KOBE UNIVERSITY

SeaQy
NAGATA and MIKI LAB
Semiconductors and Information systems

On-chip evaluation of voltage fluctuations and fault occurrence induced by Si backside EM injection

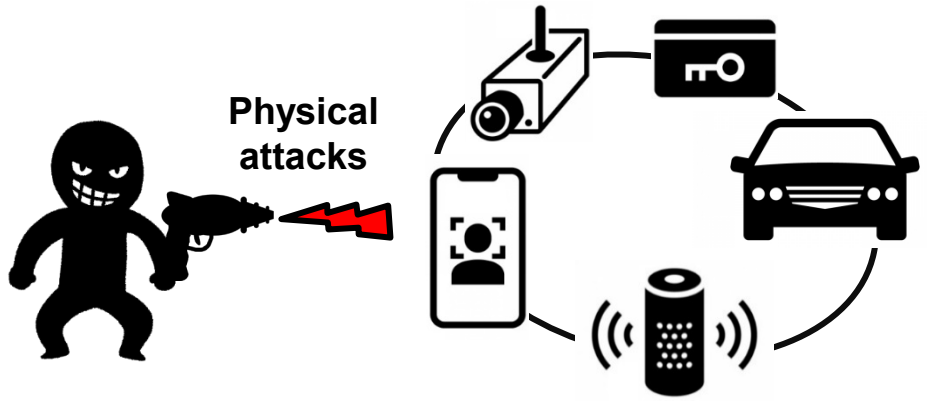
April 9th, 2024

Rikuu Hasegawa, Kazuki Monta, Takuya Wadatsumi, Takuji Miki, Makoto Nagata

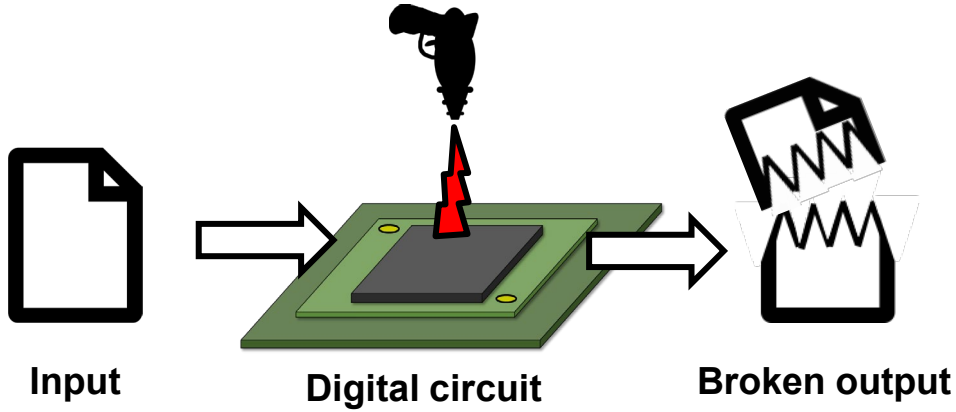
Graduate School of Science, Technology and Innovation, Kobe University

Threats of fault injection

- Security of semiconductor devices
  - ✓ Physical attack threats

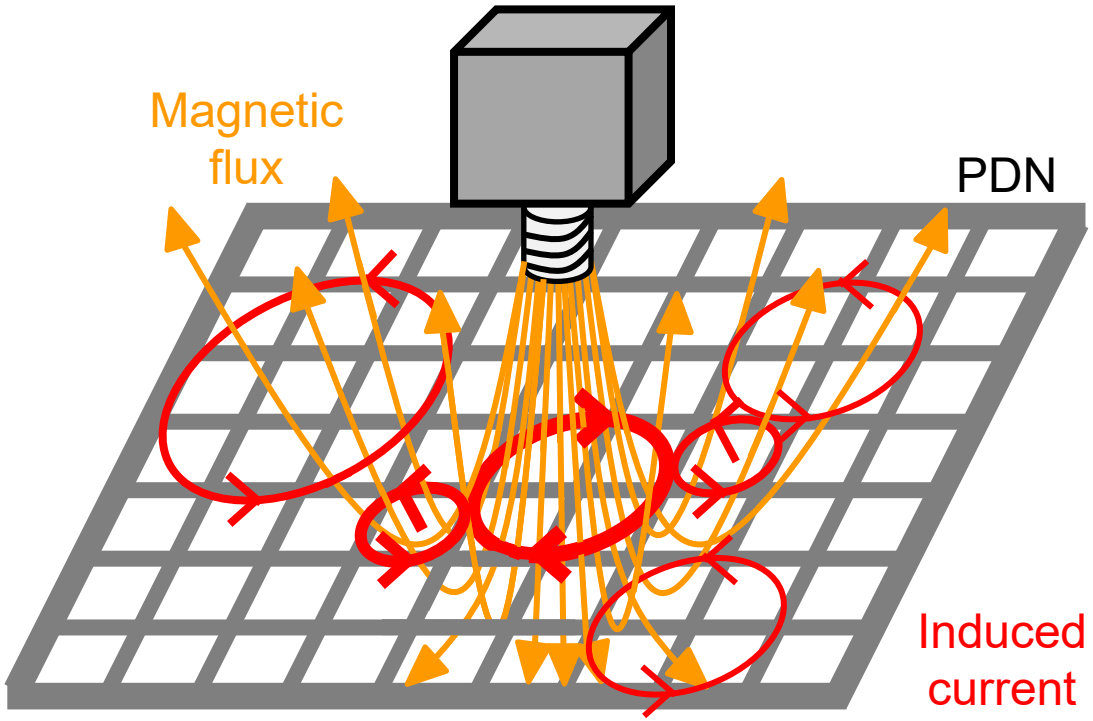


- Fault injection
  - ✓ Disturbance injection induces malfunction in the circuit operation.
    - – Laser, Voltage/Clock glitch, Body biasing, **Electromagnetic**



Electromagnetic fault injection (EMFI)

- Advantages of EMFI
  - ✓ Inexpensive and easy
  - ✓ Universal to any chip assembly technology



- Attack concept
  - ✓ Magnetic flux induces unwanted currents.

- Problems
  - ✓ The principle is not simpler as perceived from attack concepts.
  - ✓ Physical level understanding is missing.

Outline

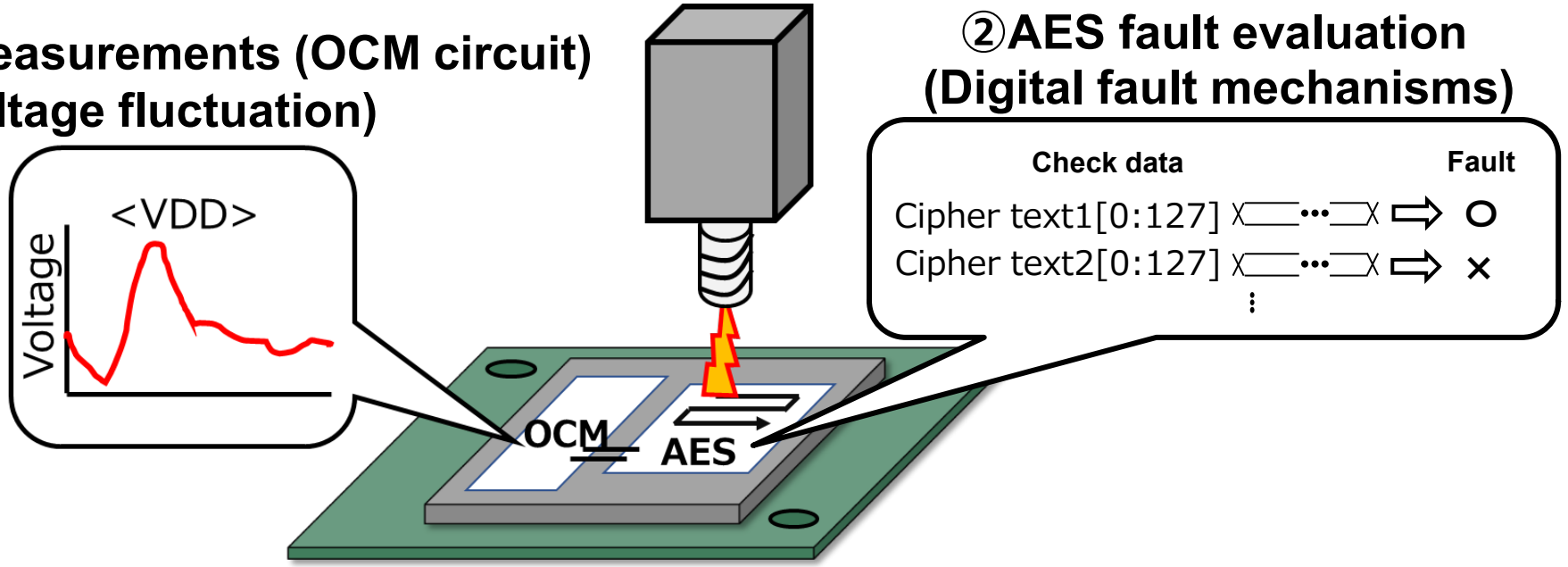
1. Background
2. Deliverables
3. Measurement and evaluation
   - On-chip voltage fluctuation
   - AES digital faults
4. EM simulation
5. Conclusion

Deliverables

- **Problems**
  - ✓ Physical mechanisms and parameters are less involved in EMFI analyses.
  - ✓ Needed more in-depth understandings from device physics
- **Contributions**
  - ✓ EMFI voltage fluctuations visualized by on-chip measurements, correlated with digital faults
  - ✓ Initial trials of EM simulation-based analysis

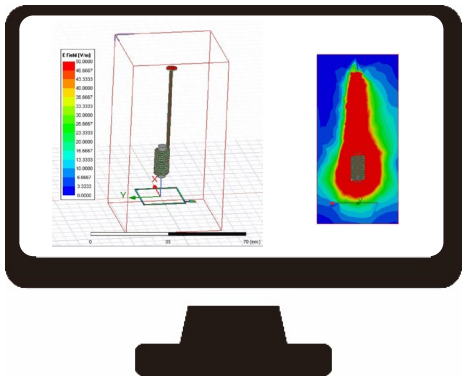
What we did…

①On-chip measurements (OCM circuit)
(Voltage fluctuation)



②AES fault evaluation
(Digital fault mechanisms)

