Re-Thinking Mixed-Criticality Architecture for Automotive Industry

Zhe Jiang, Shuai Zhao, Pan Dong, Dawei Yang, Ran Wei, Nan Guan, Neil Audsley

Confidential Restricted to Arm Board and Executives © 2020 Arm

Outline

- Mixed-Criticality System
- The State-of-the-Art in Academia
- Mismatches between Academia and Industry
- Z-MCS
- Conclusion

Confidential Restricted to Arm Board and Executives © 2020 Arm

Outline

- **Mixed-Criticality System**
- The State-of-the-Art in Academia
- Mismatches between Academia and Industry
- Z-MCS
- Conclusion

Confidential Restricted to Arm Board and Executives © 2020 Arm

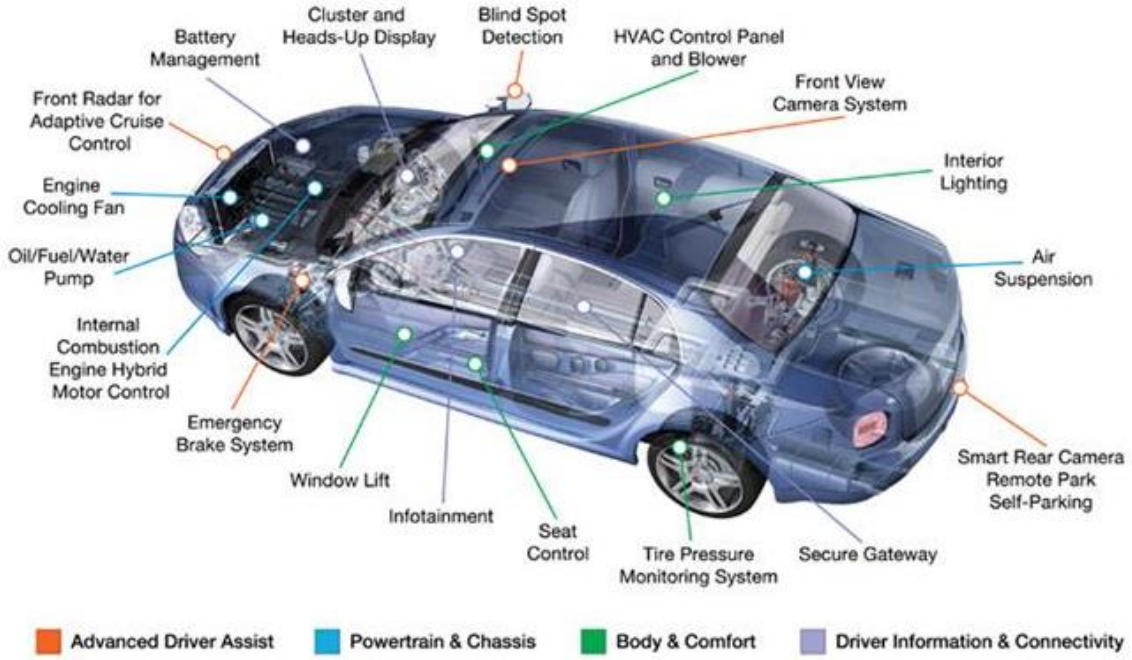
Safety-critical System

- In the last decade, the popularity of safety-critical systems has reached an unexpected height due to developments of Cyber-Physical Systems (CPS)
  - Autonomous systems (Automotive)
  - Industrial 4.0
  - Internet of Things (IOT)

Confidential Restricted to Arm Board and Executives © 2020 Arm

Mixed-Criticality System (MCS)

