SECURE-IC
THE SECURITY SCIENCE COMPANY

QUANTIFYING THE SPEED-UP OFFERED BY GENETIC ALGORITHMS DURING FAULT INJECTION CARTOGRAPHIES

Idris Raïs-Ali[1], Antoine Bouvet[1], Sylvain Guilley[1,2]

September 16, 2022

[1] Secure-IC S.A.S., Cesson-Sévigné, France

[2] Télécom ParisTech, Palaiseau, France

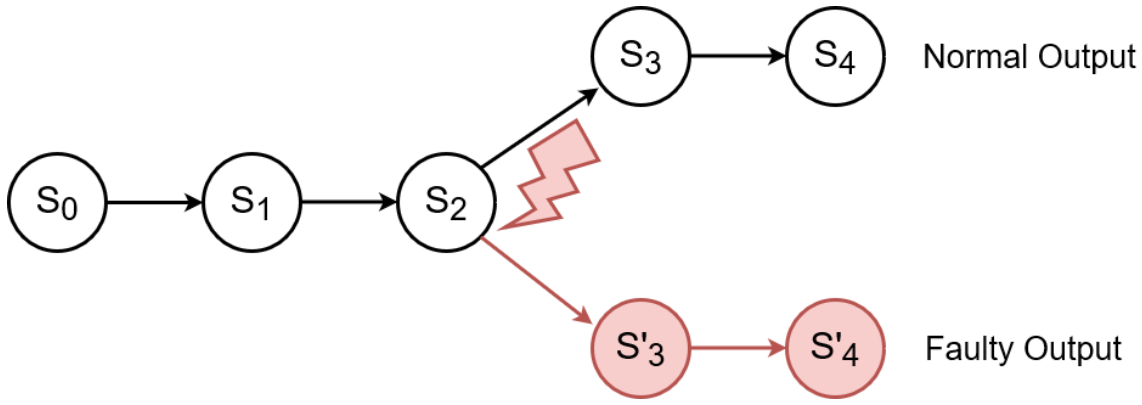
QUANTIFYING THE SPEED-UP OFFERED BY GAS DURING FAULT INJECTION CARTOGRAPHIES

1. Fault Injection Analyses & Points of Interest
2. EMFI experiments
3. Spatial cartographies and Genetic Algorithms (GAs)
4. Quantifying a cartography method effectiveness
5. Conclusions

QUANTIFYING THE SPEED-UP OFFERED BY GAS DURING FAULT INJECTION CARTOGRAPHIES

1. Fault Injection Analyses & Points of Interest
2. EMFI experiments
3. Spatial cartographies and Genetic Algorithms (GAs)
4. Quantifying a cartography method effectiveness
5. Conclusions

FIAS & POINTS OF INTEREST

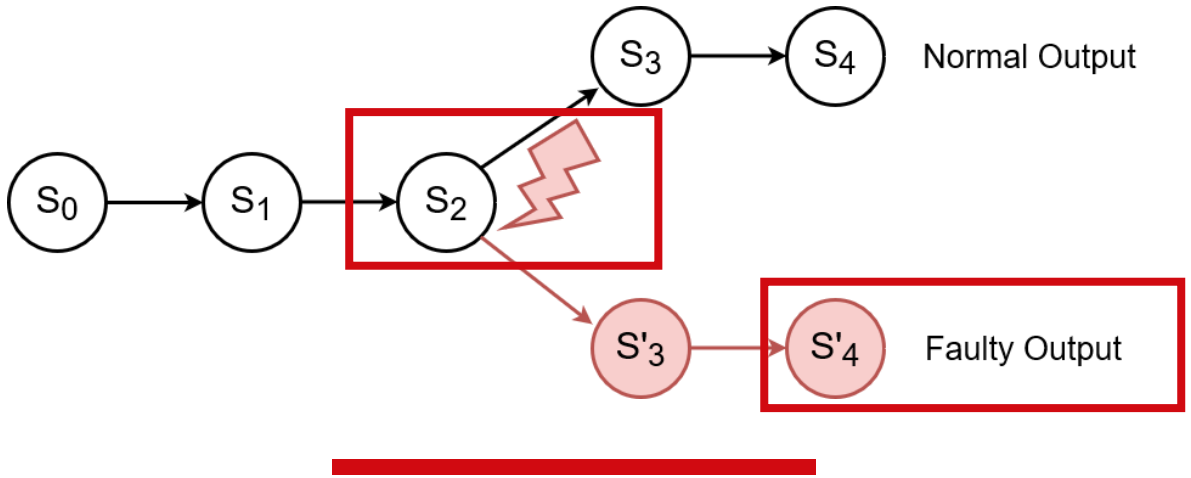


Expected intern states S sequence,
disturbed by an external perturbation

Example of perturbation techniques:

- Electro-Magnetic Fault Injection (EMFI)
- Laser Fault Injection
- Power / Clock Glitch
- Body Biasing Injection (BBI)
- Temperature Variation

FIAS & POINTS OF INTEREST

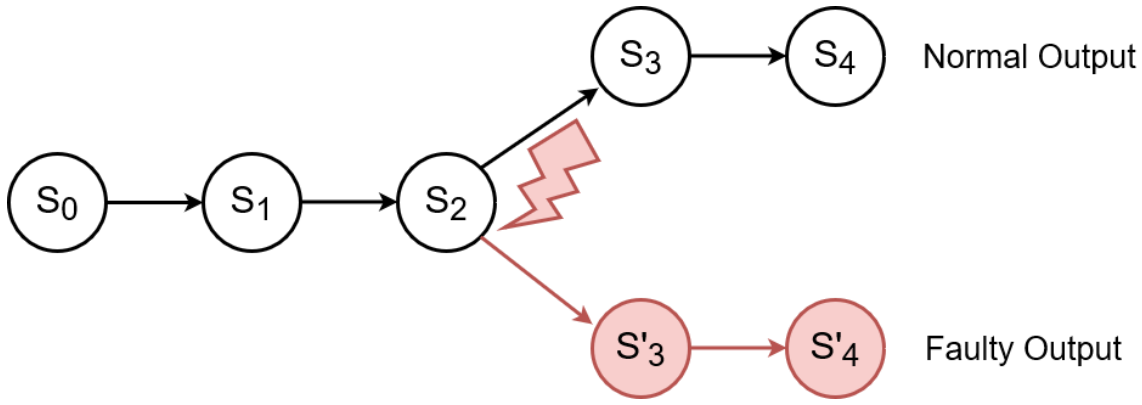


Expected intern states S sequence,
disturbed by an external perturbation

Example of perturbation techniques:

- Electro-Magnetic Fault Injection (EMFI)
- Laser Fault Injection
- Power / Clock Glitch
- Body Biasing Injection (BBI)
- Temperature Variation