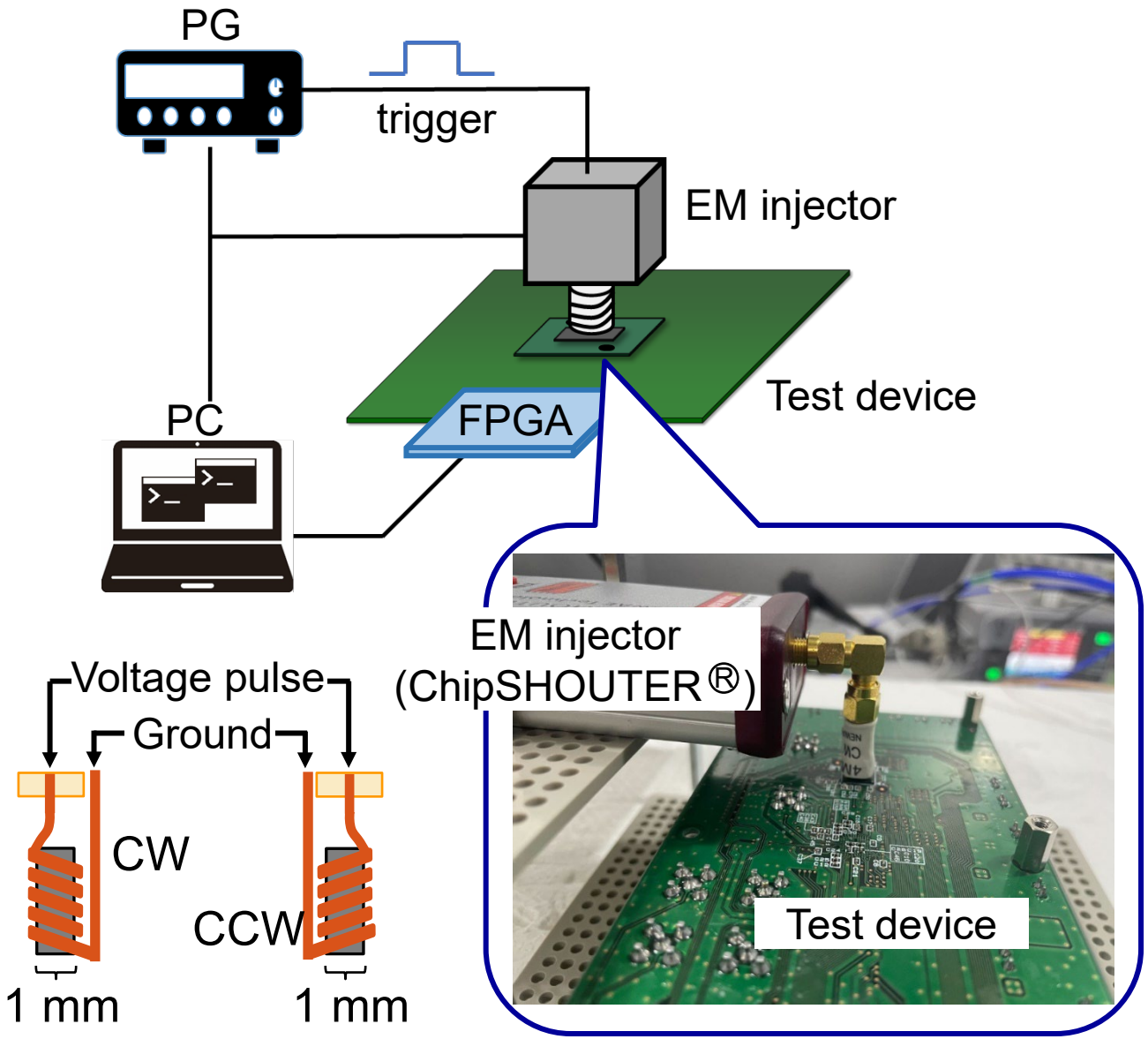
③EM simulation
(Voltage fluctuation)

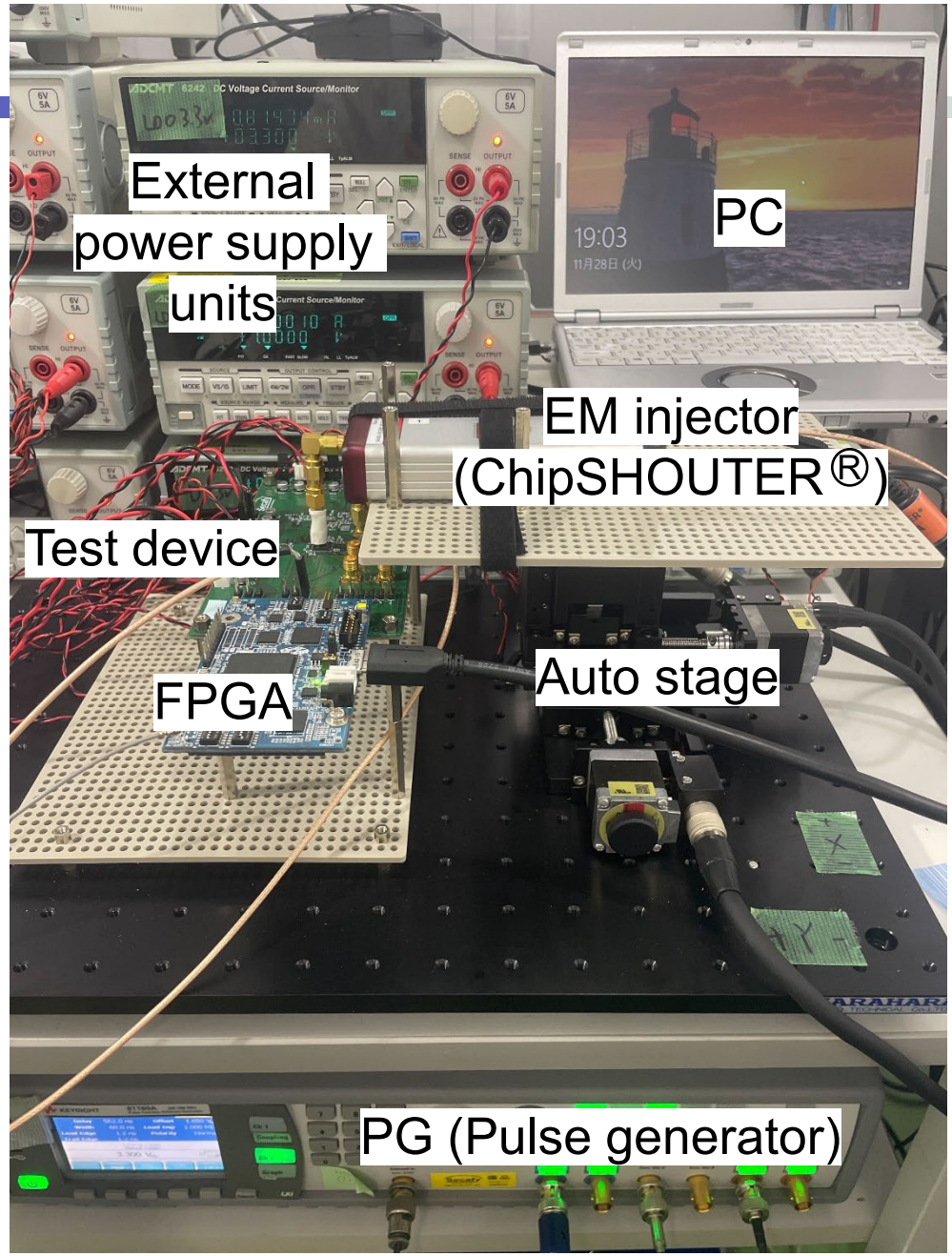


Outline

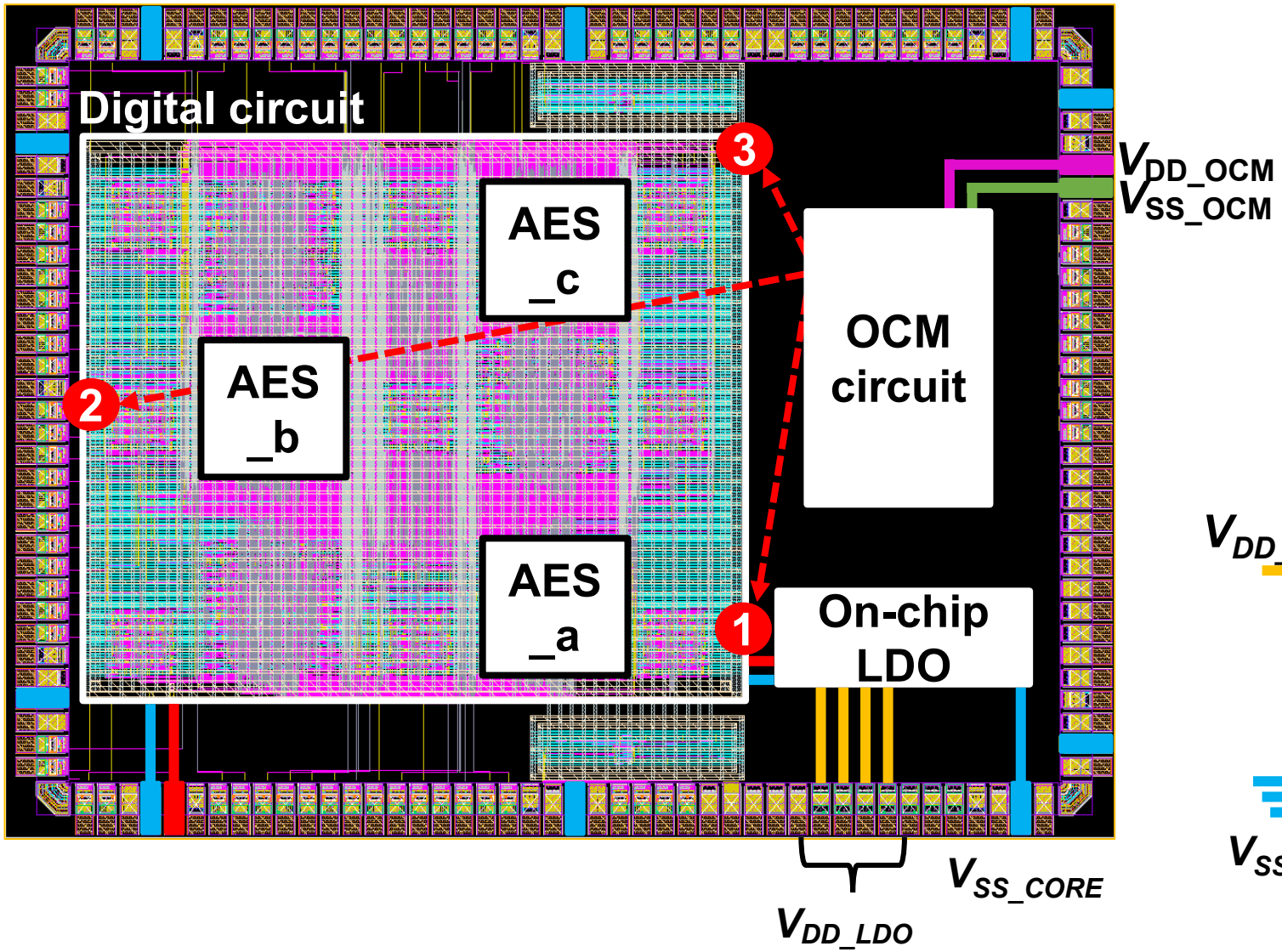
1. Background
2. Deliverables
3. Measurement and evaluation
   - On-chip voltage fluctuation
   - AES digital faults
4. EM simulation
5. Conclusion

