Model-Implemented Hybrid Fault Injection for Simulink (Tool demonstration)

Mehrdad Moradi

Oct. 22, 2018

MSDL Research day

CoSys-Lab
Constrained Systems Lab
University of Antwerp

FLANDERS MAKE
MANUFACTURING INNOVATION NETWORK

University of Antwerp

Why?

What?

How?

Conclusion

Future direction

Cyber-Physical System

http://www.real-programmer.com/interesting_things/IEEE%20SpectrumThisCarRunsOnCode.pdf

Why?

What?

How?

Conclusion

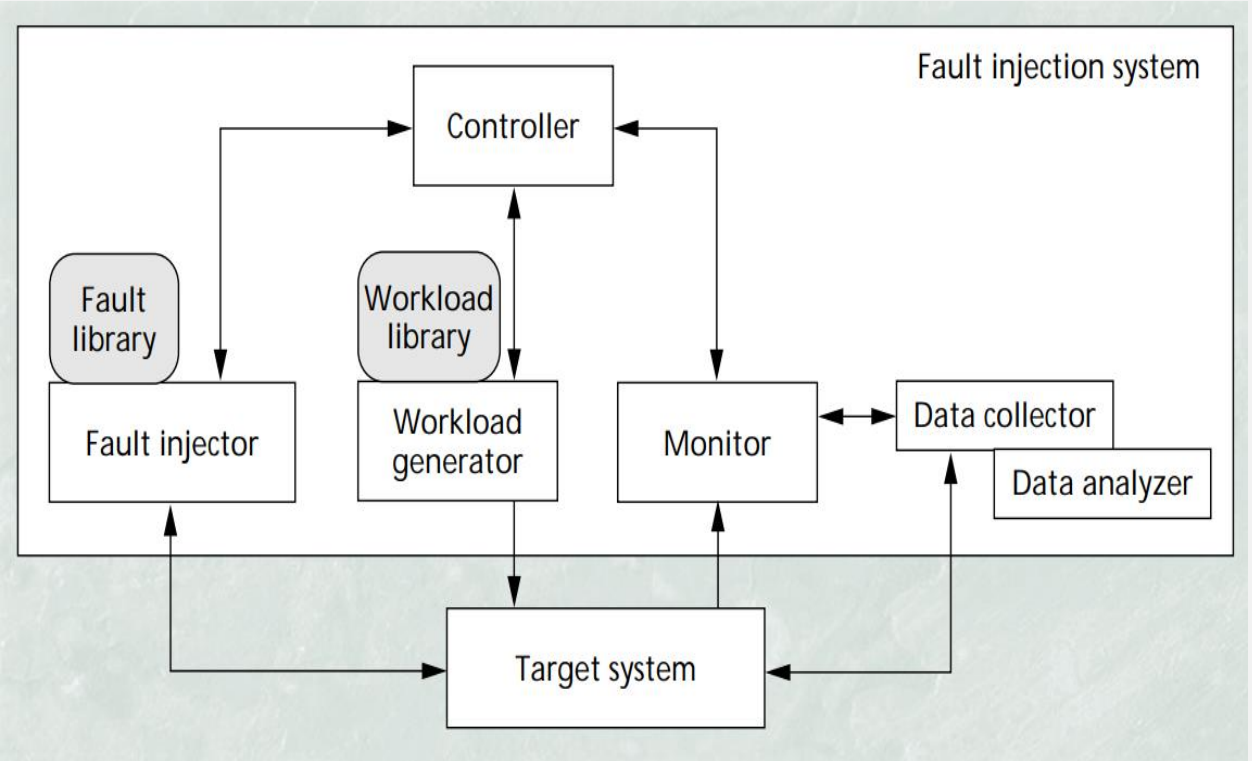
Future direction

Faults and Failures

	Computer systems (e.g., transaction processing [Gray 1990], electronic switching [Cramp et al. 1992])		Larger, controlled systems (e.g., commercial airplanes [Ruegger 1990], telephone network [Kuhn 1997])	
	Rank	Proportion of failures	Rank	Proportion of failures
Physical internal faults	3	~ 10 %	2	15 - 20 %
Physical external faults	3	~ 10 %	2	15 - 20 %
Human-made interaction faults	2	~ 20 %	1	40 - -50 %
Design faults	1	~ 60 %	2	15 - 20 %

Deswarte, Y., Creese, S., Deswarte, Y., Kursawe, K., Laprie, J.C., Powell, D., Randell, B., Riordan, J., Ryan, P., Simmonds, W., Stroud, R., Verissimo, P., Waidner, M., Wespi, A.: Conceptual Model and Architecture of MAFTIA Conceptual Model and Architecture of MAFTIA Departamento de Inform ´ Faculdade de Ciˆ. (2003).