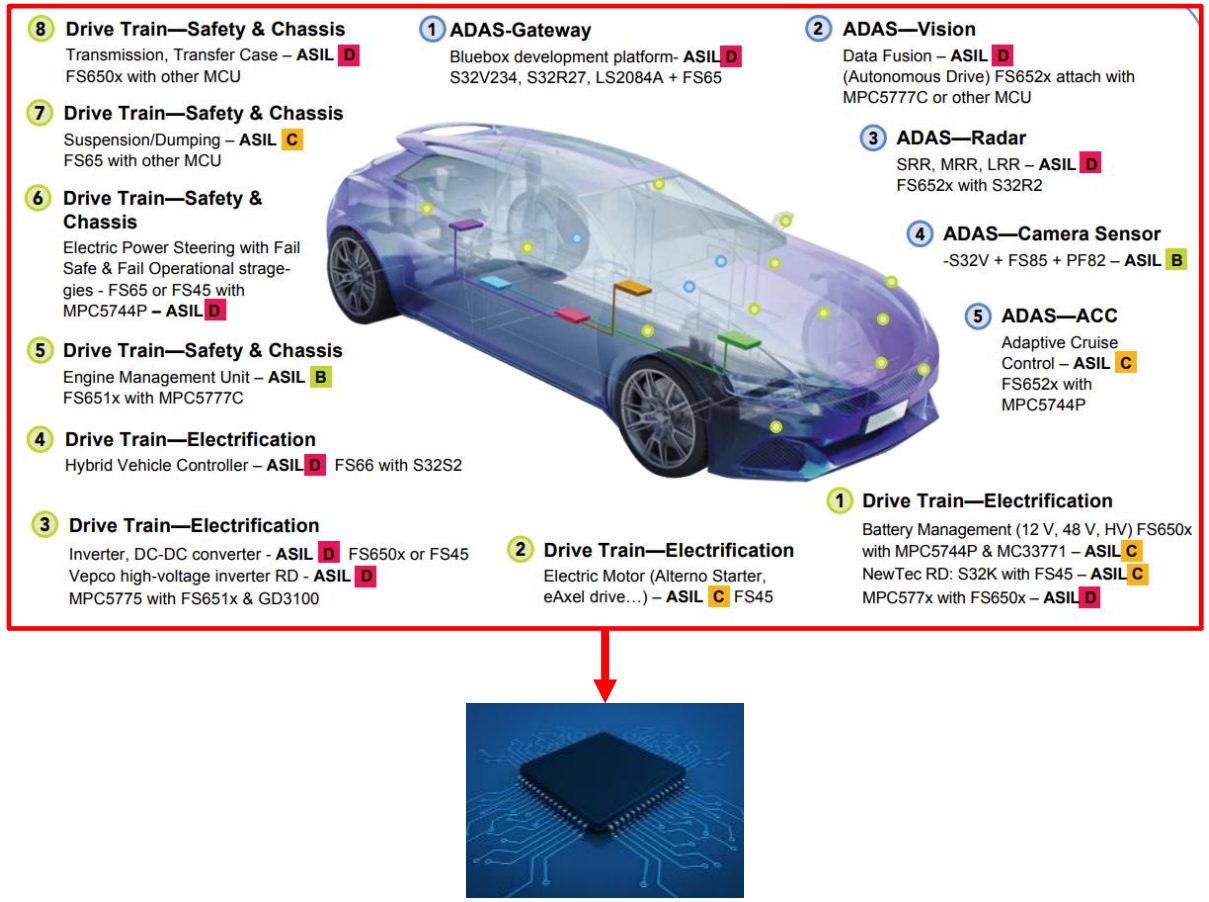
- In safety-criticality systems, integrating components with different levels of criticality onto a shared hardware platform has become increasingly important, i.e., Mixed-Criticality System (MCS)
  - *Criticality: (ISO26262-1:2018) one of four levels to specify the item's or element's necessary requirements of ISO 26262 and safety measures to apply for avoiding an unreasonable risk, with D representing the most stringent and A the least stringent level.*



Confidential Restricted to Arm Board and Executives © 2020 Arm

Mixed-Criticality System in Automotive

- With the diverse functionalities required by modern safety-critical systems and the rapid evolution of executed platforms.