Evaluation setup

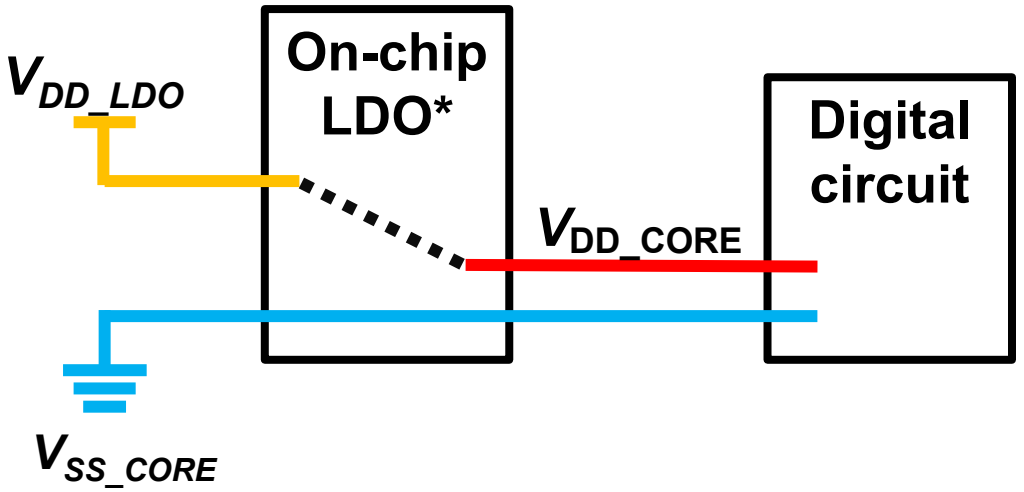




Test chip



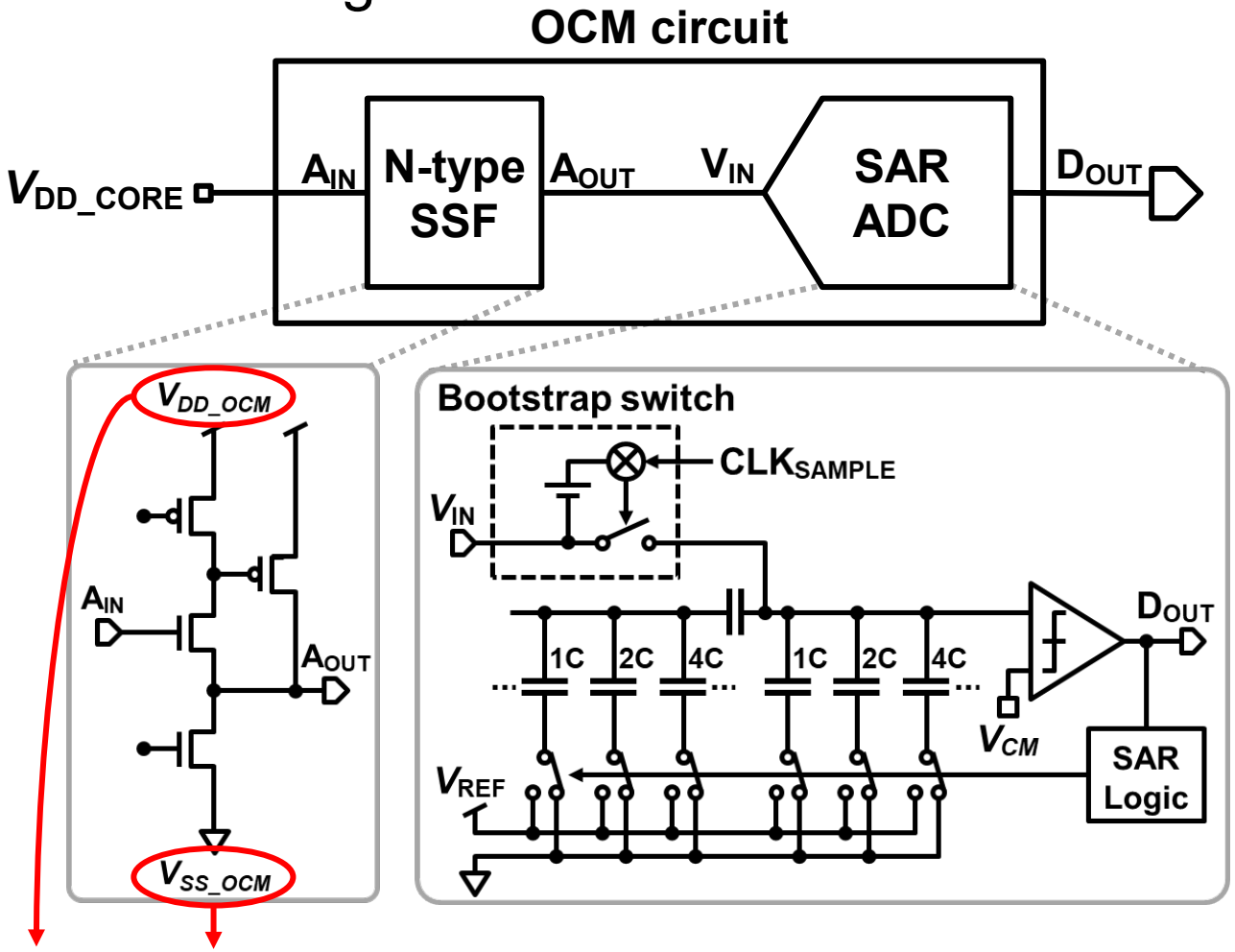
- 180 nm CMOS
- Flip-chip BGA
- Chip size : 3 mm x 4 mm



*LDO : Low drop-out voltage regulator

OCM circuits and on-chip waveforms

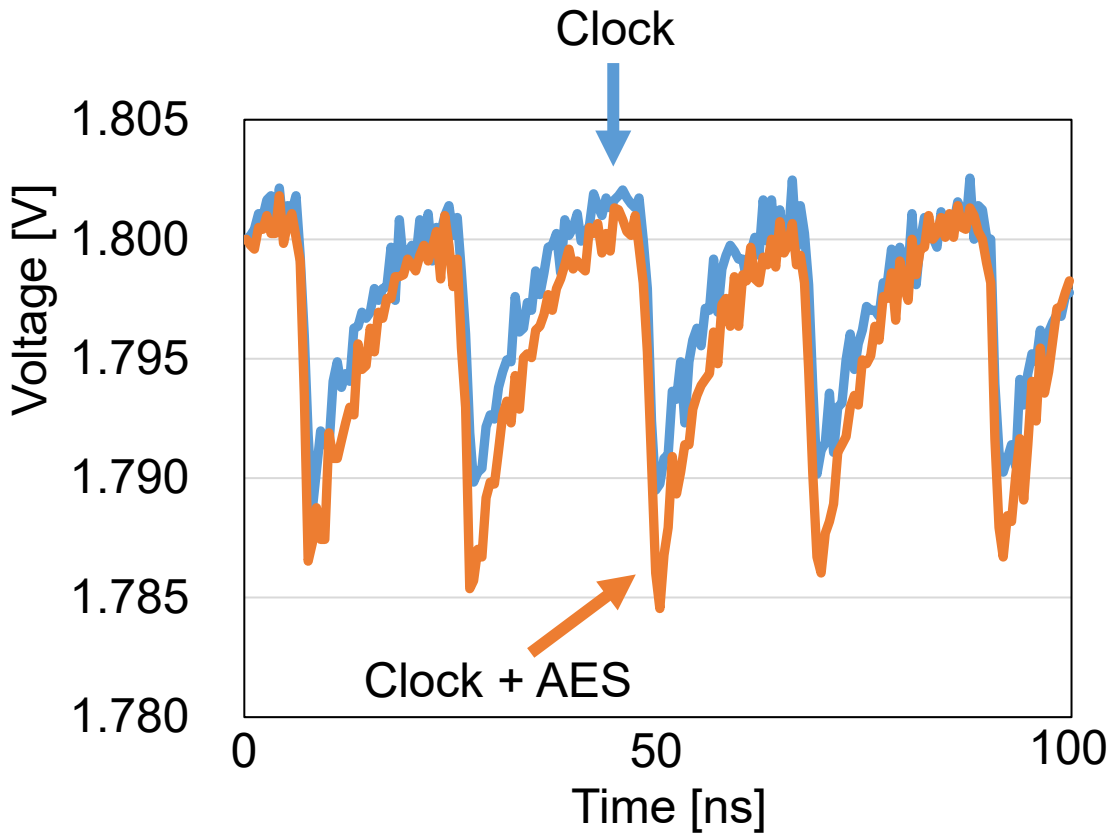
- Circuit diagrams



Isolated from digital circuit

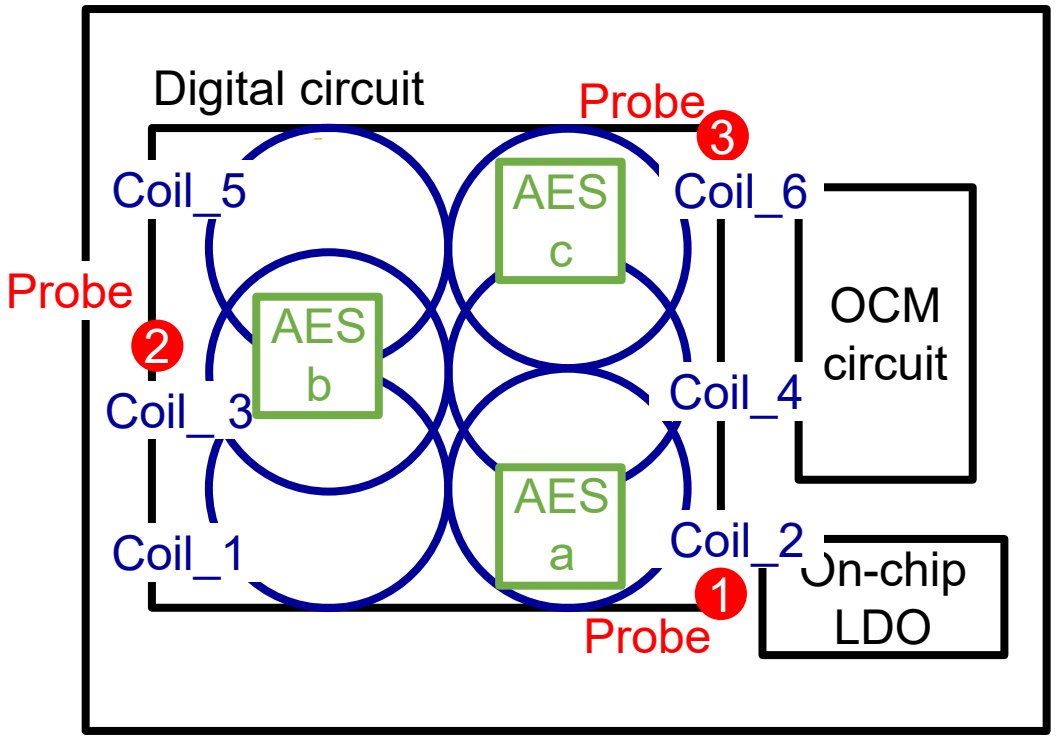
- ✓ Frequency bandwidth : 1 GHz
- ✓ Voltage resolution: 11 bit, 1 mV for 1 *V*pp

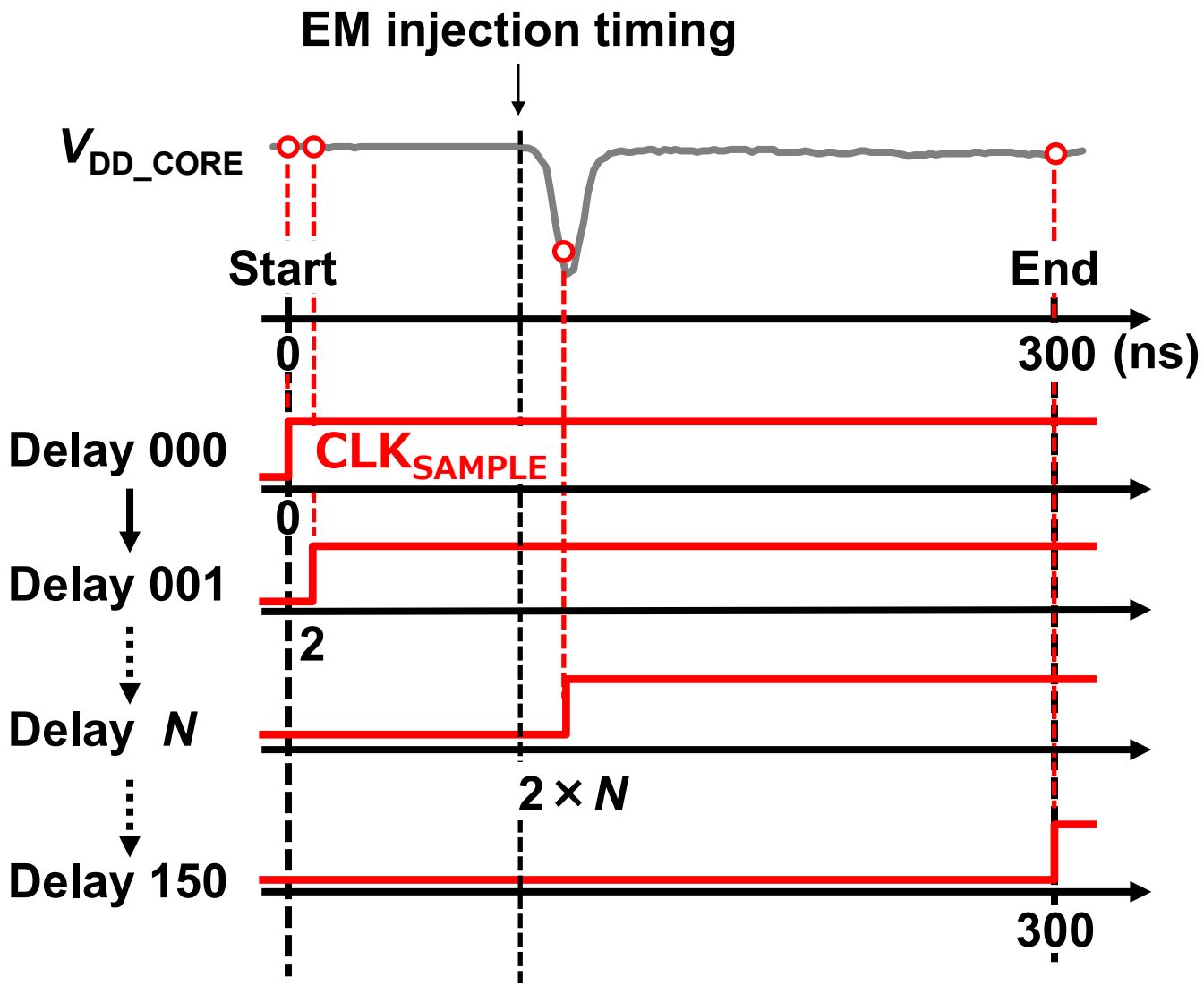
- Power noise waveforms
  - ✓ Differences due to the scale of the circuit in operation