FIAS & POINTS OF INTEREST



Expected intern states S sequence,
disturbed by an external perturbation

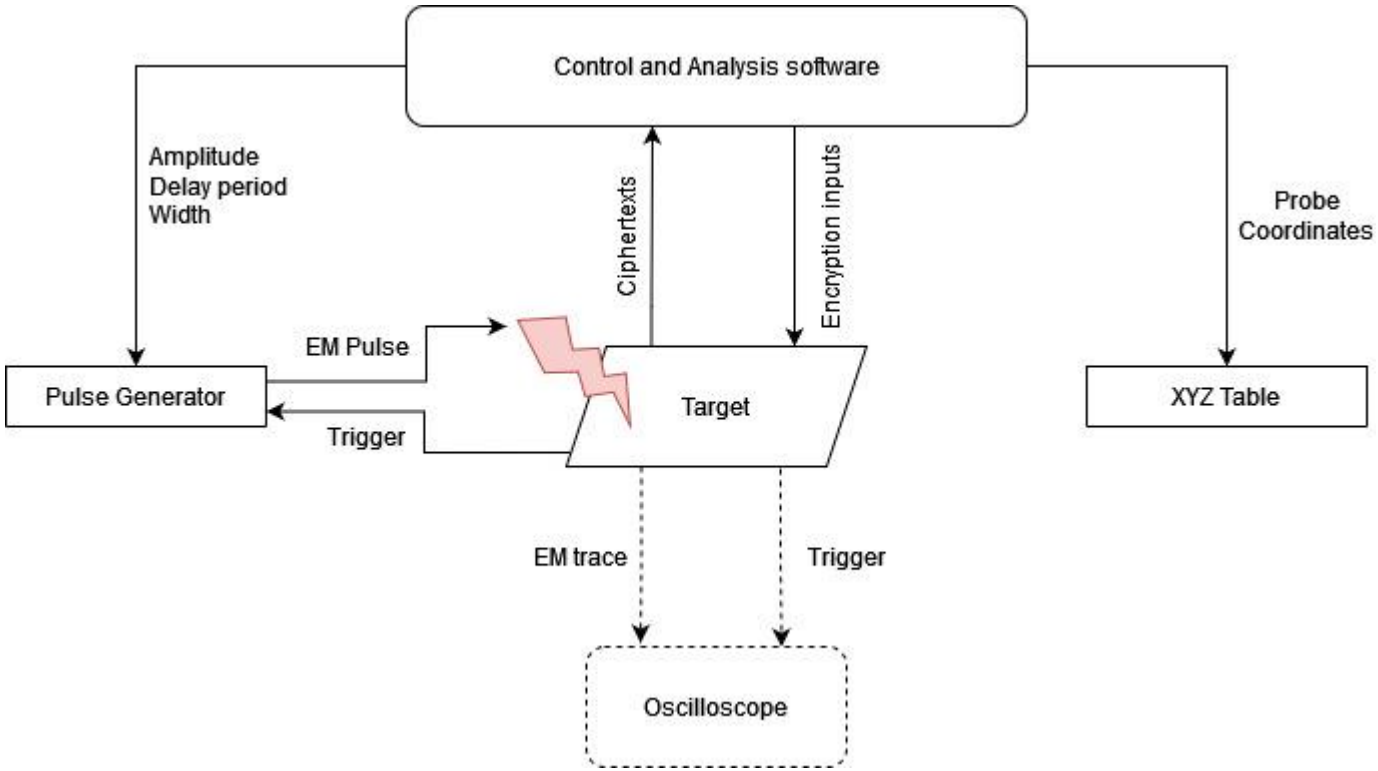
Example of perturbation techniques:

- Electro-Magnetic Fault Injection (EMFI)
- Laser Fault Injection
- Power / Clock Glitch
- Body Biasing Injection (BBI)
- Temperature Variation

QUANTIFYING THE SPEED-UP OFFERED BY GAS DURING FAULT INJECTION CARTOGRAPHIES

1. Fault Injection Analyses & Points of Interest
2. EMFI experiments
3. Spatial cartographies and Genetic Algorithms (GAs)
4. Quantifying a cartography method effectiveness
5. Conclusions

EMFI EXPERIMENTAL SETUP

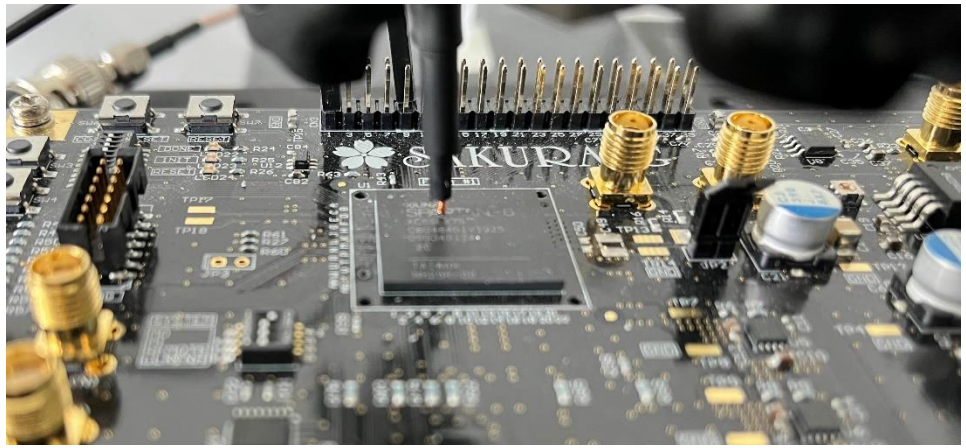


Electromagnetic Fault Injection setup

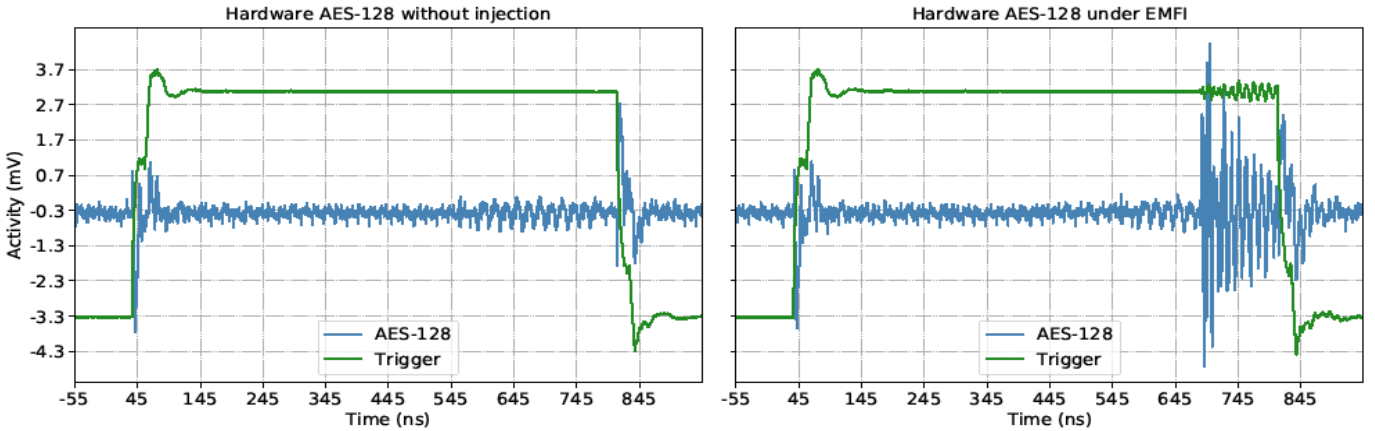
Parameters:

- Pulse amplitude
- Pulse width
- Delay period
- Probe position over the chip (spatial coordinates: X, Y, Z)