Confidential Restricted to Arm Board and Executives © 2020 Arm

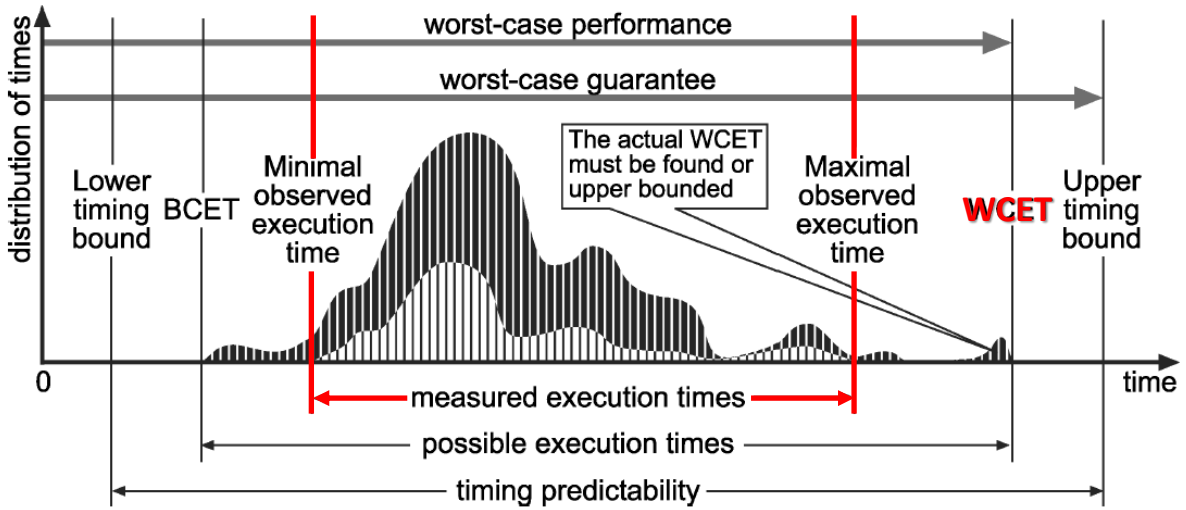
Outline

- Mixed-Criticality System
- **The State-of-the-Art in Academia**
- Mismatches between Academia and Industry
- Z-MCS
- Conclusion

Confidential Restricted to Arm Board and Executives © 2020 Arm

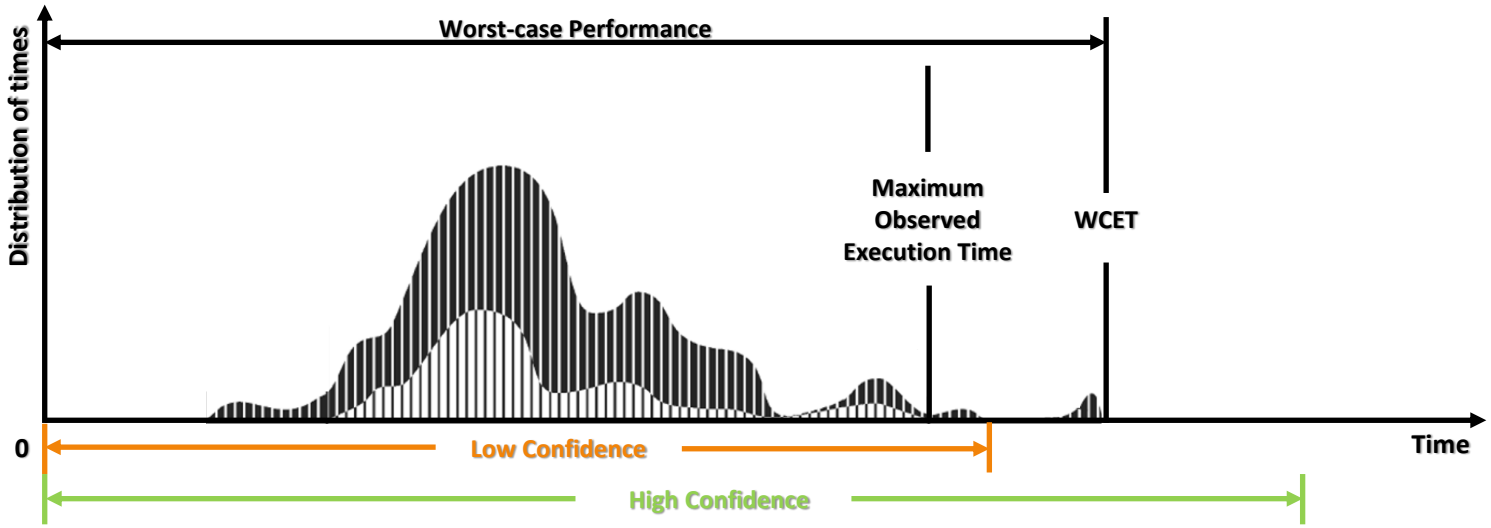
Real-time Requirements in MCS

- In MCS, meeting real-time constraints is always a key.
- To meet the requirement, acquiring the Worst-Case Execution Time (WCET) of each task is the first step.
  - However, it is unlikely to achieve the WCET of a tasks via measurement.