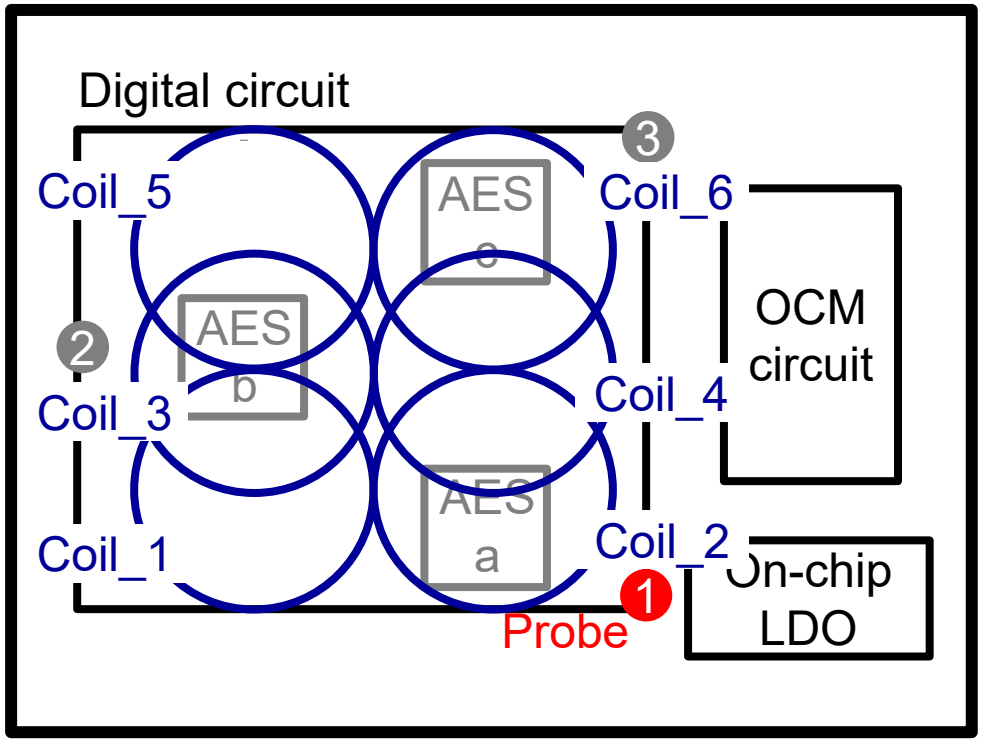
EMFI on-chip voltage measurements

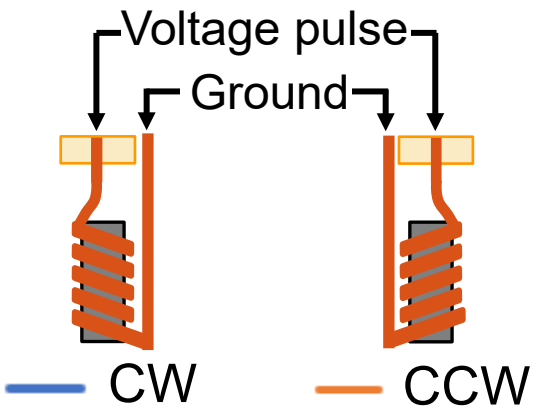
- Waveform acquisition under EMFI
- Time equivalent sampling method applied in measurement