EMFI EXPERIMENTAL SETUP

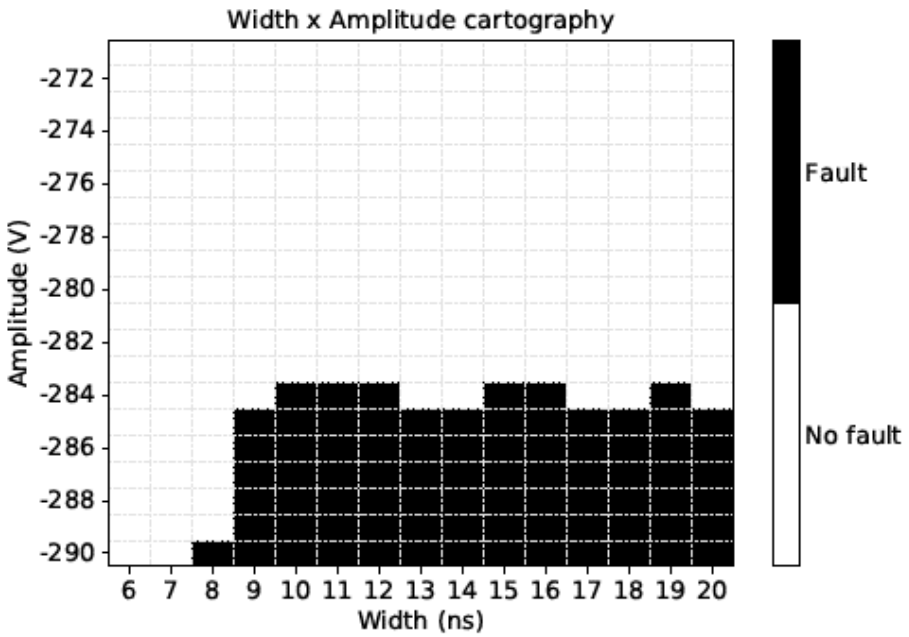


Picture of the target
with injection probe over the FPGA

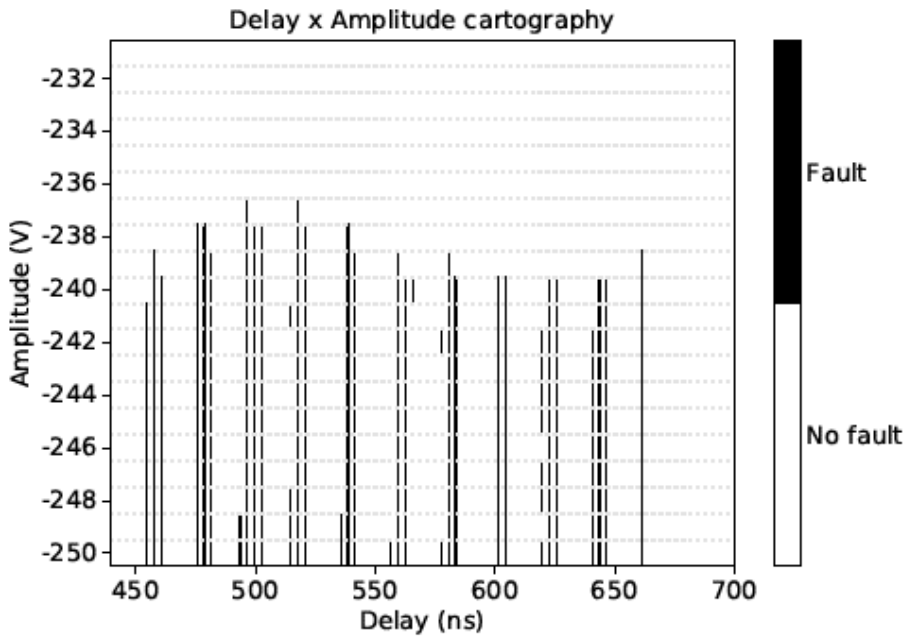


EM activity of the hardware AES-128,
without (left) and with (right) EMFI over the chip

EM PARAMETERS CARTOGRAPHIES



Width x Amplitude cartography

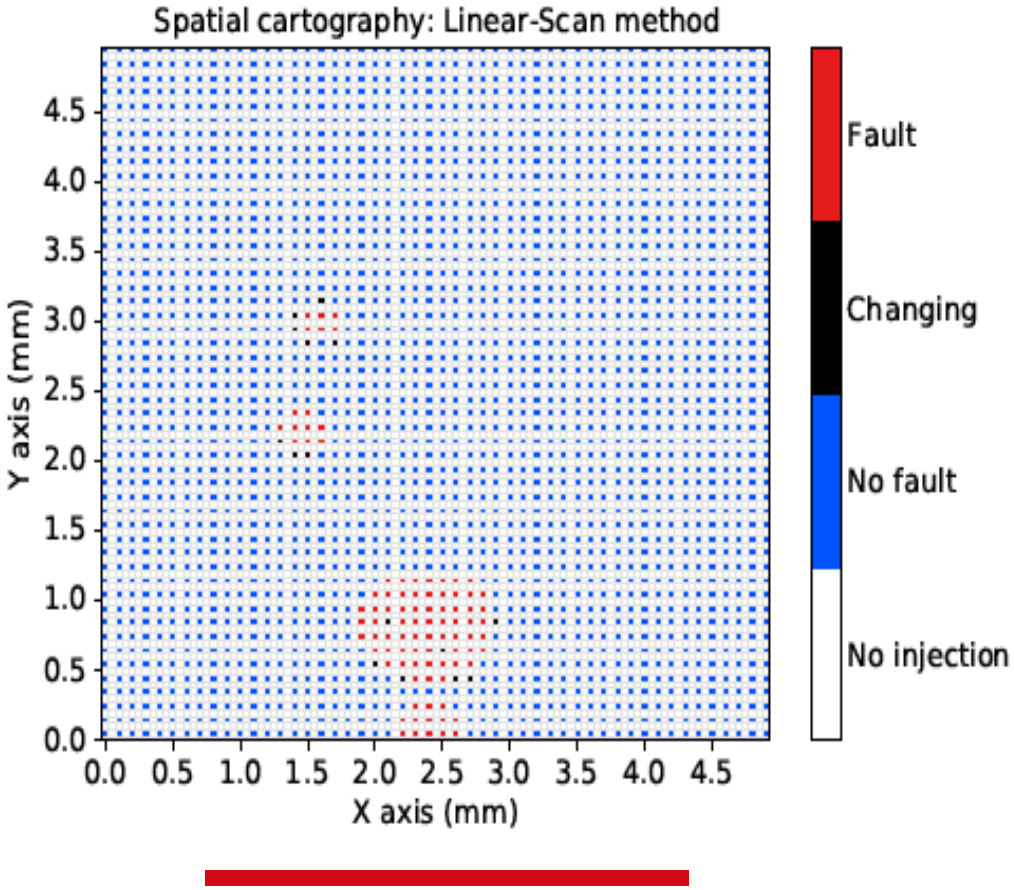


Delay x Amplitude cartography

QUANTIFYING THE SPEED-UP OFFERED BY GAS DURING FAULT INJECTION CARTOGRAPHIES

1. Fault Injection Analyses & Points of Interest
2. EMFI experiments
3. Spatial cartographies and Genetic Algorithms (GAs)
4. Quantifying a cartography method effectiveness
5. Conclusions