Confidential Restricted to Arm Board and Executives © 2020 Arm

Estimation of WCET in MCS



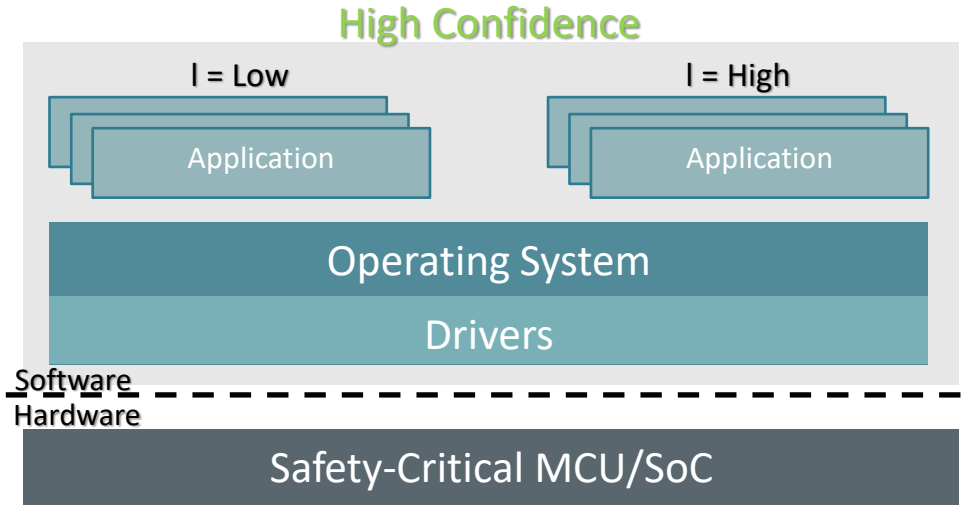
- In MCS, WECT is normally estimated with different level of confidence*:
- Low confidence: optimistic, saving system resource, but risky.
- High confidence:, pessimistic, safe, but wasting system resource.
- **How to allocate the shared resources effectively and keep the system safe if the key question in MCS (Academia).**

*More levels of confidence can be considered.

Confidential Restricted to Arm Board and Executives © 2020 Arm

MCS Models: SMC-no

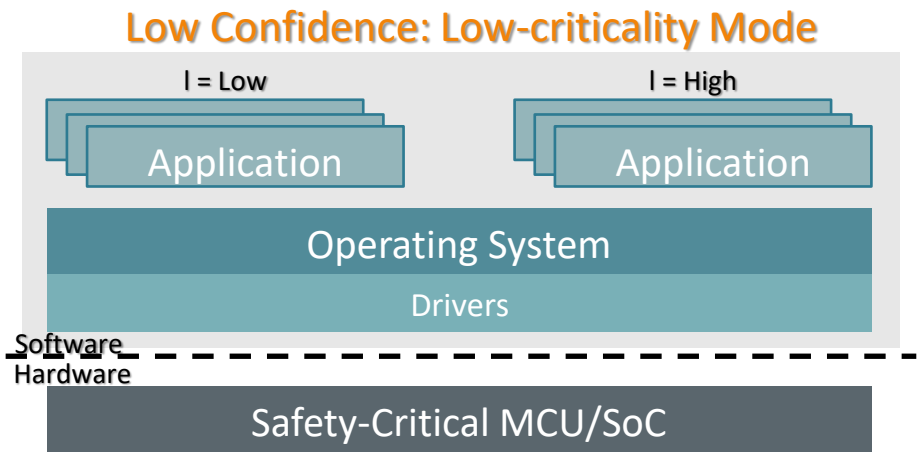
- In the earliest MCS model (i.e., SMC-no [1]), all the tasks used the high confident estimation of WCET.
  - The system is safe
  - Utilization of the resources is low