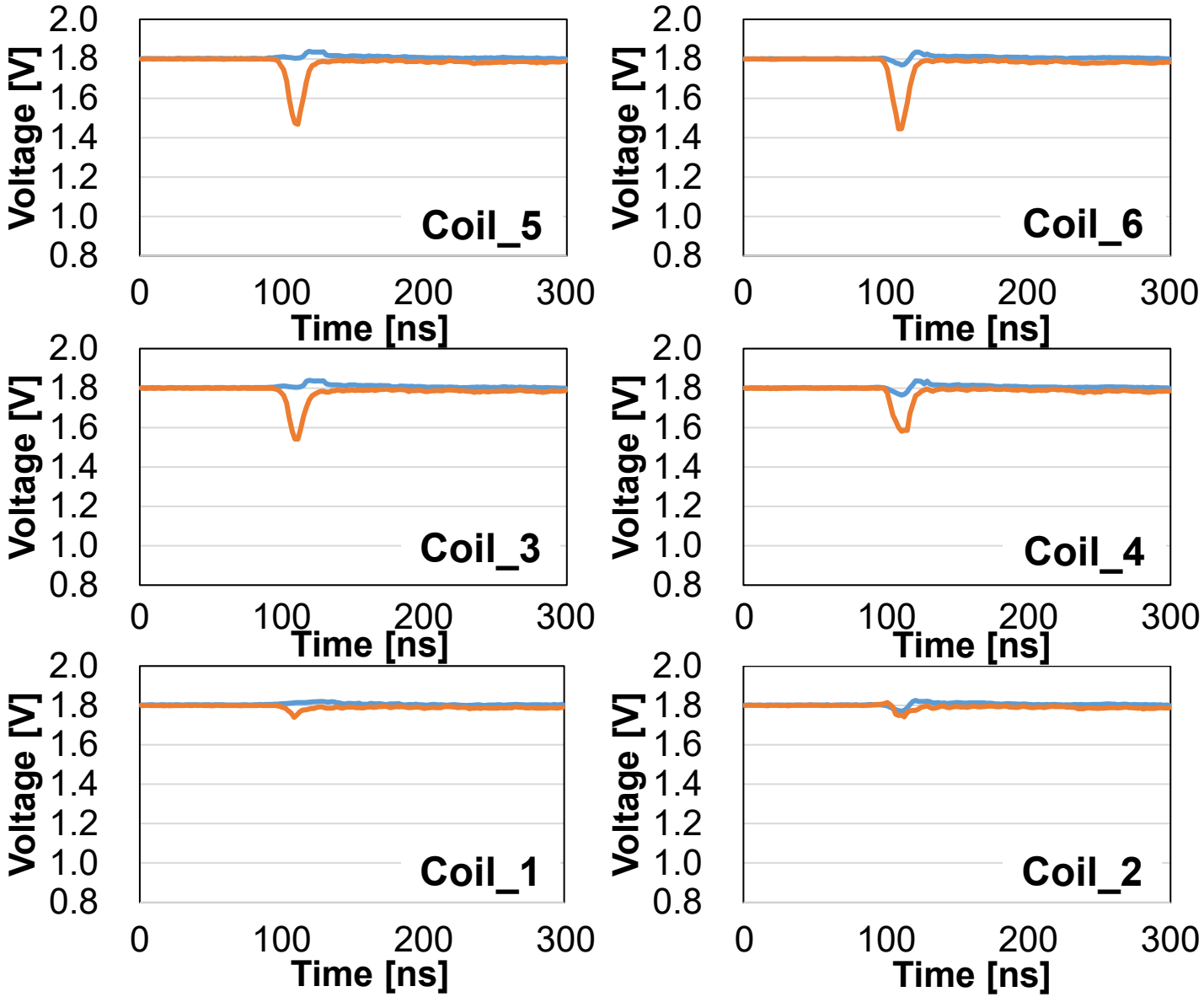




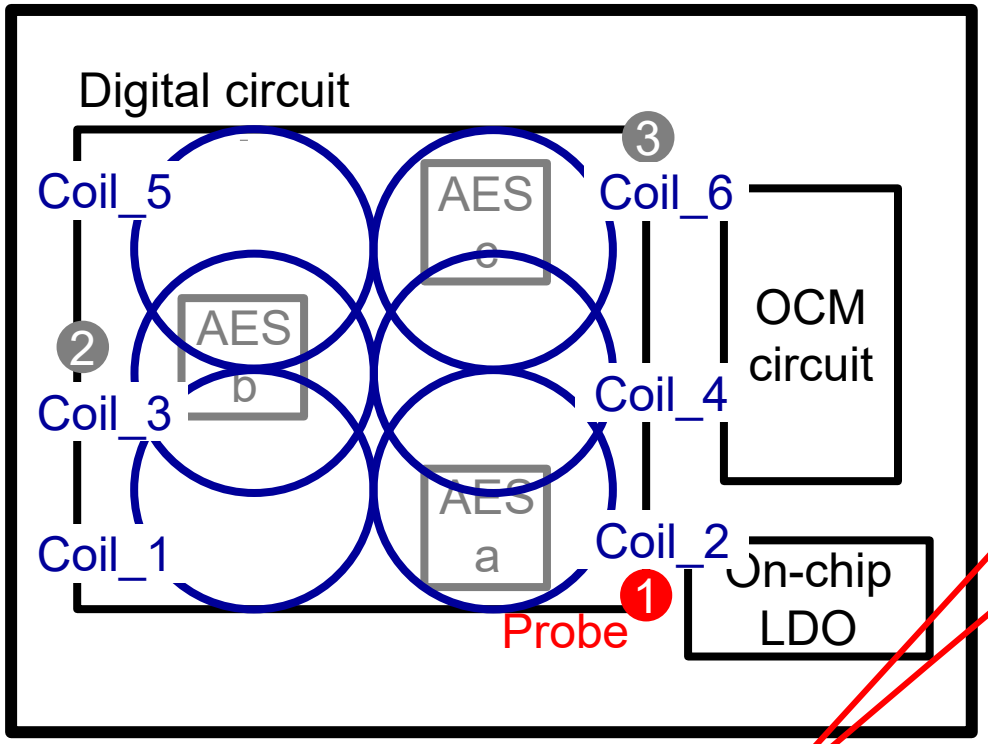
Measurement results



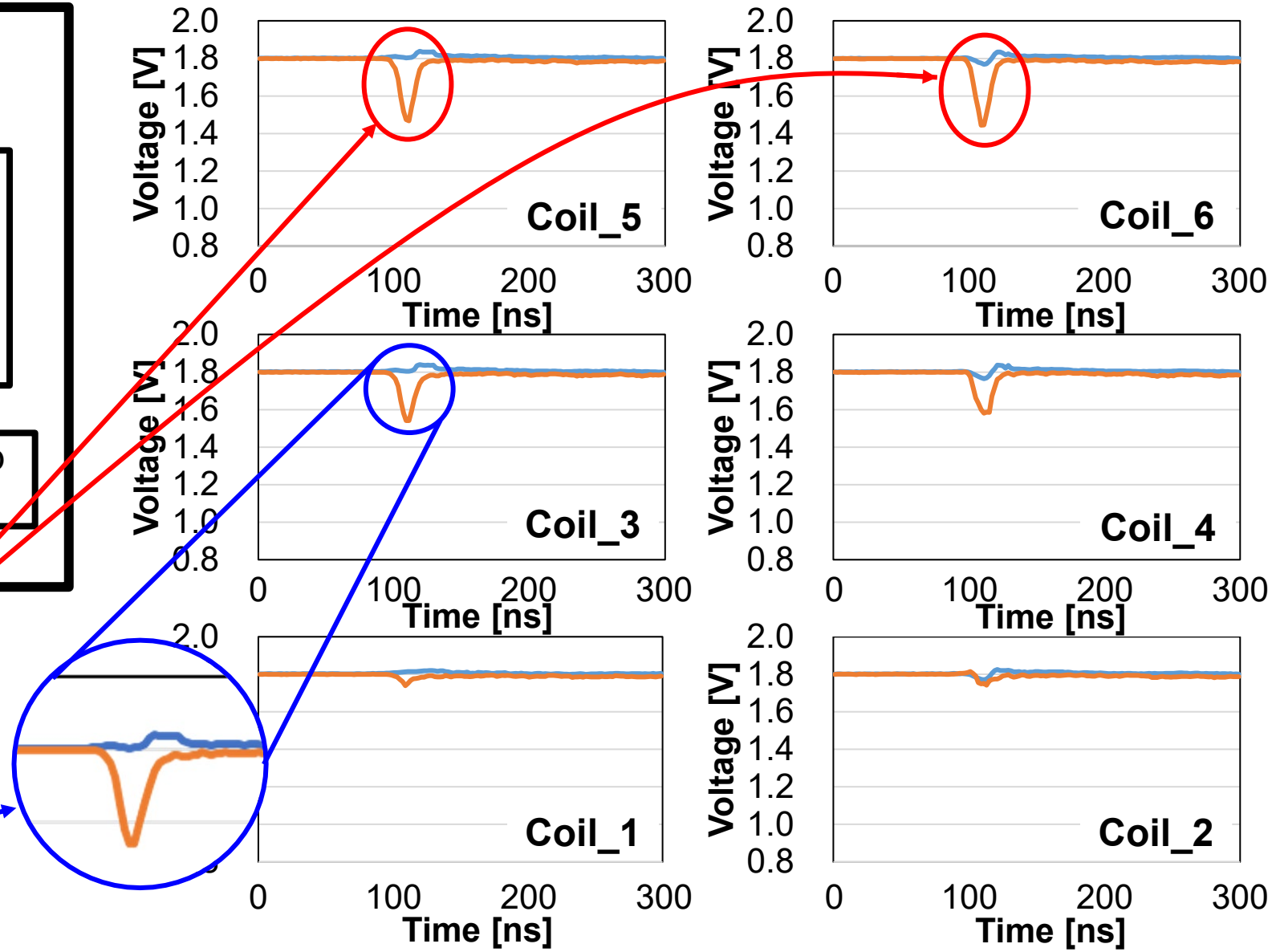




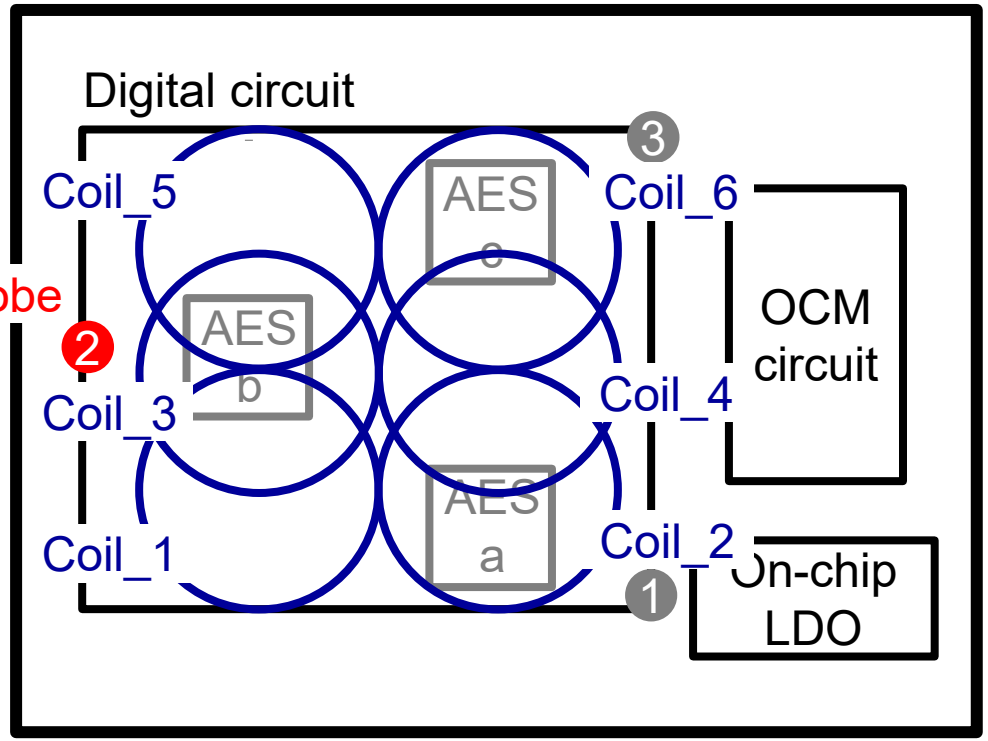
Findings from measurements

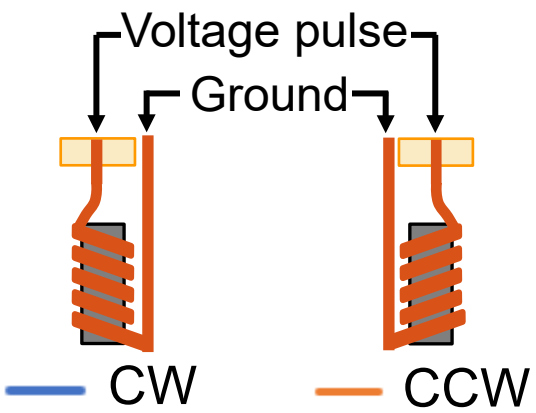


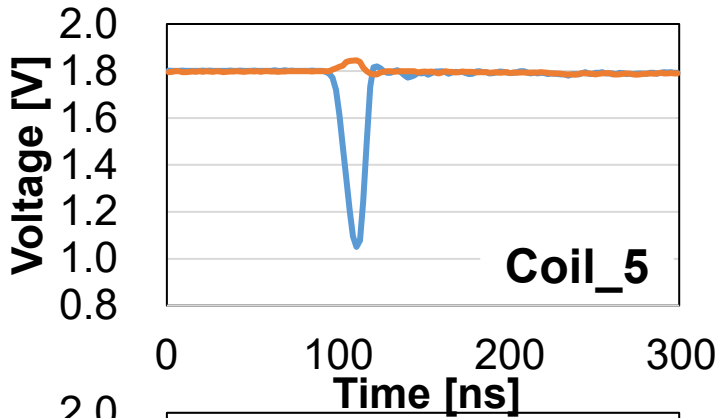
- Large drops in areas far from the coil
- Both positive and negative voltage fluctuation

