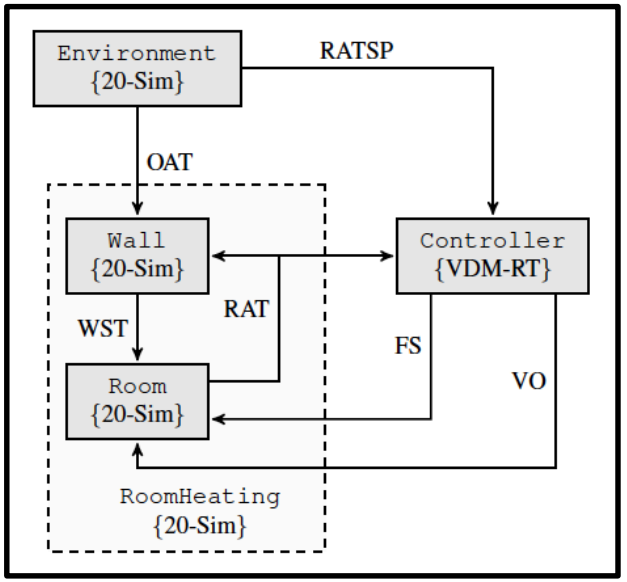


http://projects.au.dk/fileadmin/D3.5_Examples_Compendium_2.pdf

Multi-Modelling

(cyber – discrete events) (physical – continuous time)

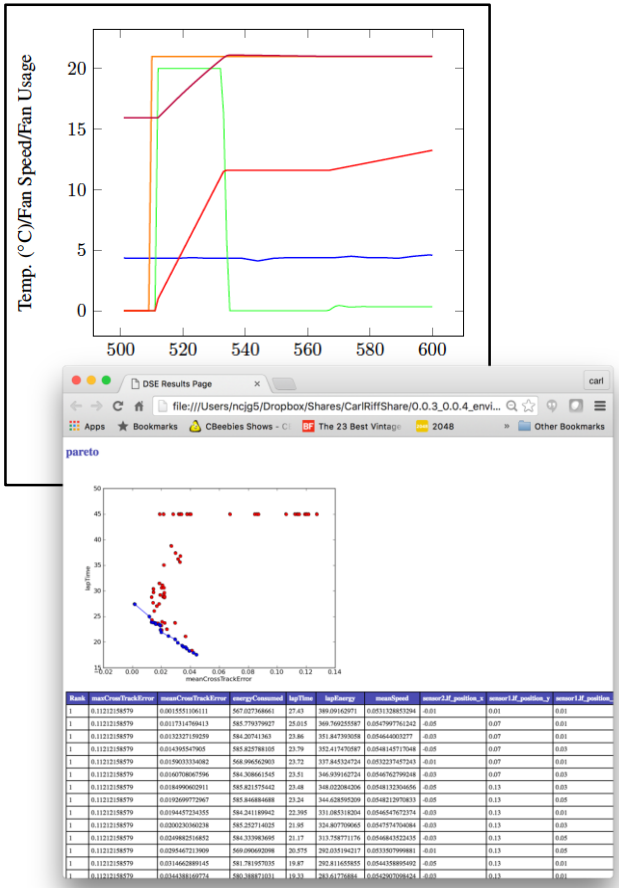




FMUs are connected in the INTO-CPS application to create a multi-model.