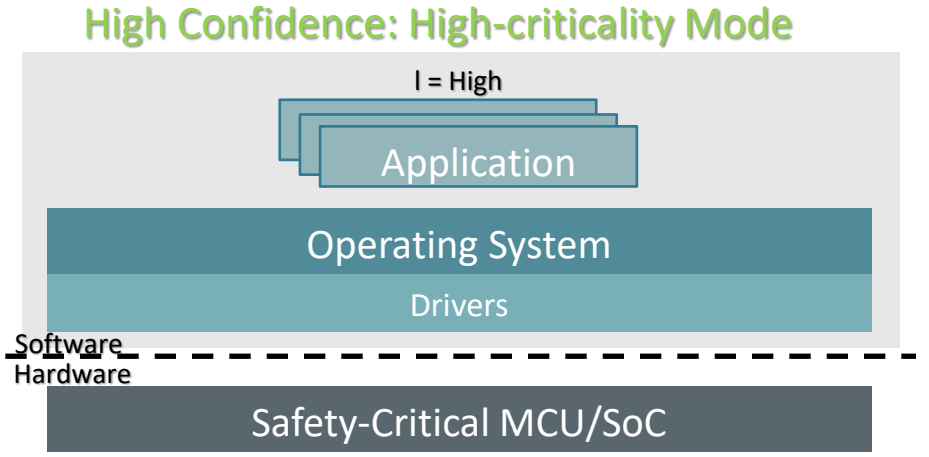


Confidential Restricted to Arm Board and Executives © 2020 Arm

MCS Model: AMC

- Adaptive resource management (i.e. AMC [2]) is an effective approach to address the issue, introducing different ***system mode***:
  - System first executes at the *low-criticality mode* (low confident WCET is used)
  - System goes to the *high-criticality mode* (high confident WCET is used), while meeting a predefined condition (e.g., over-run of a task)
  - In the high-criticality mode, low-criticality tasks are terminated.

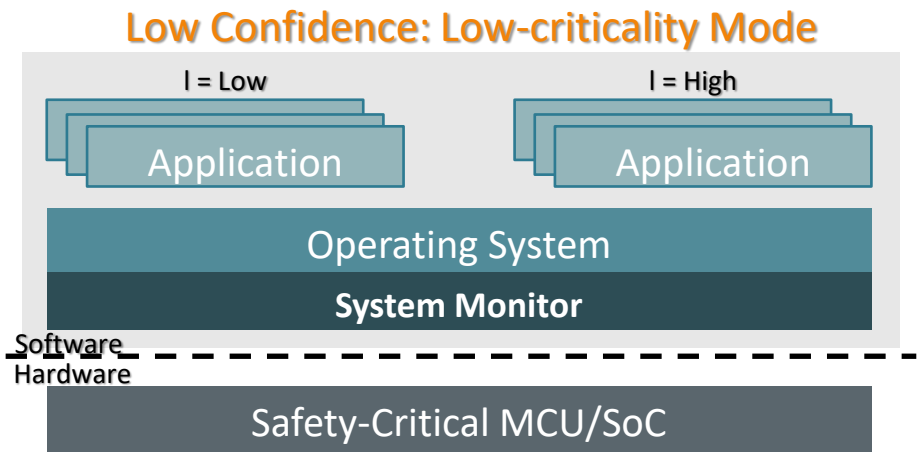


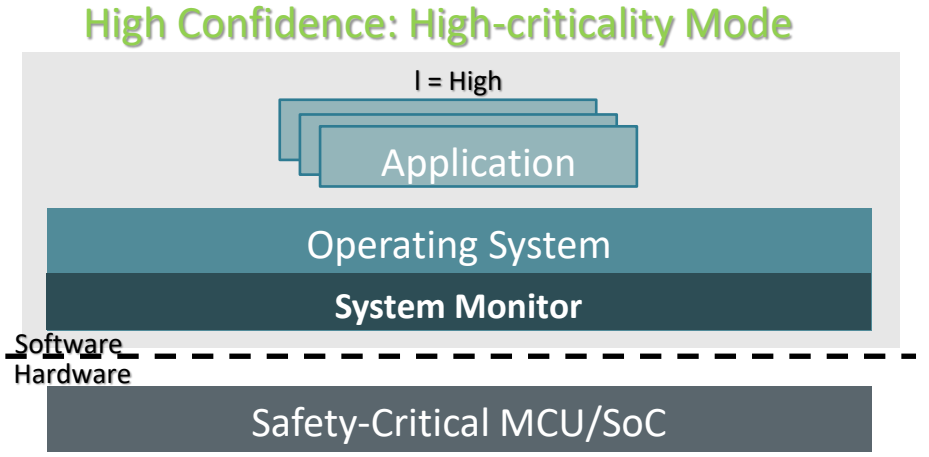


Confidential Restricted to Arm Board and Executives © 2020 Arm

MCS Model: AMC

- Adaptive resource management (i.e. AMC [2]) is an effective approach to address the issue, introducing different ***system mode***:
  - System first executes at the *low-criticality mode* (low confident WCET is used)
  - System goes to the *high-criticality mode* (high confident WCET is used), while meeting a predefined condition (e.g., over-run of a task)
  - In the high-criticality mode, low-criticality tasks are terminated.