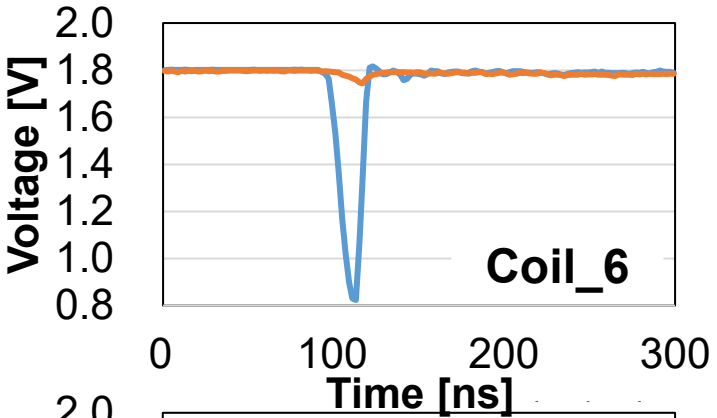


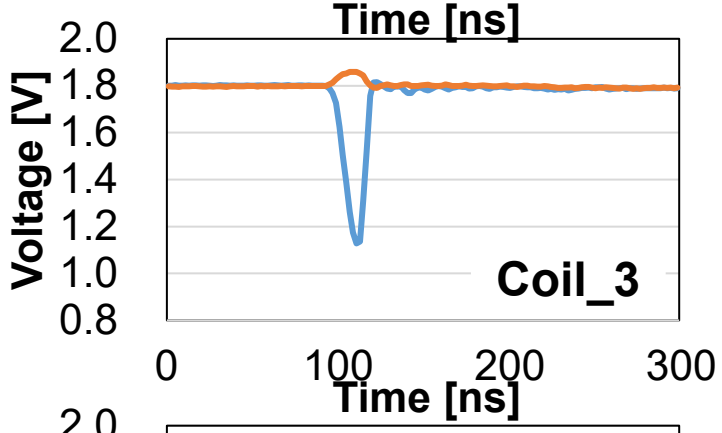
Measurement results

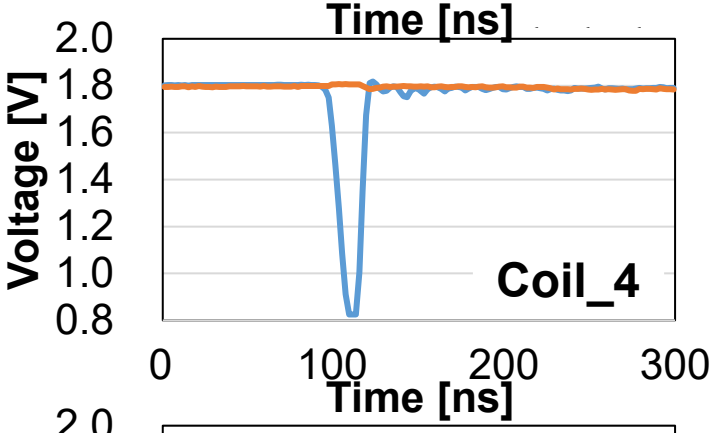


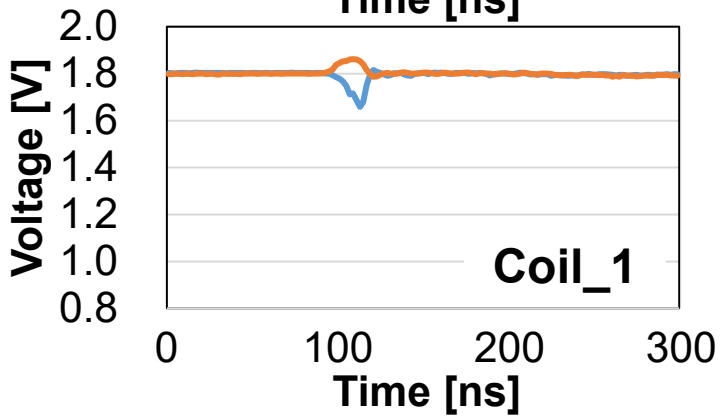


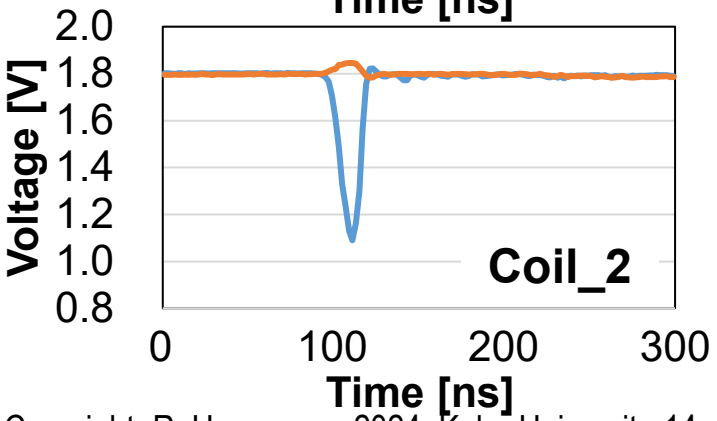




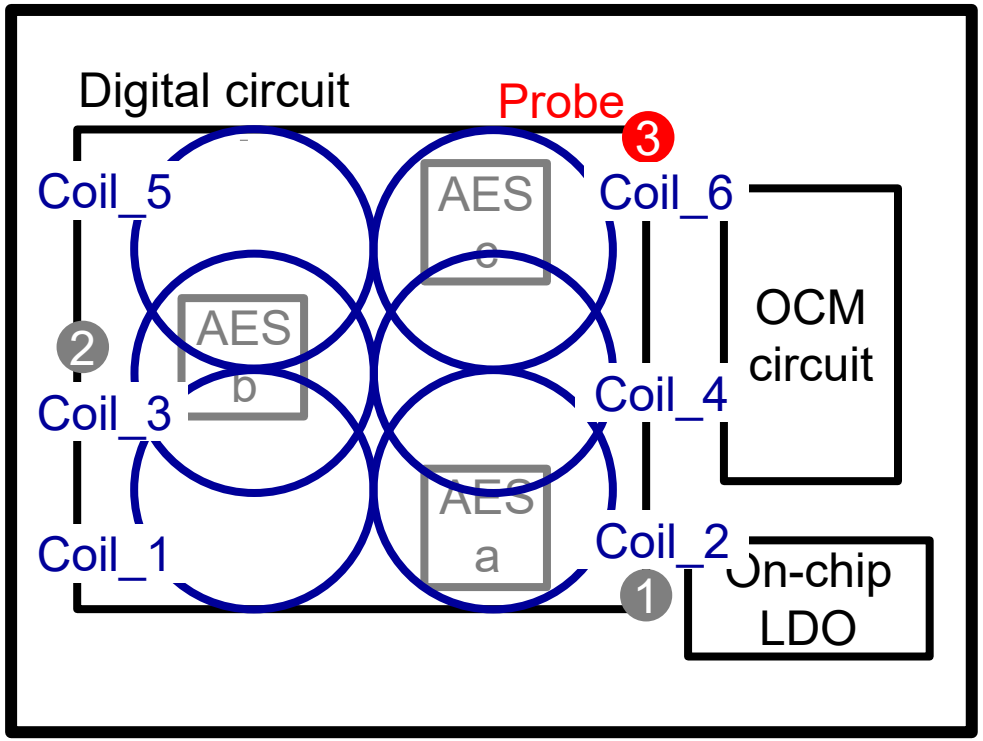


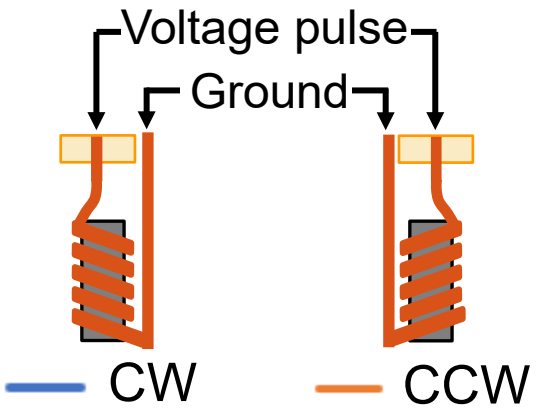


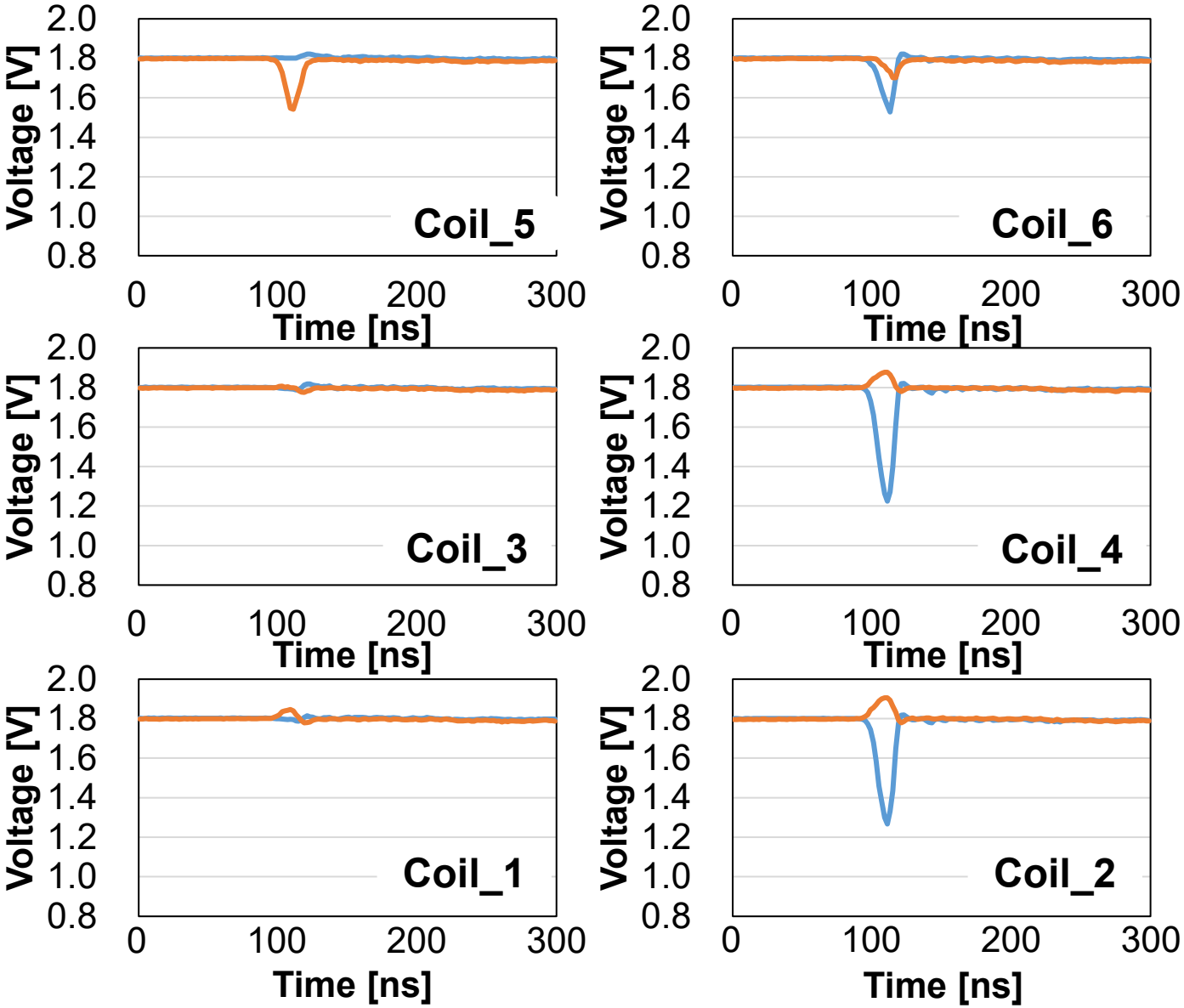




Measurement results

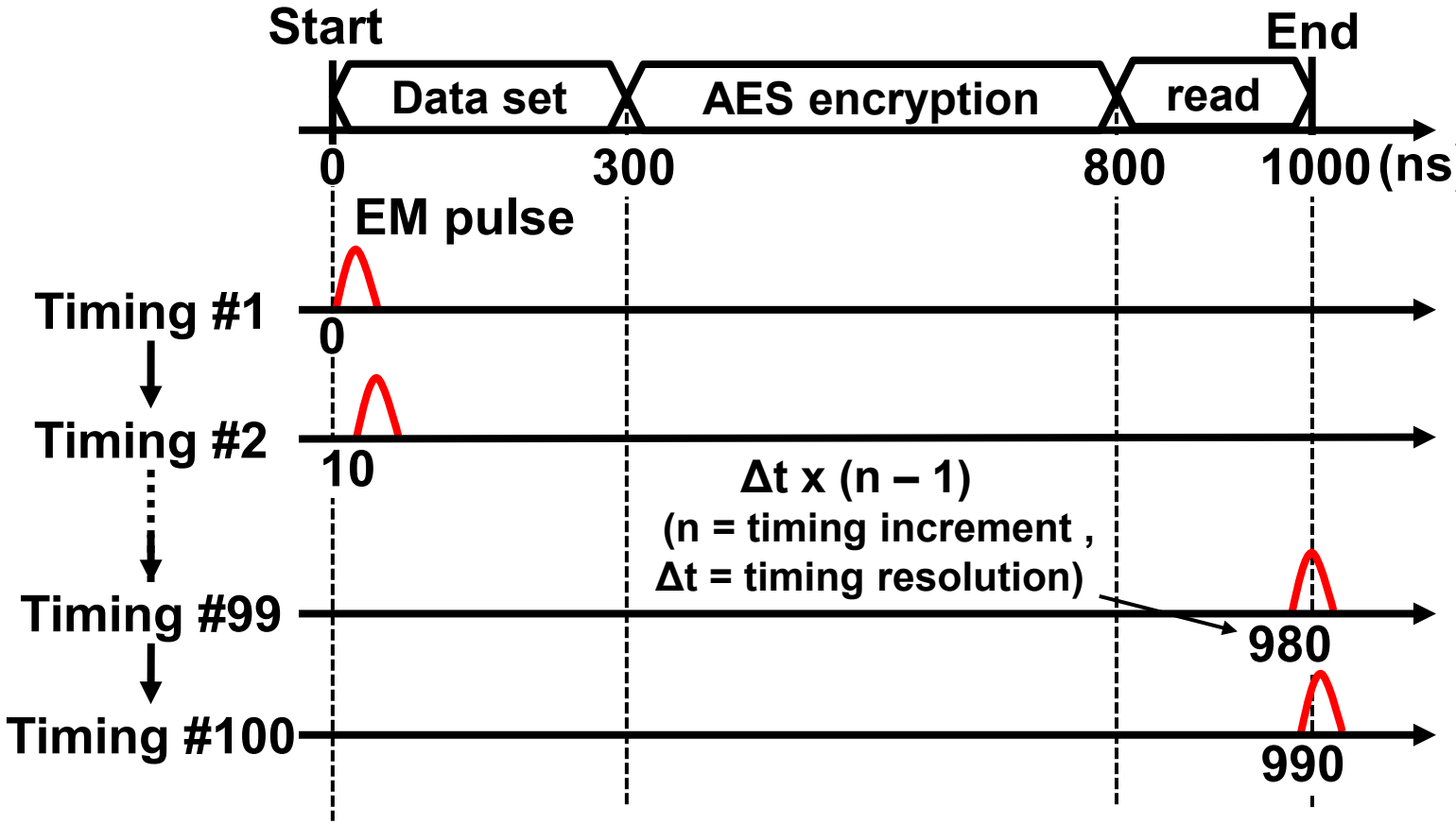


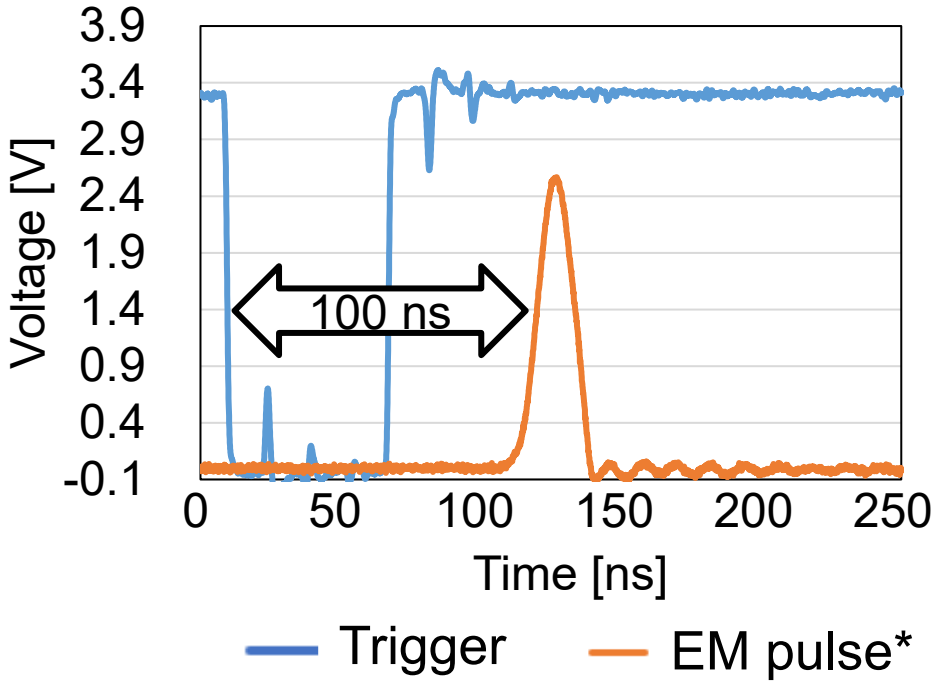




Evaluation of digital faults

- Irradiate EM pulse during digital circuit operation

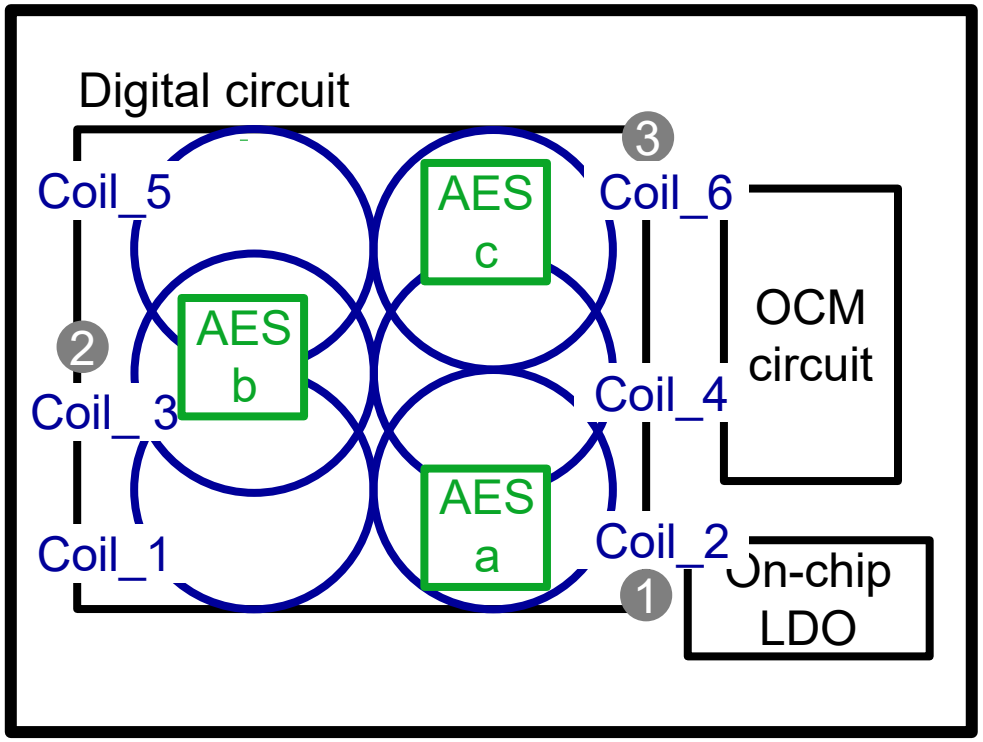




Repeat 3 time at each timing
⇒Total 300 ciphertext

*measured by EM probe

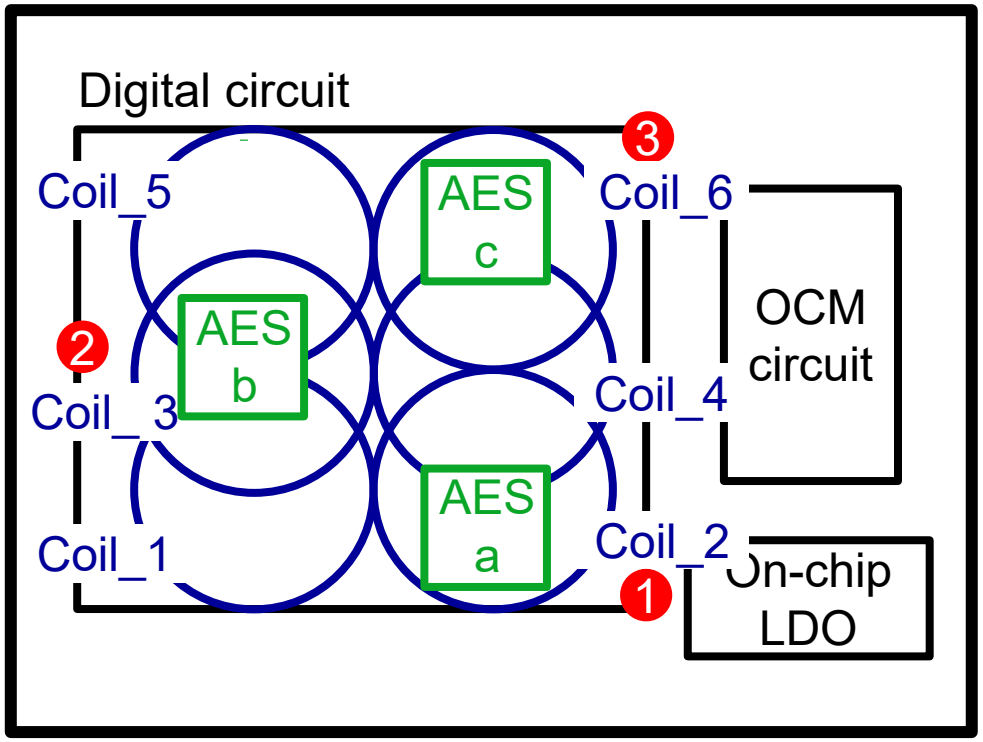
Evaluation results