Fault Injection

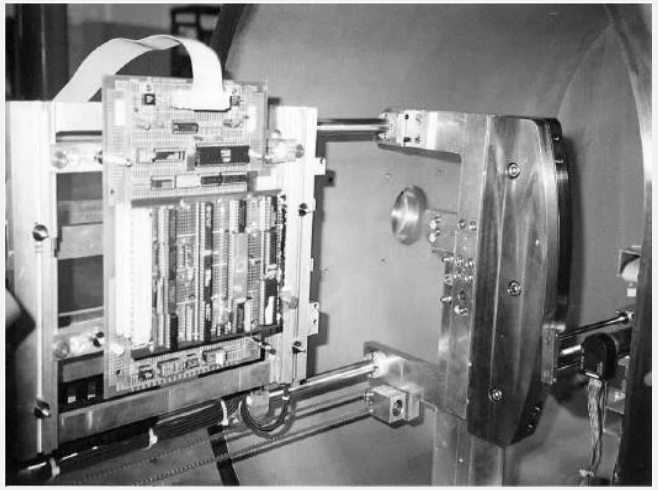


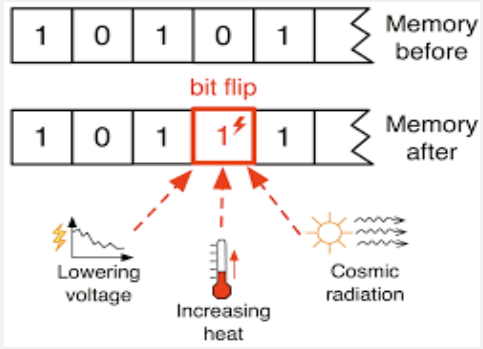
FARM model:

1. the set of **F**aults to be injected,
2. the set of **A**ctivations exercised during the experiment,
3. the **R**eadouts to define observers of system behavior,
4. the **M**easures dependability properties.

- Fault Injection Techniques and Tools
- J. Arlat, M. Aguera, L. Amat, Y. Crouzet, J.C. Fabre, J.-C. Laprie, E. Martins, D. Powell, Fault Injection for Dependability Validation: A Methodology and some Applications, IEEE Transactions on Software Engineering, Vol. 16, No. 2, February 1990, pp. 166–182