Confidential Restricted to Arm Board and Executives © 2020 Arm

Outline

- Mixed-Criticality System
- The State-of-the-Art in Academia
- **Mismatches between Academia and Industry**
- Z-MCS
- Conclusion

Confidential Restricted to Arm Board and Executives © 2020 Arm

Mismatch 1: Graceful Degradation v.s. Mode Switch

- Mode Switch is the key strategy in MCS.
- In industry, different standards have different definitions on criticality level. However, the fundamental idea is same.
  - ISO26262 as an example

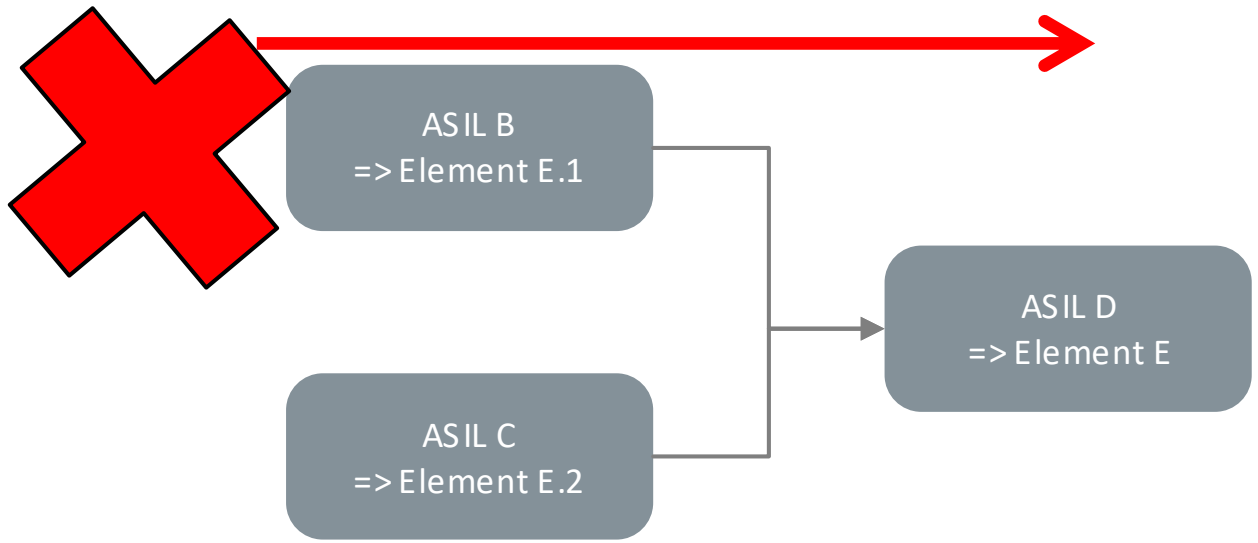
Severity	Exposure	Controllability		
		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B ← Keep
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A ← Kill
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

Confidential Restricted to Arm Board and Executives © 2020 Arm

Mismatch 2: Dependency

- If a high-criticality tasks is dependent on a low-criticality task, killing low-criticality tasks will cause the corruption of the high-criticality task.

- And further corrupt the whole system.



Confidential Restricted to Arm Board and Executives © 2020 Arm

Mismatch 3: Partitioning and Isolation

- Isolation between different criticality tasks is regulated by all the safety-related standards. **This is always the essential requirements**.
  - *ISO26262: If freedom from interference between elements implementing safety requirements cannot be argued in the preliminary architecture then the architectural elements shall be developed in accordance with the highest ASIL for those safety requirements*

- Isolation includes: Timing isolation, space isolation, and fault isolation.