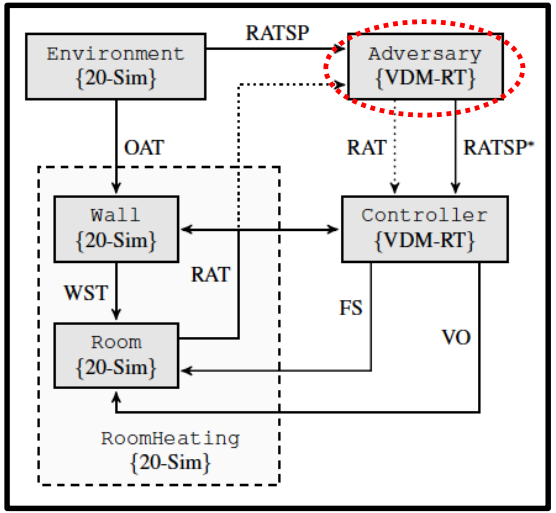
Design Space Exploration

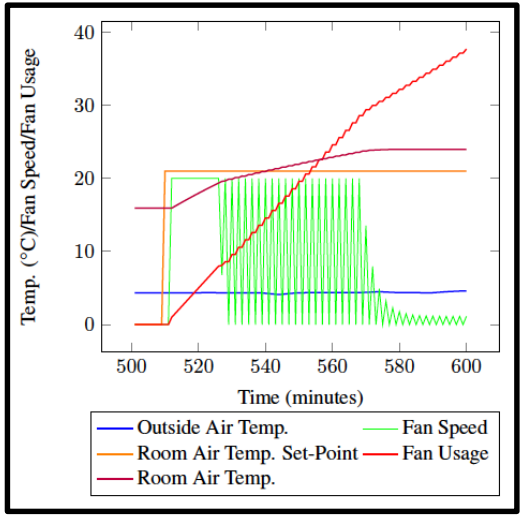
- Multi-model can be co-simulated to observe holistic system behaviour
- Range of values for each parameter defines set of all possible system designs (design space)
- INTO-CPS application automatically simulates all designs with DSE functionality
  - Groups and ranks designs according to criteria (best designs ranked 1)
  - Generates Pareto front of non-dominated designs



Modelling Adversaries

```
instance variables
ACSP : real := 0.0 -- Attack Current Set-Point

operations
public setAttack: () ==> ()
setAttack()==
(
  let SP = RATSP_IN.getReading() in
  if SP > 0.0 then
    if ACSP < SP then ACSP = SP + upperModificationLimit
    else ACSP = SP - lowerModificationLimit;
  )
  else ACSP = SP;


  RATSP_OUT.setState(ACSP)
);

thread periodic(attackFrequency)(setAttack);
```





VDM-RT Adversary block is created to read/modify Room Air Temperature Set-Point (RATSP).

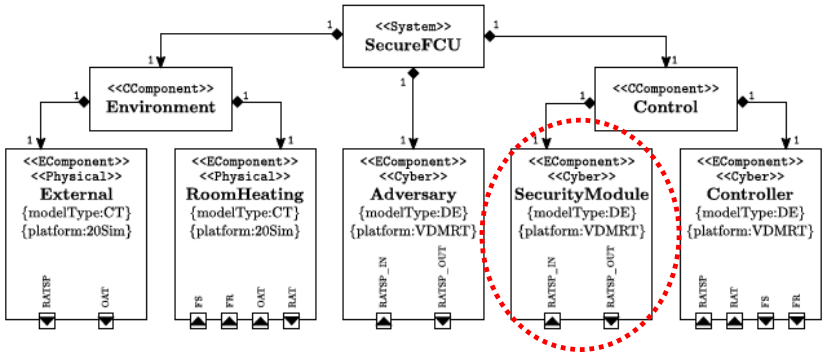
Adversary block is added to original multi-model

Adversary modifies RATSP by +/- 3°C causing rapid fan oscillation and high fan usage.

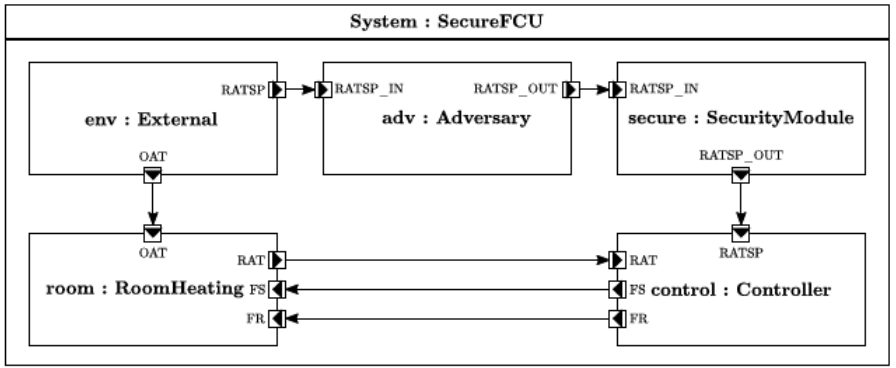
Security Monitor Specification

- Security monitor is implemented using Overture as a **SecurityModule** model

Architectural Structure Diagram



Connections Diagram



Security Monitor Specification (2)