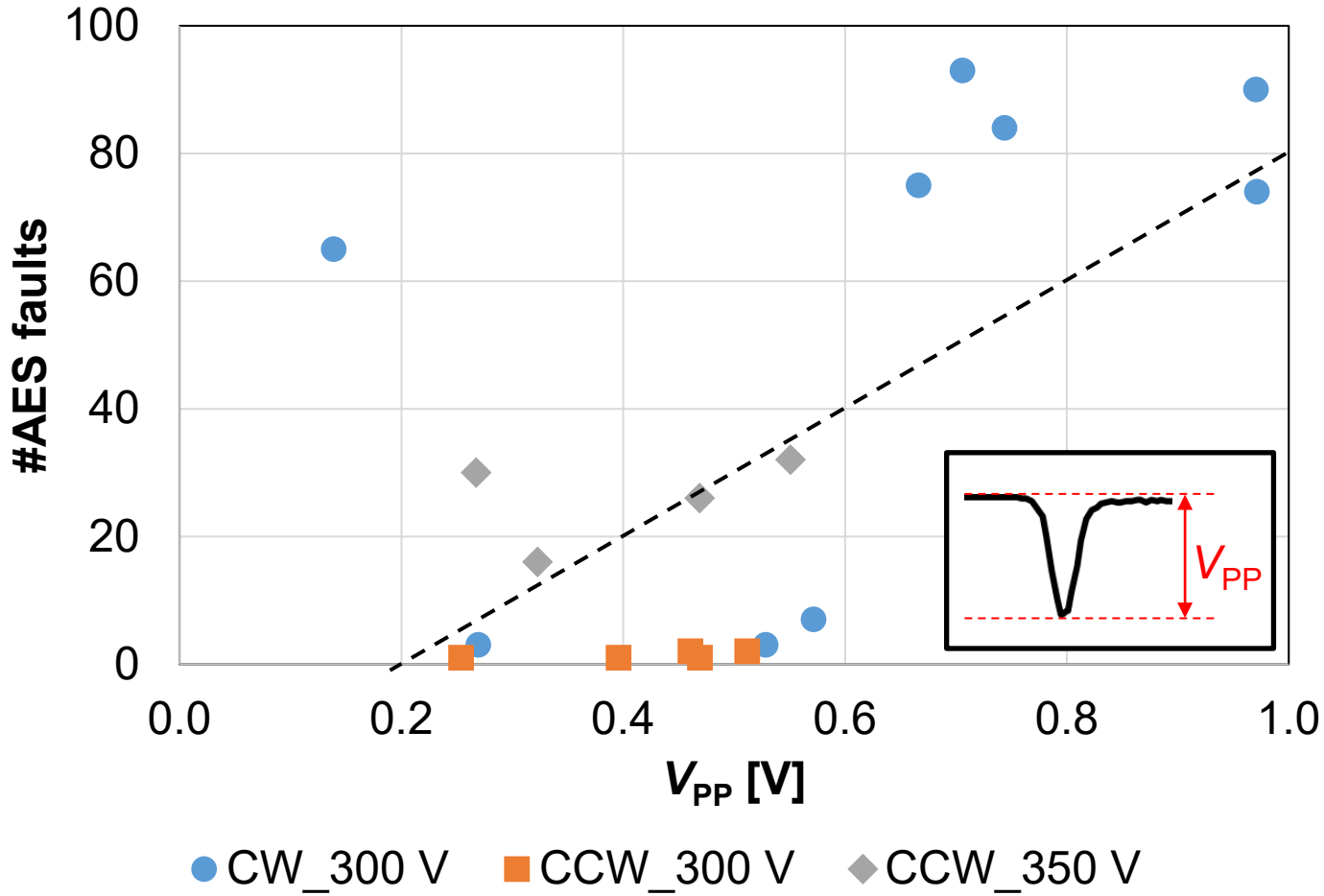


CW				CCW			
AES_c				AES_c			
Coil_5	**6**	Coil_6	3	Coil_5	1	Coil_6	3
Coil_3	1	Coil_4	**7**	Coil_3	1	Coil_4	2
Coil_1	2	Coil_2	3	Coil_1	1	Coil_2	2
AES_b				AES_b			
Coil_5	**84**	Coil_6	**74**	Coil_5	1	Coil_6	1
Coil_3	**75**	Coil_4	**90**	Coil_3	1	Coil_4	0
Coil_1	**65**	Coil_2	**93**	Coil_1	1	Coil_2	1
AES_a				AES_a			
Coil_5	**9**	Coil_6	**6**	Coil_5	2	Coil_6	1
Coil_3	3	Coil_4	**13**	Coil_3	2	Coil_4	1
Coil_1	4	Coil_2	2	Coil_1	4	Coil_2	1

- Key findings
  - ✓ # of digital faults reflect different layout positions among identical AES cores

Analysis : Voltage fluctuations and AES faults





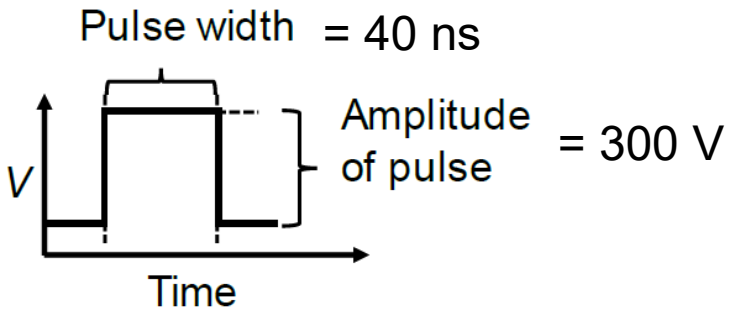
- On-chip voltage fluctuations and AES digital faults are correlated