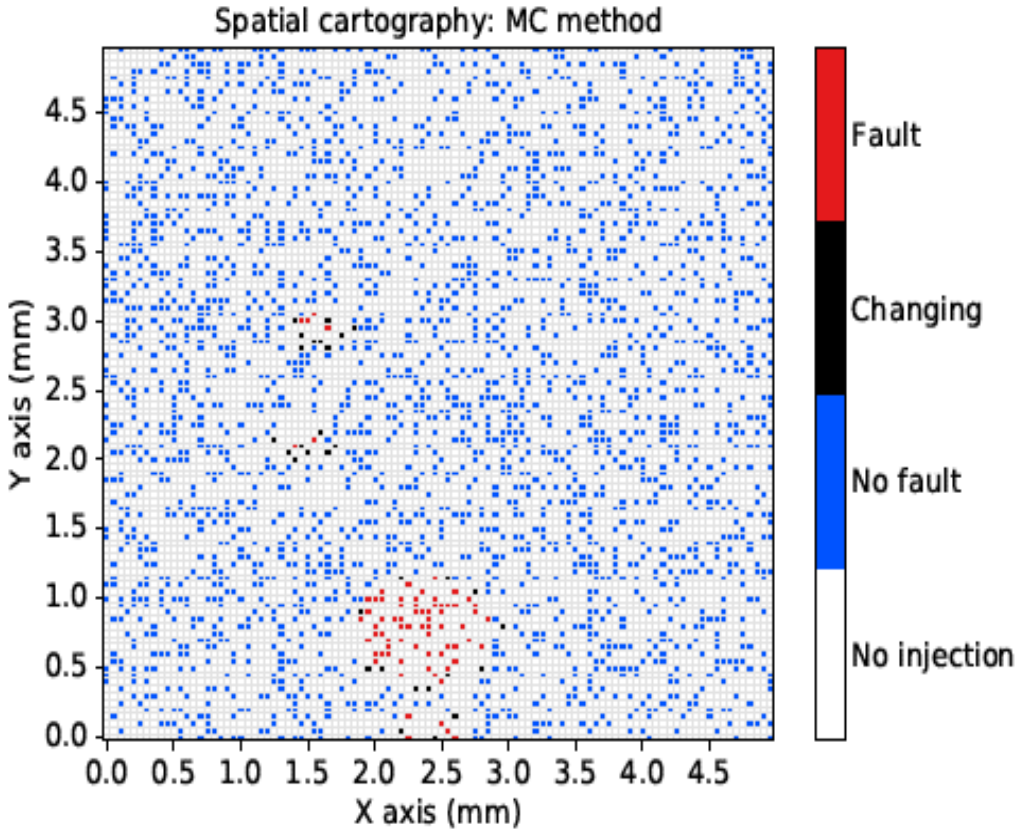
SPATIAL CARTOGRAPHIES: INTRODUCTION



Spatial cartography with Linear-Scan method

- Two-dimensional cartographies
- Injection probe moves above the targeted FPGA
- Linear-Scan: fixed step

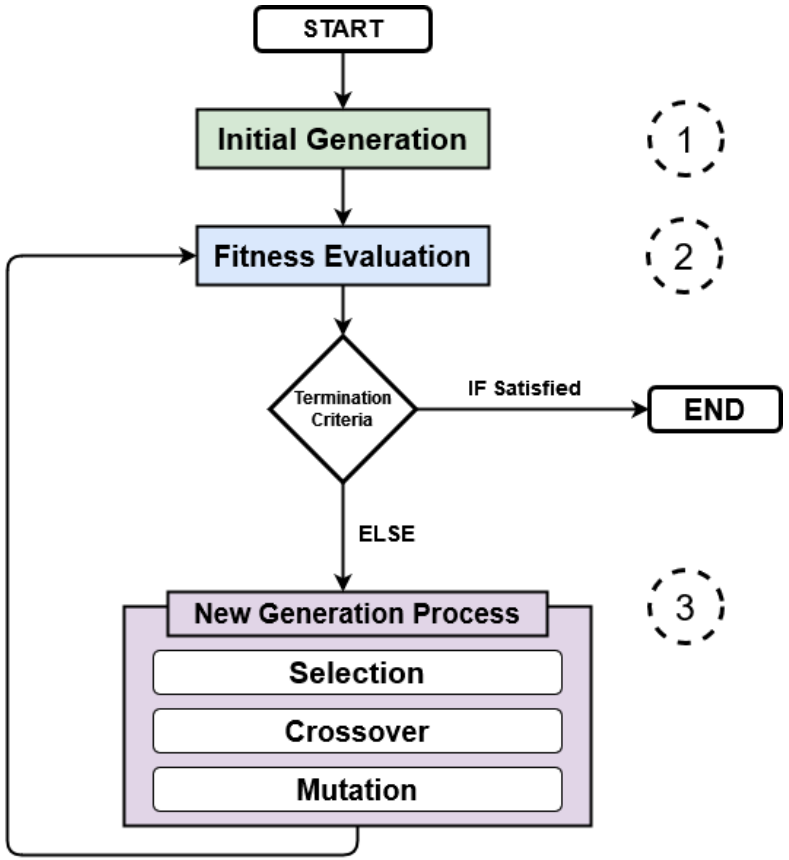
SPATIAL CARTOGRAPHIES: MONTE-CARLO



Random selection
(Monte-Carlo)

- Monte-Carlo: randomly selected points
- Allow to make an estimation of the proportion / number of PoIs above the scanned surface.

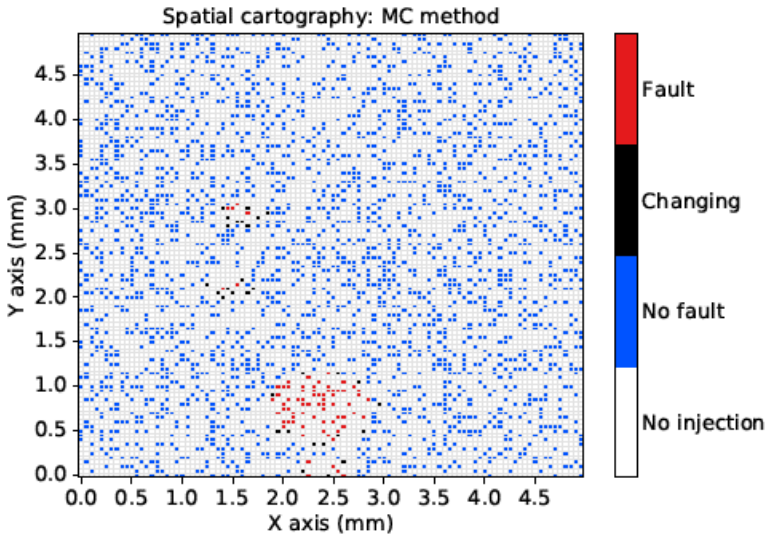
SPATIAL CARTOGRAPHIES: GENETIC ALGORITHMS



Genetic Algorithms scheme

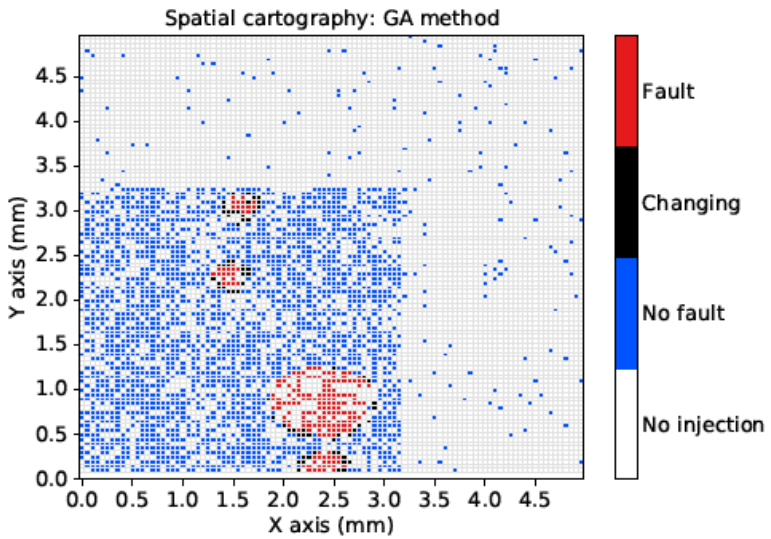
- Analyze injection results though the process
- Main steps:
  1) Initial Generation
  2) Fitness Evaluation
  3) New Generation Process
- Pros:
  - Leave areas without interest
  - Focus on Areas of Interest (AoIs)