- Security monitor contains an example attack countermeasure
  - Filters fluctuating RATSP* inputs using a moving average over a sampling period parameter
  - RATSP input fluctuations can be dampened but delay to temperature change introduced
  - Range of sampling period values defines **monitor strategies**

```
instance variables
samples : seq of real;

operations
private monitorInput:()==>()
monitorInput()==
(
  if len samples = sample_period then samples := tl samples;
  samples := samples ^ [RATSP_IN.getReading()];
  RATSP_OUT.setState(sum(samples) / len samples);
);

functions
sum: seq of real -> real
sum(s) == if len s = 1 then hd s else hd s + sum(tl s);

thread periodic(monitorFrequency)(monitorInput);
```

*RATSP = Room Air Temperature Set-Point

Security Monitor Optimisation

- Fan Coil Unit multi-model parameters

Security Monitor Strategies

RATSP Sampling period : 1 ~ 500 min
(1 sample taken per minute)

Controller Strategy

RATSP polling frequency : 1 sec (Fixed)

Adversary Strategies

RATSP modification frequency : 0.25 ~ 2.00 sec
Upper RATSP modification limit : 0 ~ +3.0^{O}C
Lower RATSP modification limit : 0 ~ -3.0^{O}C

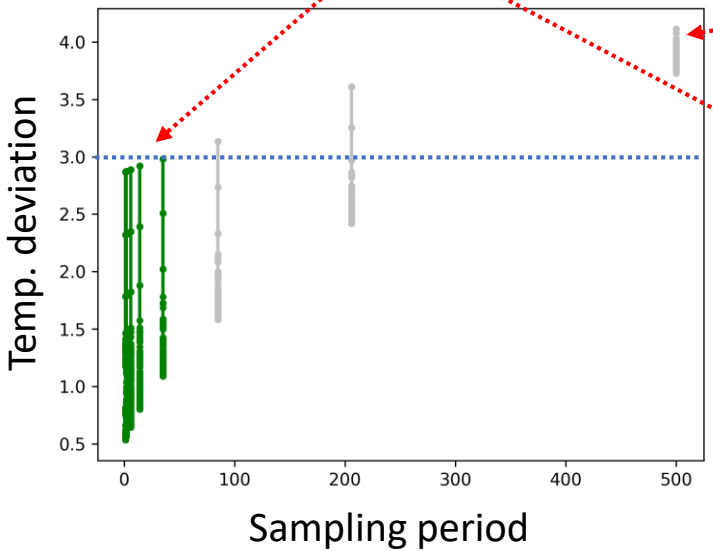
```
samplePeriod:[1,2,6,14,35,85,206,500]

modFrequency:[0.25,0.60,0.95,1.30,
1.65,2.00]

upperModLimit:[0,0.6,1.2,1.8,2.4,3]

lowerModLimit:[0,0.6,1.2,1.8,2.4,3],
```

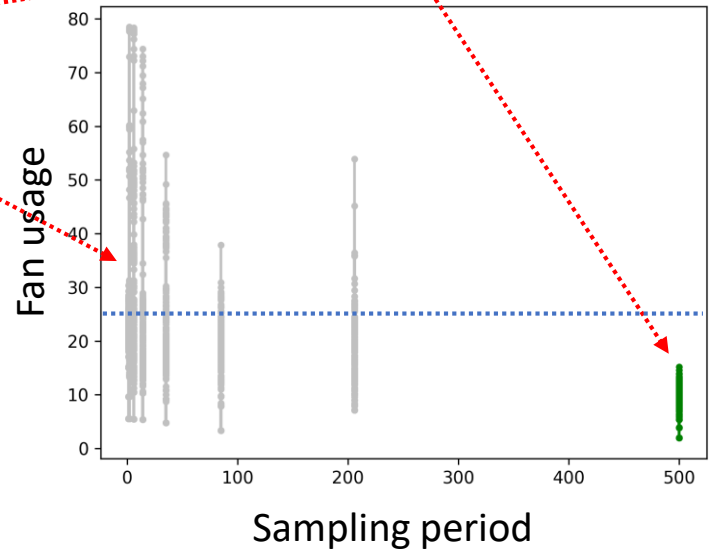
- Acceptable security properties
  - Fan usage limit : 25
  - Room Air Temp. deviation limit : 3^{o}C
- **What is best security monitor strategy?**