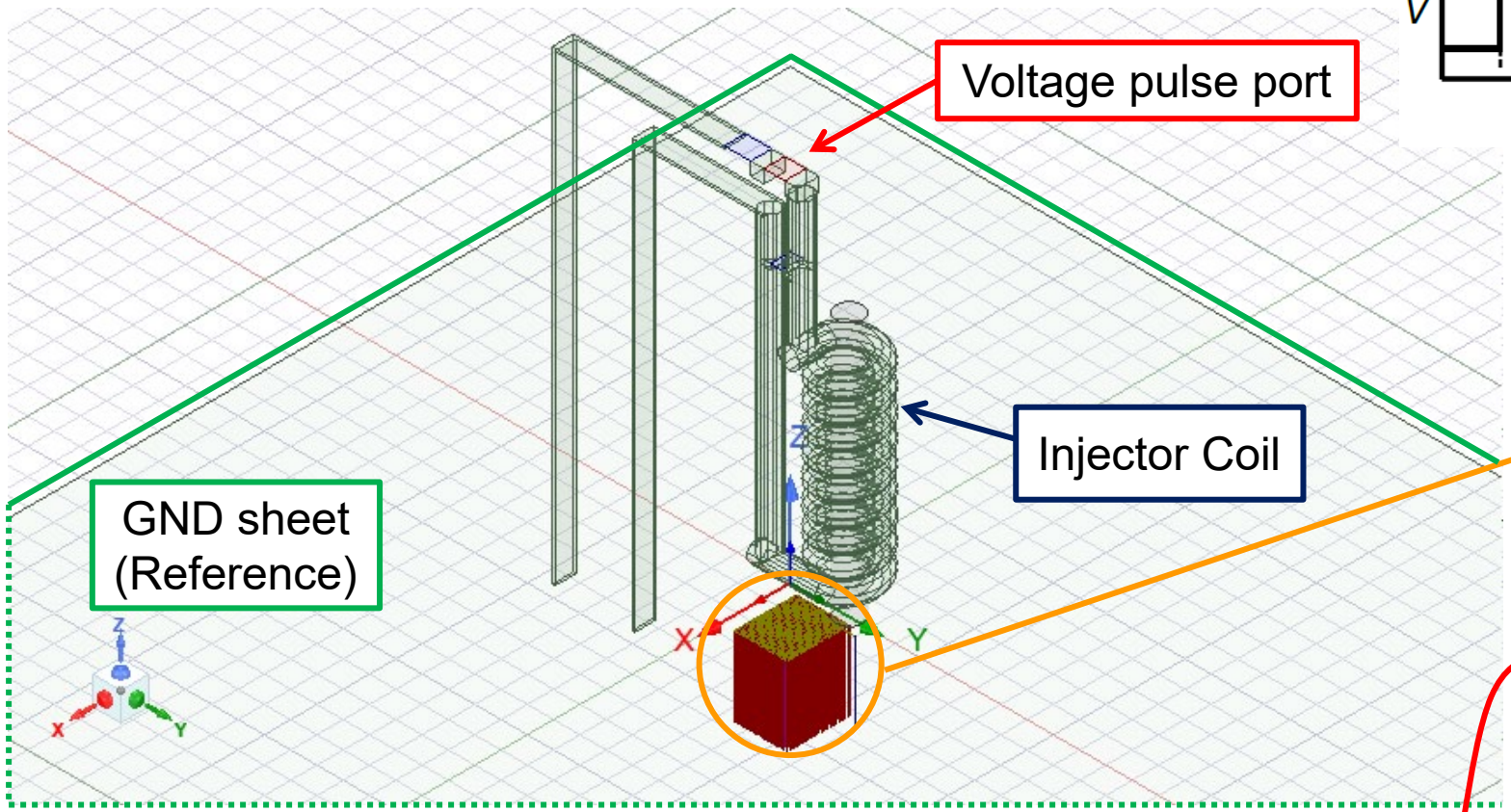
Outline

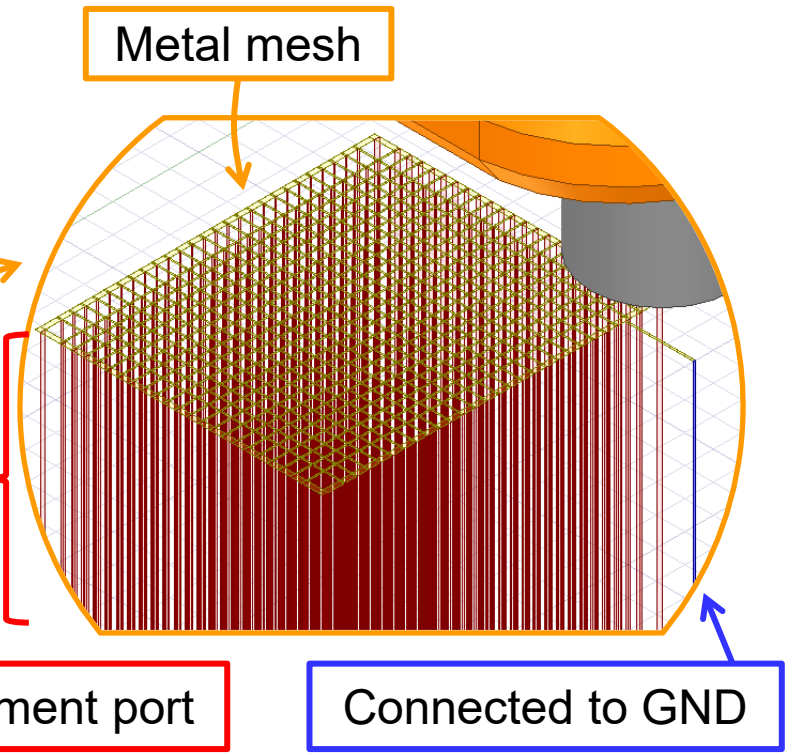
1. Background
2. Deliverables
3. Measurement and evaluation
   - On-chip voltage fluctuation
   - AES digital faults
4. EM simulation
5. Conclusion

EM simulation trials

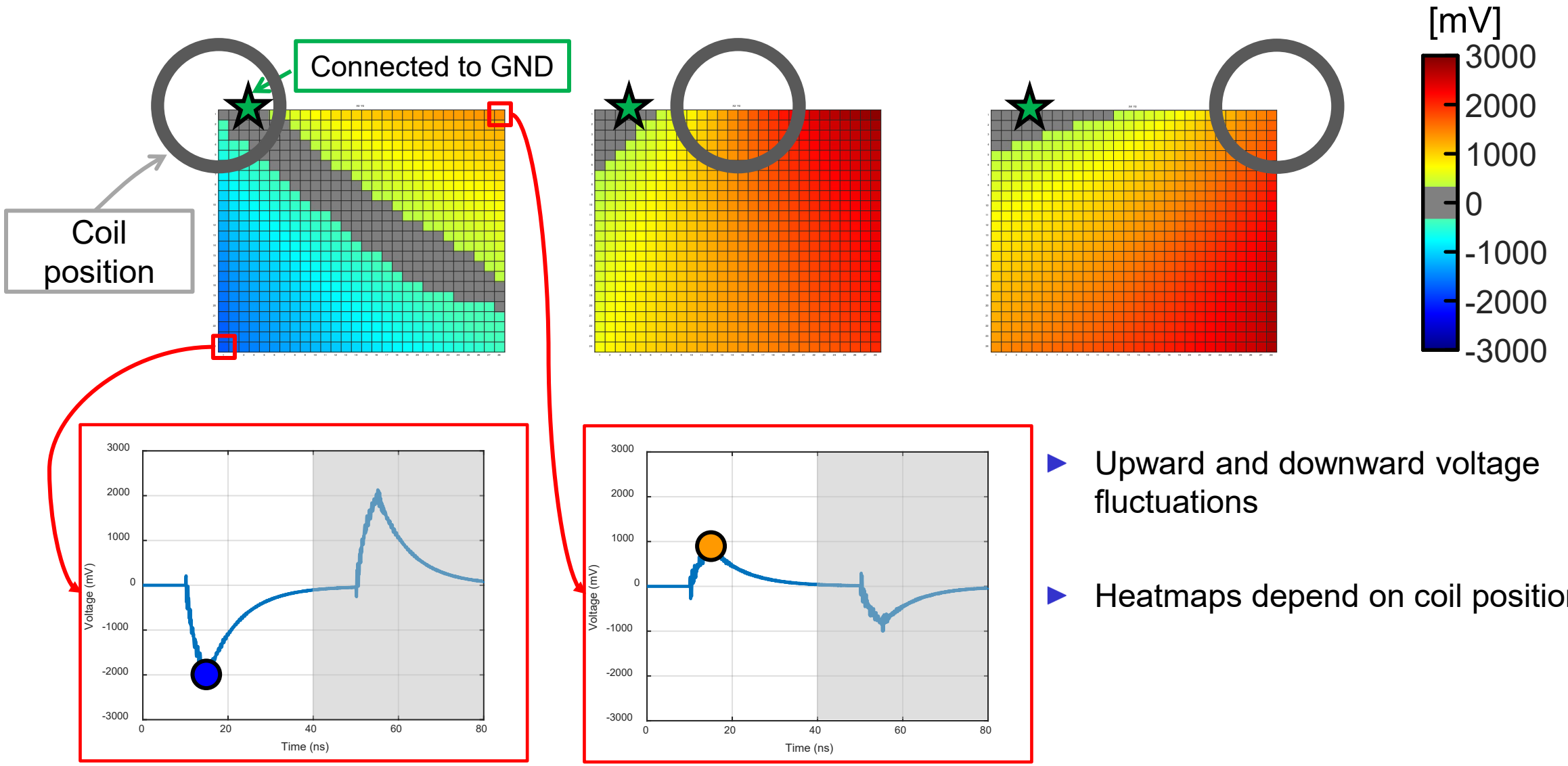
- Simulation models built for EM field solver







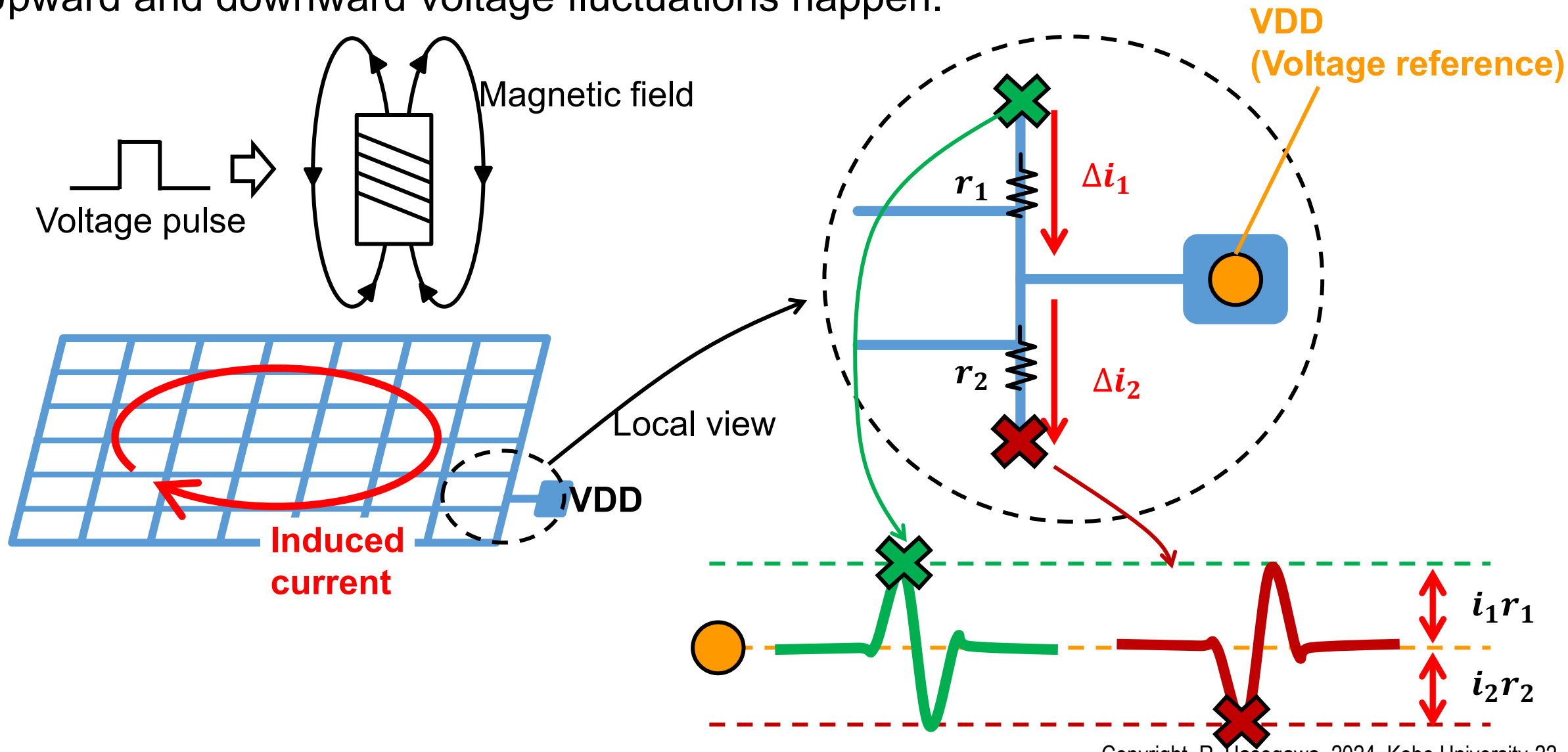
Simulation results



- Upward and downward voltage fluctuations
- Heatmaps depend on coil positions

Interpretation

- Upward and downward voltage fluctuations happen.



Conclusion

- EMFI voltage fluctuations visualized by on-chip measurements
  - ✓ Large drops in areas far from the coil
  - ✓ Both positive and negative voltage fluctuation
- Digital fault evaluation
  - ✓ On-chip voltage fluctuations and AES digital faults are correlated
- EM simulation trial
  - ✓ Positive and negative voltage fluctuations happen.

This work has been partly supported by JSPS KAKENHI Grant No. JP22H04999
and by SECOM Science and Technology Foundation