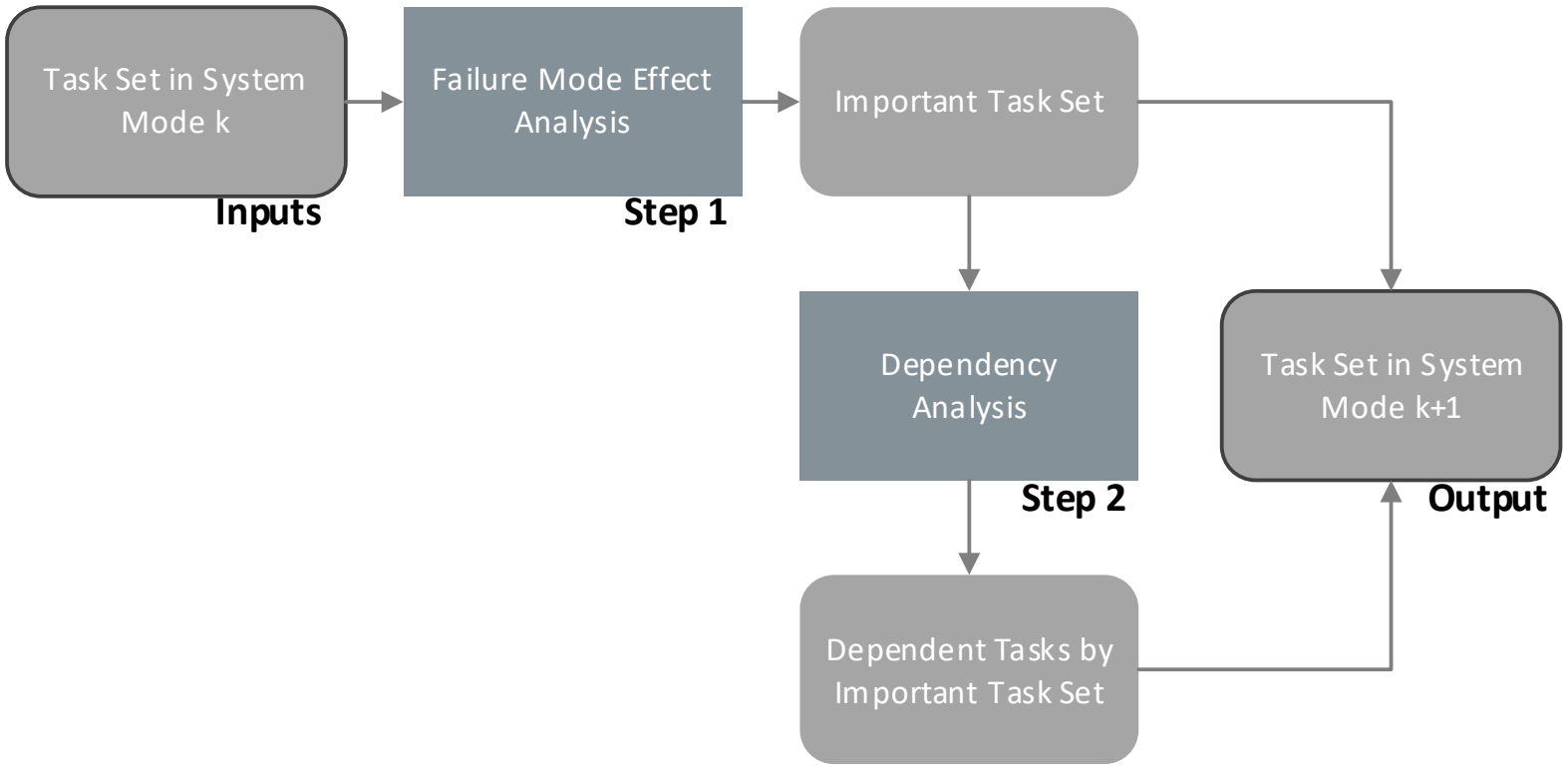
Confidential Restricted to Arm Board and Executives © 2020 Arm

Outline

- Mixed-Criticality System
- The State-of-the-Art in Academia
- Mismatches between Academia and Industry
- **Z-MCS**
- Conclusion