SPATIAL CARTOGRAPHY BASED ON RANDOM PROCESS



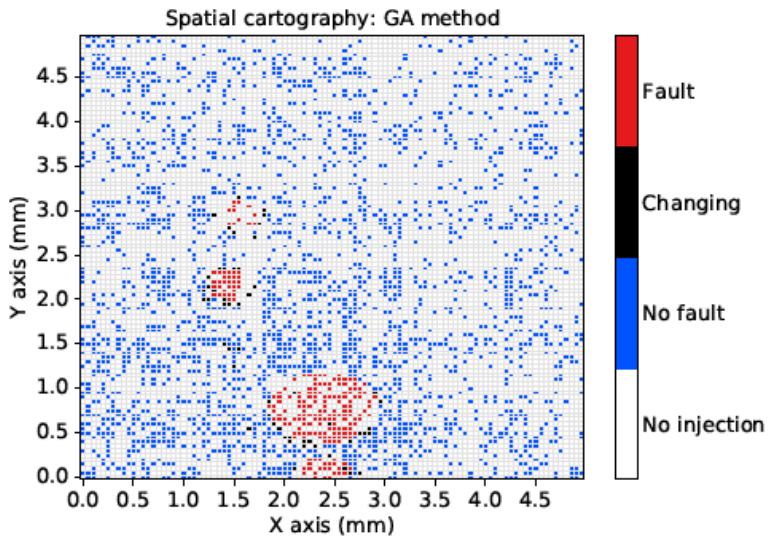
Random selection

(Monte-Carlo)



Genetic Algorithm

(GA 100%)

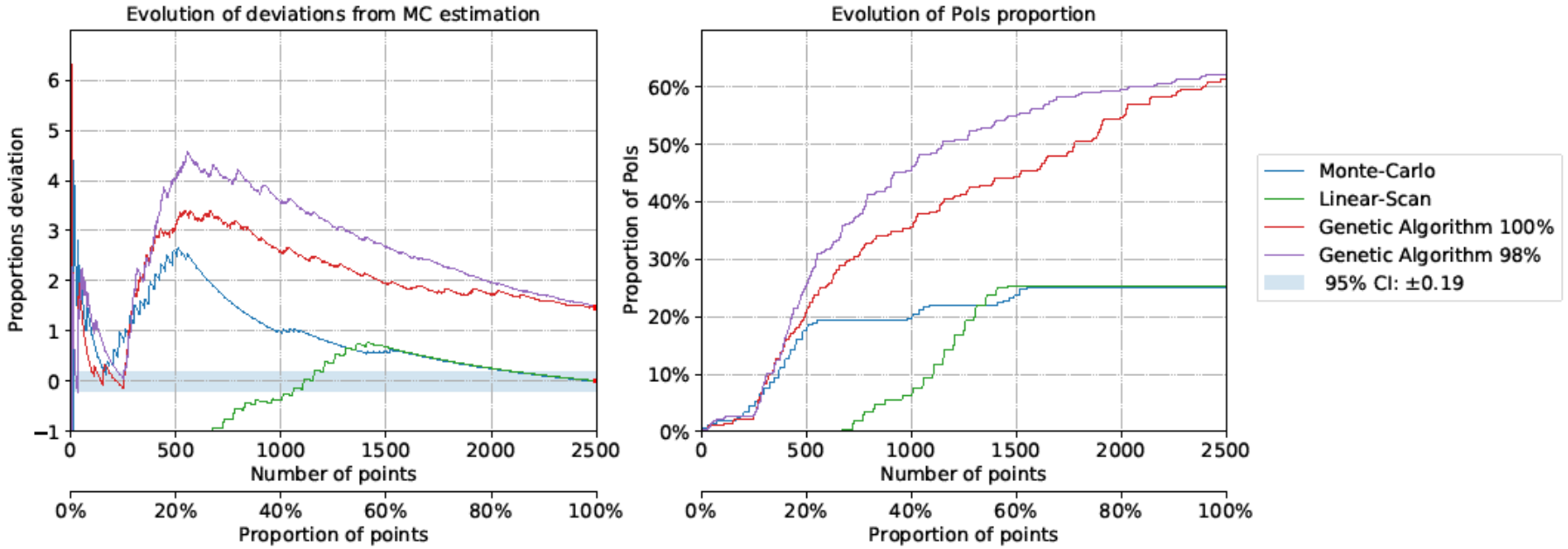


Genetic Algorithm mixed with random selection at 2%
(GA 98%)

QUANTIFYING THE SPEED-UP OFFERED BY GAS DURING FAULT INJECTION CARTOGRAPHIES

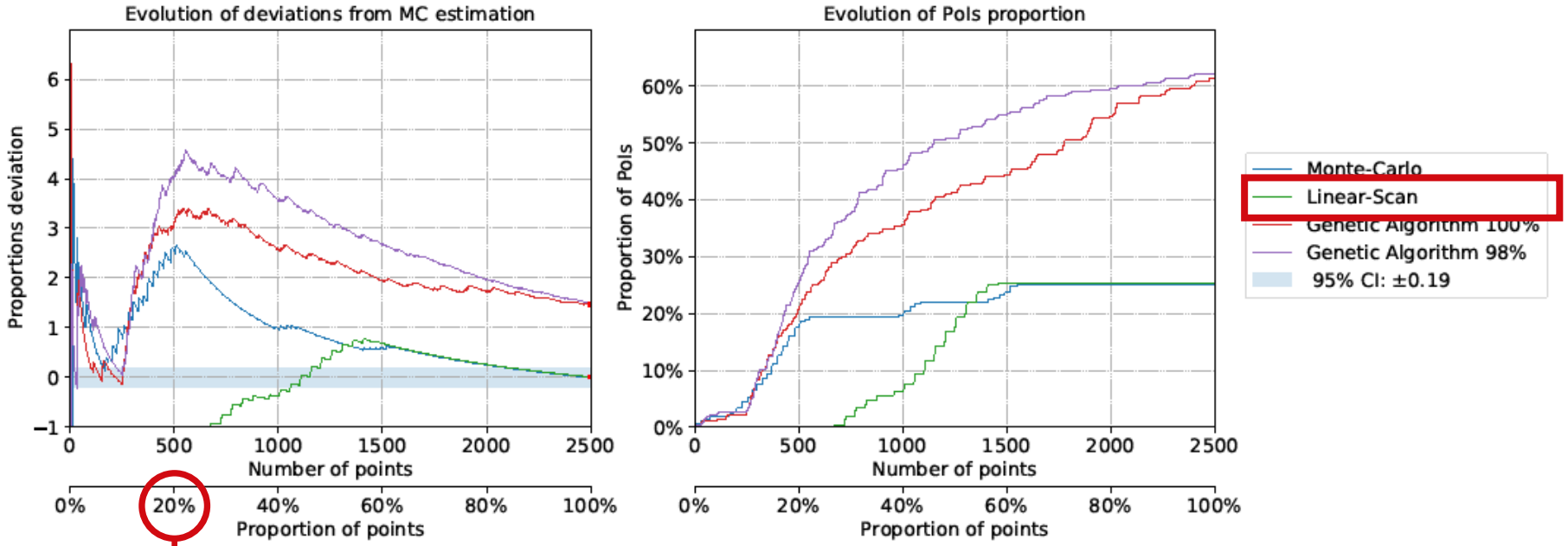
1. Fault Injection Analyses & Points of Interest
2. EMFI experiments
3. Spatial cartographies and Genetic Algorithms (GAs)
4. Quantifying a cartography method effectiveness
5. Conclusions