Fault Injection's Types





Mutated target component

```
if(a && b)
{
  c=1;
}
```

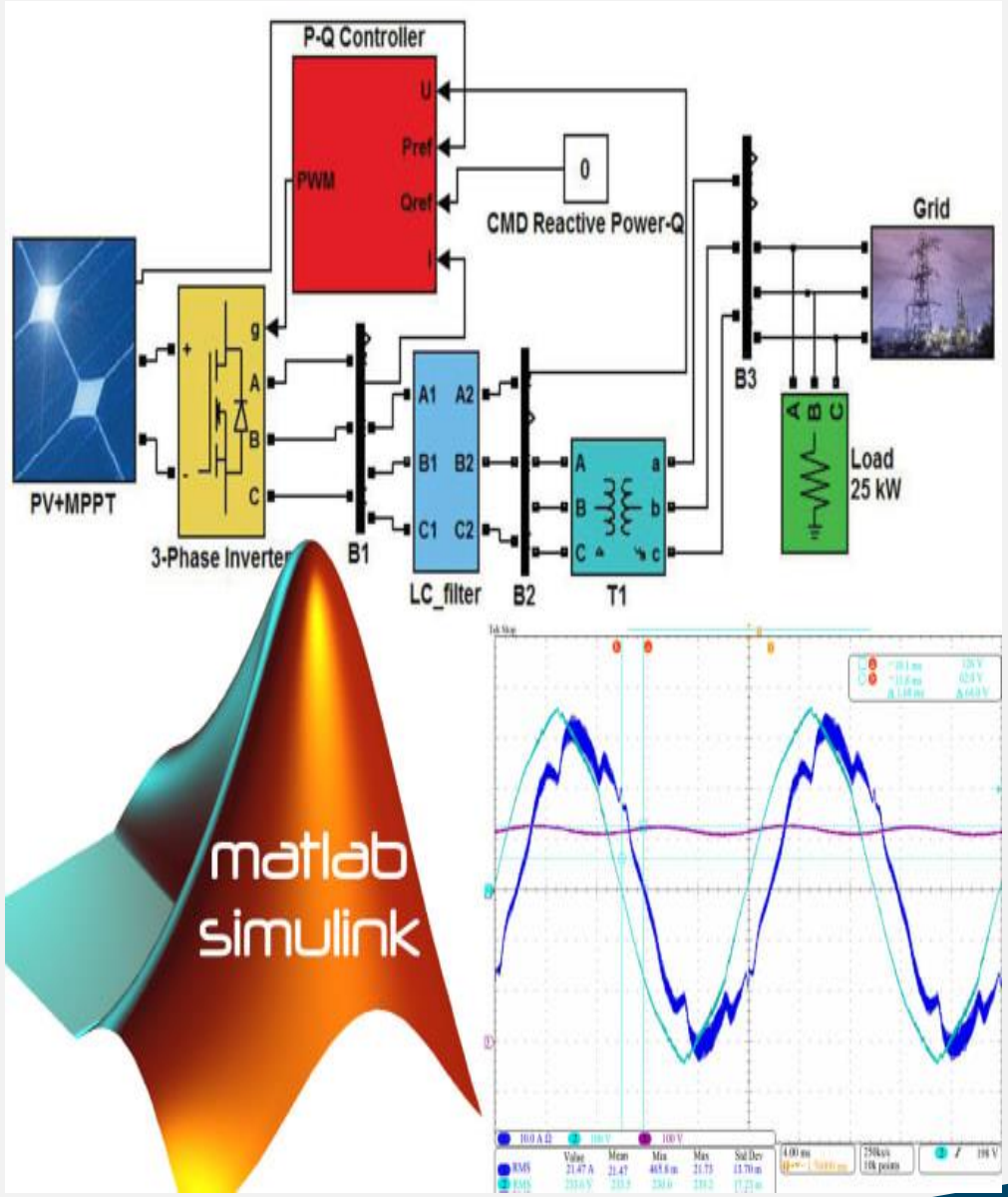
```
if(a && b)
{
  c=1;
}
```

```
if(a && b)
{
  c=1;
}
```

```
if(a && b)
{
  c=2;
}
```

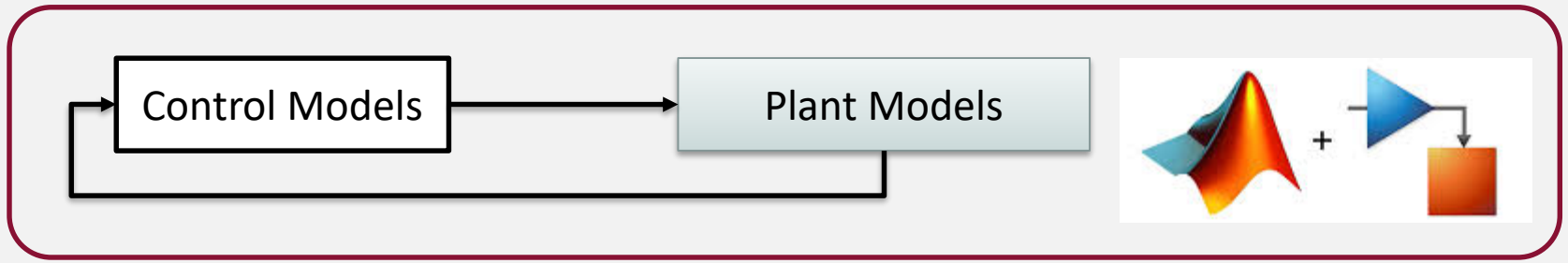
...