Confidential Restricted to Arm Board and Executives © 2020 Arm

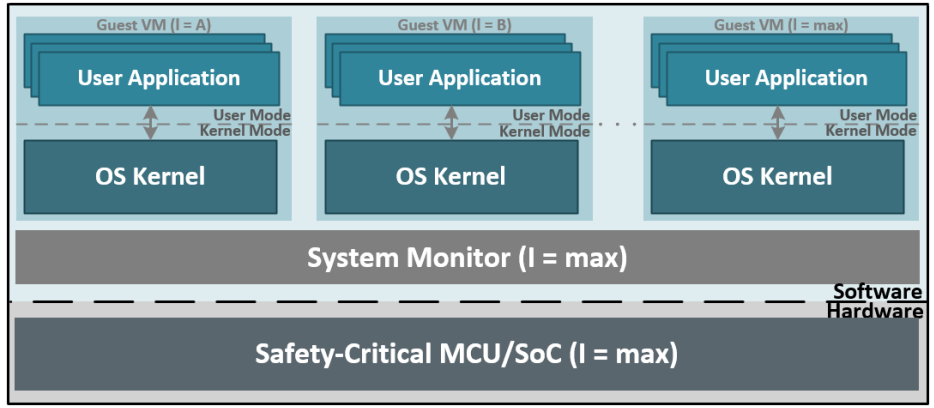
Solving Mismatches 1 & 2: Run-time Safety Analysis



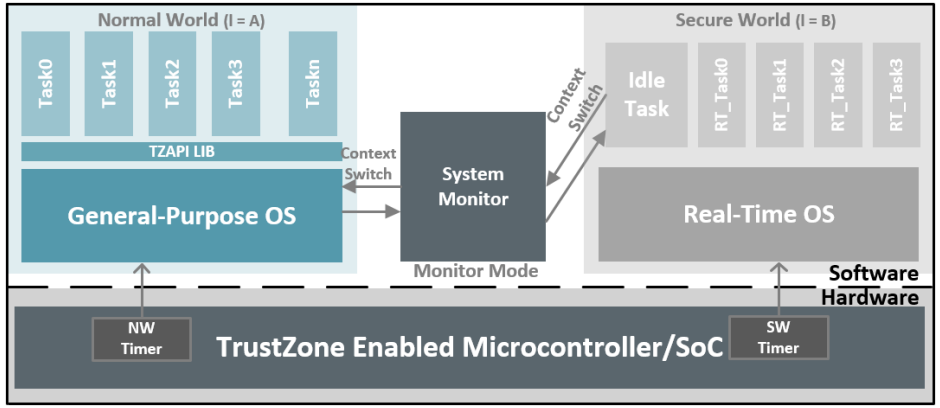
Confidential Restricted to Arm Board and Executives © 2020 Arm

Solving Mismatch 3: Three System Architectures

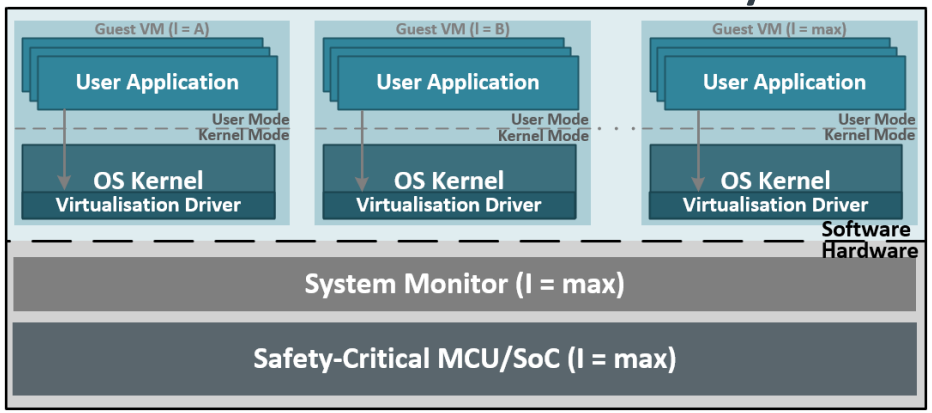
- Software virtualized System



- ARM TrustZone System



- Hardware virtualized System



Confidential Restricted to Arm Board and Executives © 2020 Arm

Outline

- Mixed-Criticality System
- The State-of-the-Art in Academia
- Mismatches between Academia and Industry
- Z-MCS
- **Conclusion**

Confidential Restricted to Arm Board and Executives © 2020 Arm

Conclusion

- MCS is a key direction in safety-critical systems, it is well studied in academia, but still has gaps in industry.
- In this paper, we proposed run-time safety analysis and three system architectures to solve the gaps.
- The main intention of this paper is to encourage tighter connections between academia and industry.

Confidential Restricted to Arm Board and Executives © 2020 Arm

arm

Thank You
Danke
Merci
谢谢
ありがとう
Gracias
Kiitos
감사합니다
धन्यवाद
شكرًا
ধন্যবাদ
תודה

Confidential Restricted to Arm Board and Executives © 2020 Arm