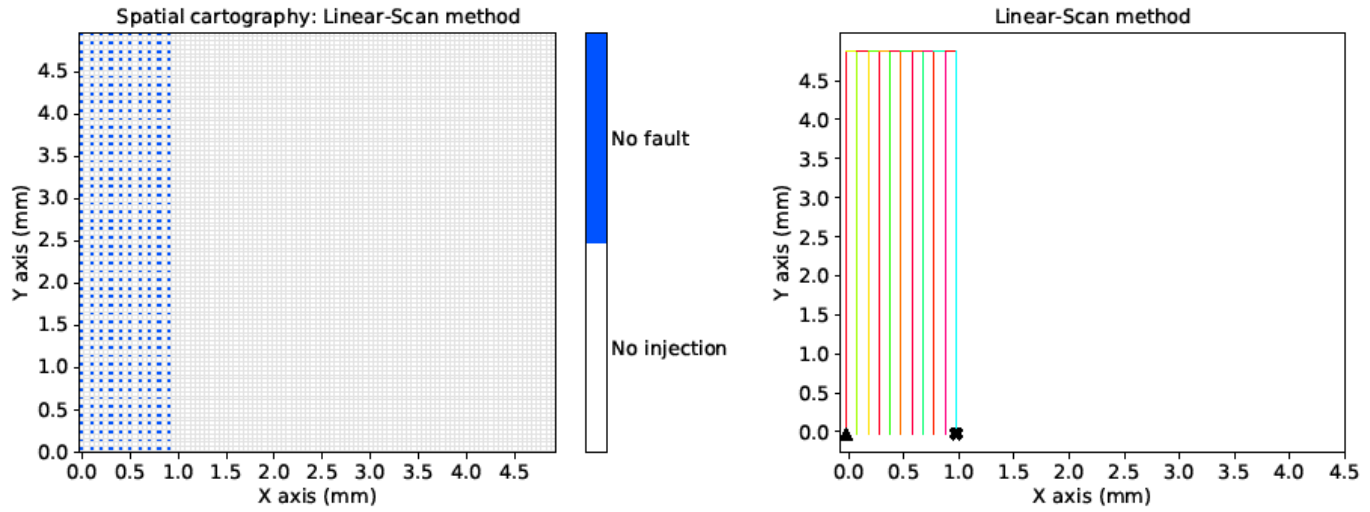
COMPARISON OF CARTOGRAPHY STRATEGIES



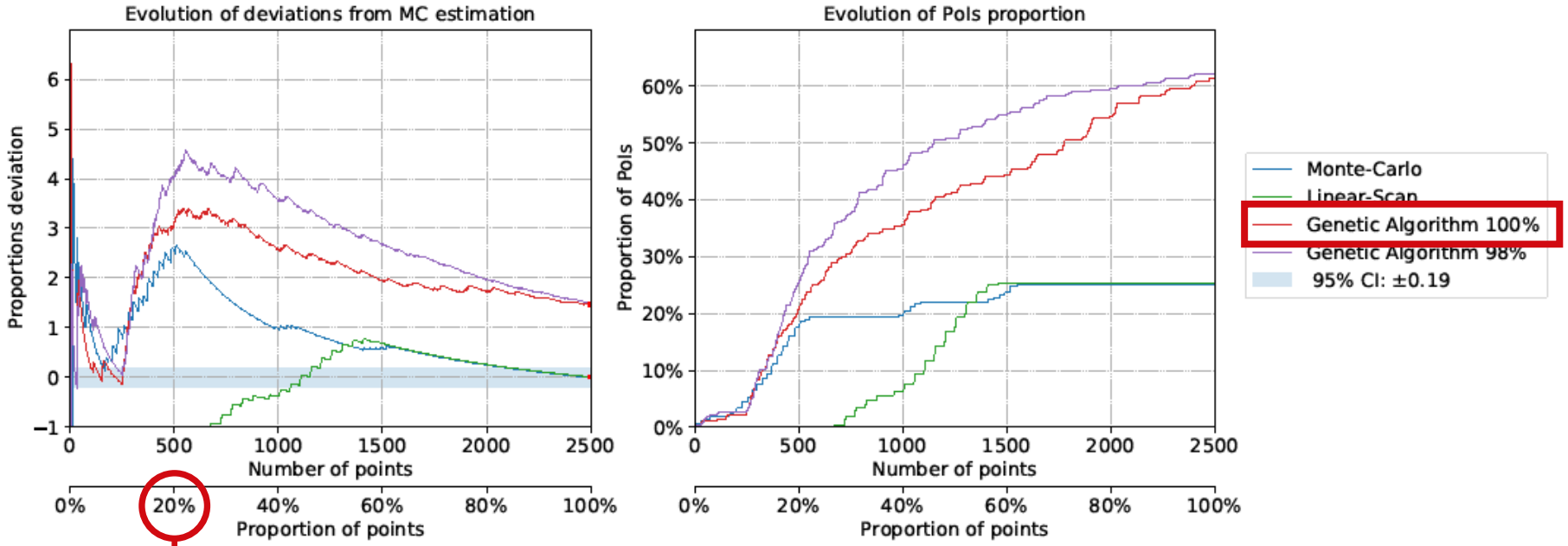
- Using Monte-Carlo, we estimate the proportion of PoIs in the set of selectable points over the scanned surface, and its total number.
- These reference values are compared with the proportion/number of PoIs in the samples from the different scan methods.