http://wpage.unina.it/roberto.natella/tools.html

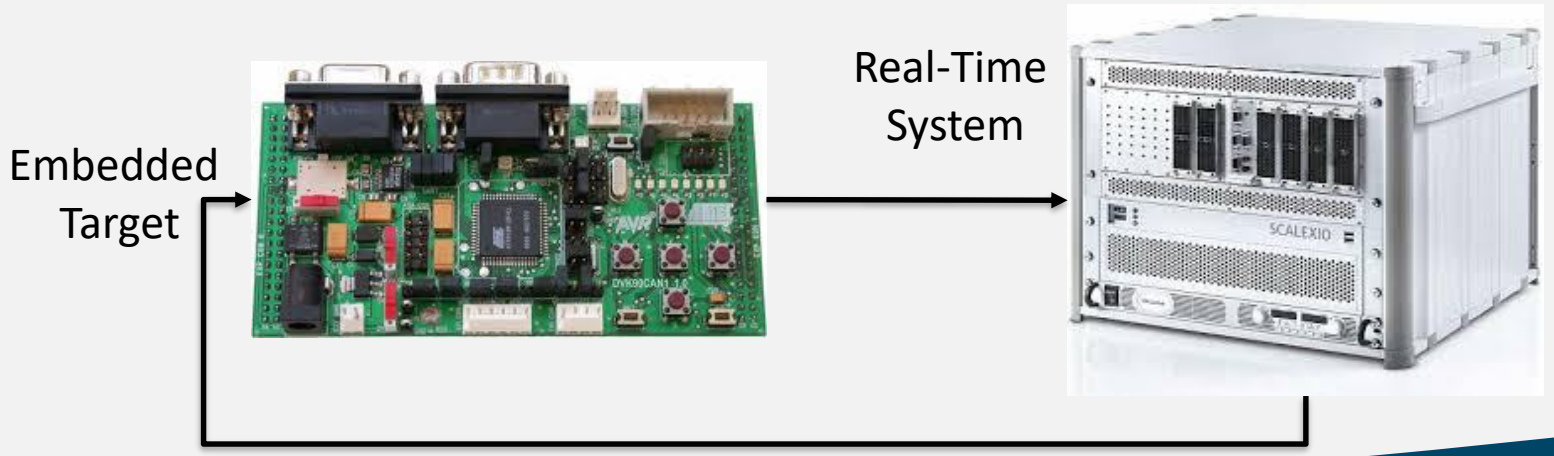


Framework

Generative techniques: **Model-Implemented Hybrid Fault Injection** by explicit modelling of **FARM** in Simulink to setup the experiments both for **Model-in-the-Loop (MiL)** and **Hardware-in-the-Loop (HiL)**



MiL

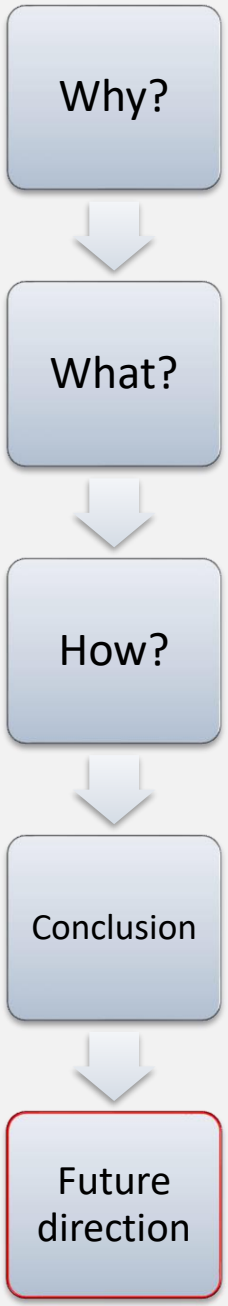


HiL

Why?
What?
How?
Conclusion
Future direction

Conclusion

- The framework automated the FI process
  - MiL to simulation-based fault injection
  - HiL to execution-based fault injection
  - Cover wide variety of fault type
  - Flexible fault injection scenario



Future direction

- Complete FARM model
  - Temporal Logic
- Efficient fault injection
  - Increase fault coverage and speed
- Complex fault injection
- INES and aSET projects

Thank you for your attention