Security Monitor Optimisation (2)

Temp. deviation property **satisfied**
& Fan usage property **unsatisfied**

Fan usage property **satisfied** &
Temp. deviation property **unsatisfied**

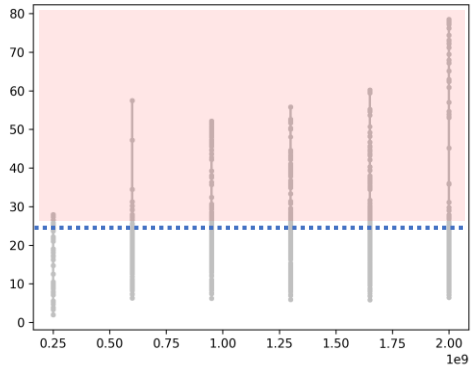
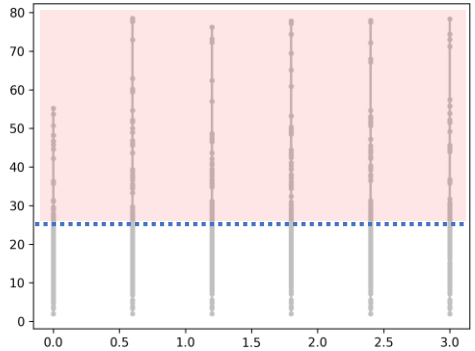
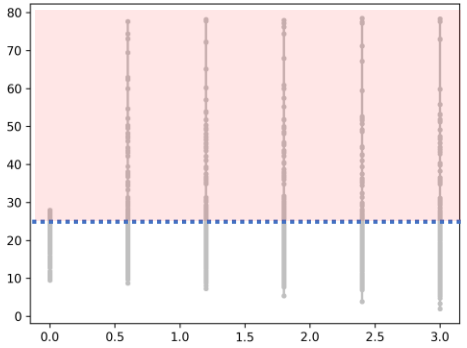
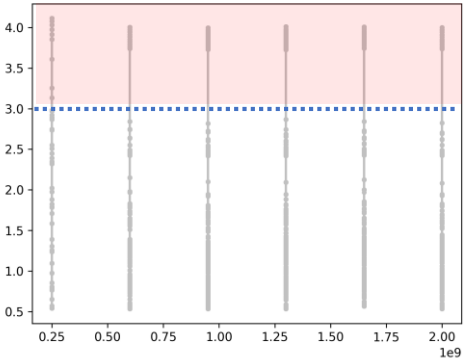
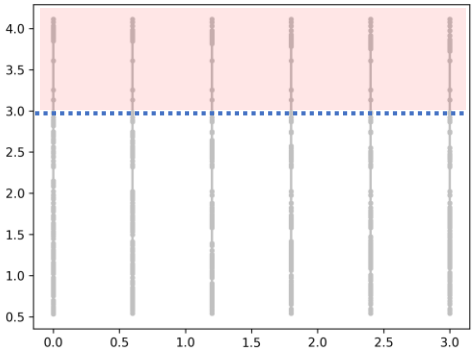
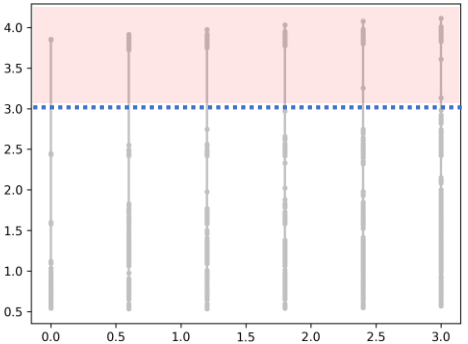




- No monitor strategy can ensure both security properties are satisfied
- Indicates a trade-off between security and usability

Attacker Strategies

Newcastle University

	RATSP modification frequency	RATSP upper modification limit	RATSP lower modification limit
Fan usage			
Room air temp. deviation			

Conclusion

- Illustrated how Overture can be used in security domain (of CPSs)
  - Design cyber countermeasures
  - Find best defensive strategies
  - Identify trade-offs

- Future work
  - Game theory - Dynamic monitor with an adaptive strategy
  - Explore using Overture to modelling different attackers, countermeasures, defence strategies, etc.
  - More complex attacks (e.g. multiple attackers synchronising attacks)

Contact: john.mace@ncl.ac.uk