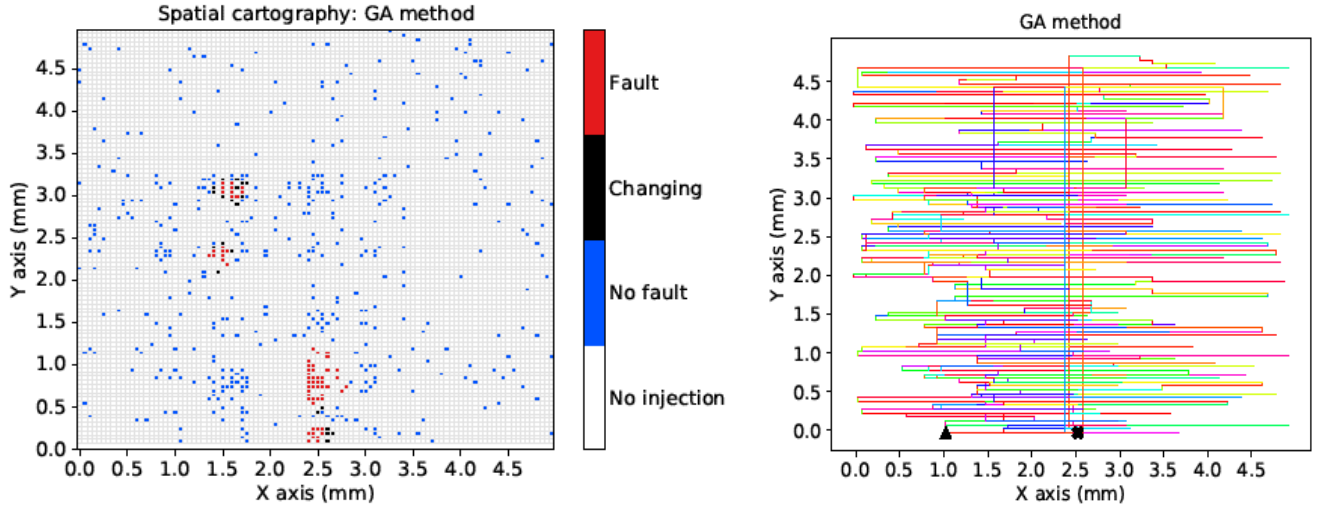
COMPARISON OF CARTOGRAPHY STRATEGIES



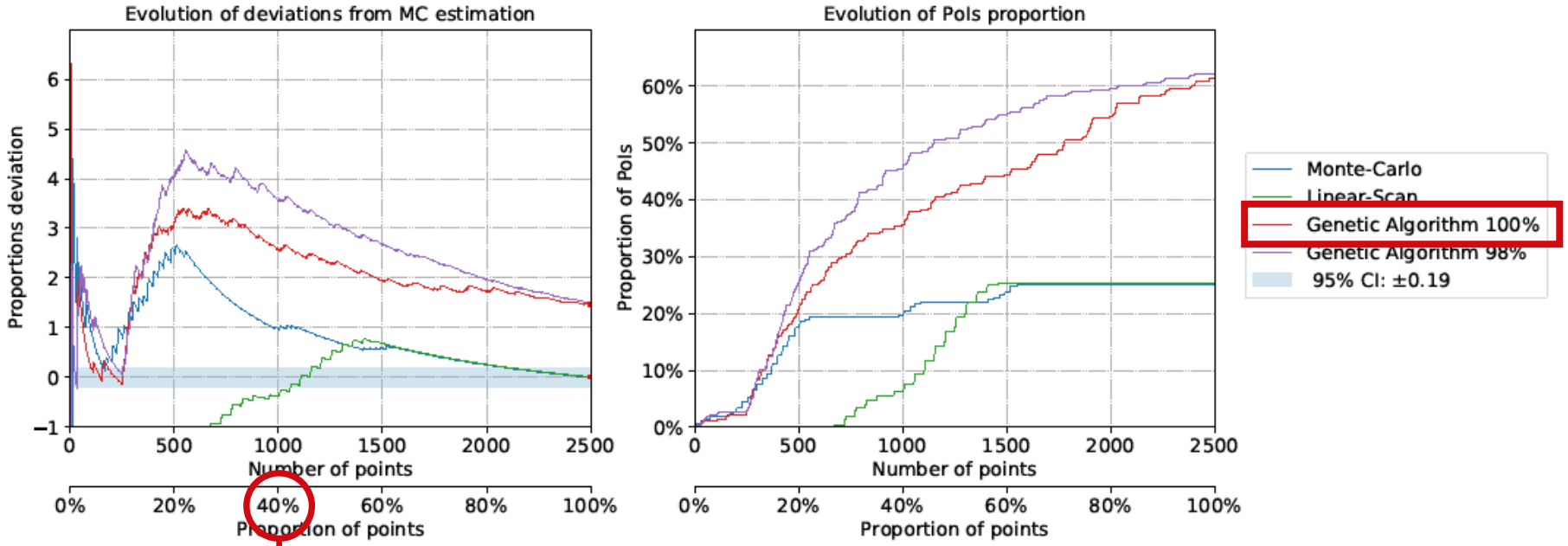


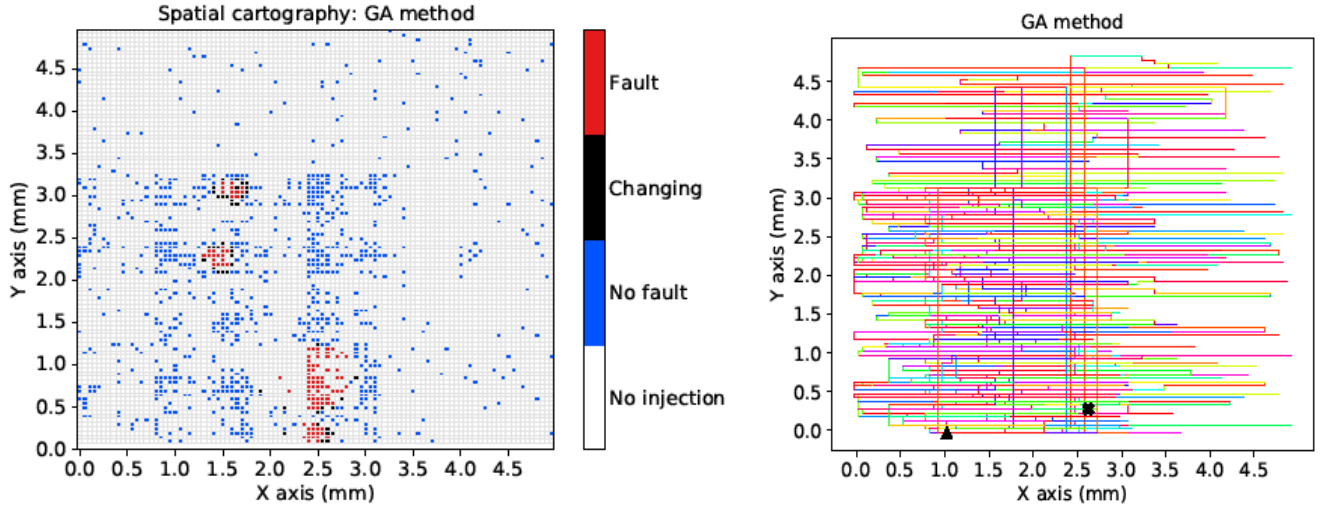
COMPARISON OF CARTOGRAPHY STRATEGIES



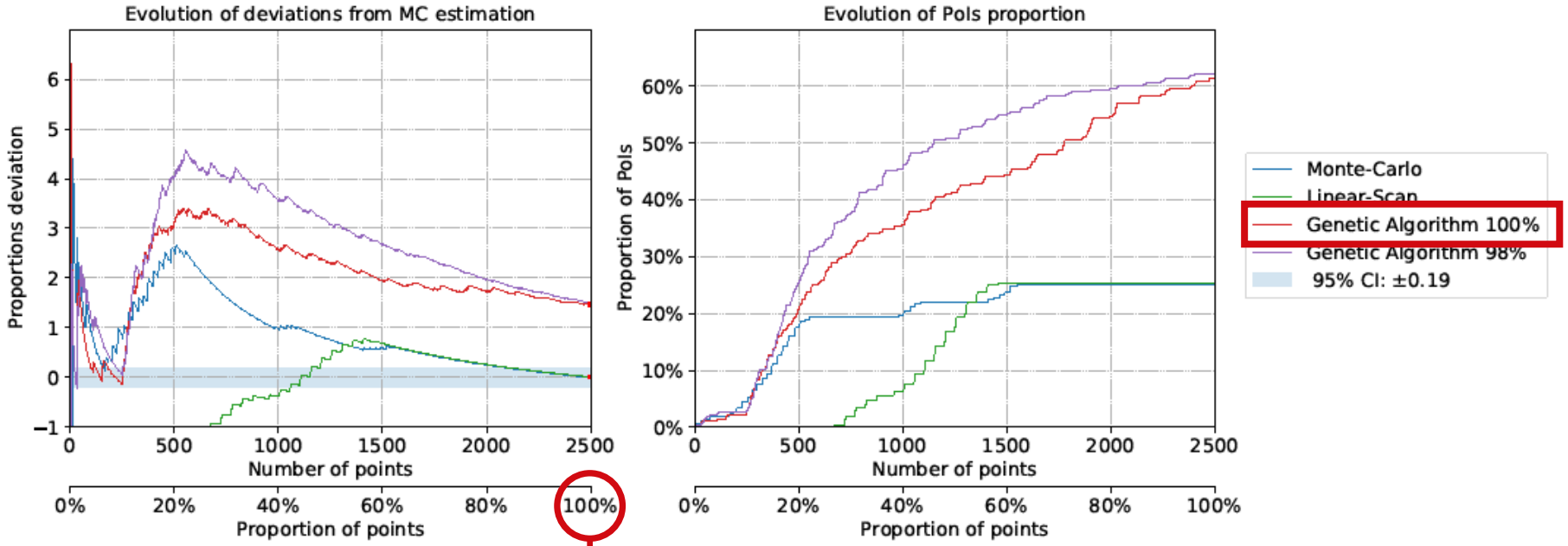


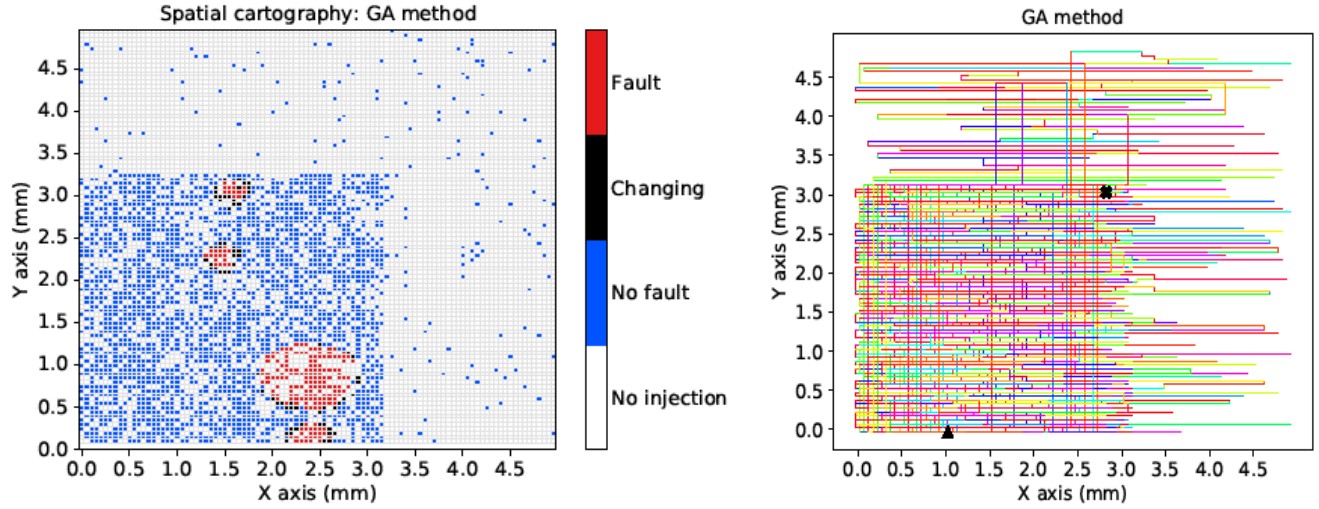
COMPARISON OF CARTOGRAPHY STRATEGIES



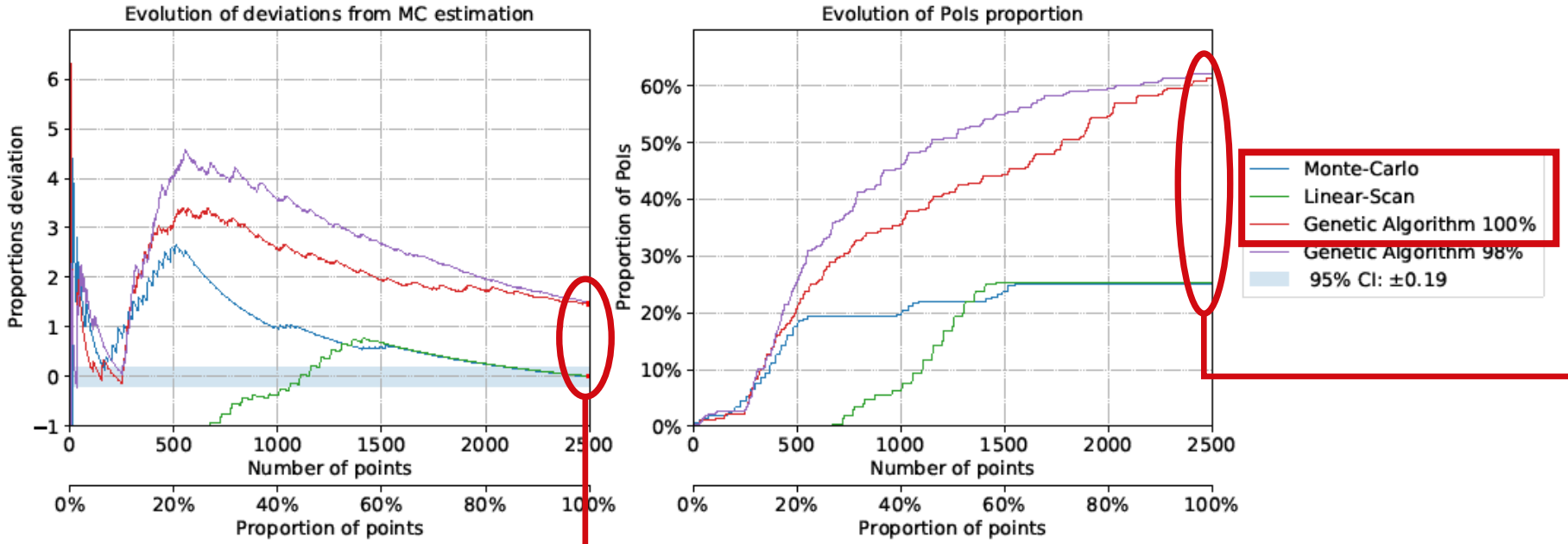


COMPARISON OF CARTOGRAPHY STRATEGIES





COMPARISON OF CARTOGRAPHY STRATEGIES



Cartography method	Proportion of PoIs in the sample	Deviation from estimation	Proportion of recovered PoIs
Linear-Scan	4.2%	1.0%	25.2%
Monte-Carlo	4.2%	0% *(reference)*	25.0%
Genetic Algorithm (98%)	10.4%	148.6%	62.1%
Genetic Algorithm (100%)	10.3%	145.7%	61.4%

QUANTIFYING THE SPEED-UP OFFERED BY GAS DURING FAULT INJECTION CARTOGRAPHIES

1. Fault Injection Analyses & Points of Interest
2. EMFI experiments
3. Spatial cartographies and Genetic Algorithms (GAs)
4. Quantifying a cartography method effectiveness
5. Conclusions

CONCLUSION

- We introduced a way to evaluate and compare the efficiency of different cartography methods.
- For spatial cartographies, the use of Genetic Algorithm has a significant benefit to identify Area of Interests and obtain a qualitative sample.
- Outlooks:
  - Comparison with Memetic Algorithms (GA + local search).
  - Adaptation for cartographies in higher dimensions.
  - Study of the impact of the intern functions of the GA (initial generation selection, fitness evaluation, selection, crossover and mutation).

SECURE-IC
THE SECURITY SCIENCE COMPANY

THANK YOU FOR YOUR ATTENTION

CONTACTS

EMEA	sales-EMEA@secure-IC.com
APAC	sales-APAC@secure-IC.com
CHINA	sales-CHINA@secure-IC.com
JAPAN	sales-JAPAN@secure-IC.com
AMERICAS	sales-US@secure-IC.com

REFERENCES

- [Mor+13] N. Moro, A. Dehbaoui, K. Heydemann, B. Robisson, and E. Encrenaz, “Electromagnetic fault injection on microcontrollers,” in Chip-to-Cloud Security Forum 2013, 2013.
- [Mal+18] A. Maldini, N. Samwel, S. Picek, and L. Batina, “Genetic algorithm-based electromagnetic fault injection,” in 2018 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC). IEEE, 2018, pp.35–42.
- [Ree10] C. R. Reeves, “Genetic algorithms,” in Handbook of metaheuristics. Springer, September 2010, pp. 109–139, DOI: 10.1007/978-1-4419-1665-5_5.

APPENDIXES: GREAT AOI