Challenges of meeting diversity requirements in Aviation Security Standard ED203A/DO-356A

Adrian Waller and Naomi Farley

adrian.waller@uk.thalesgroup.com
naomi.farley@uk.thalesgroup.com
www.thalesgroup.com

HICLASS Project Overview

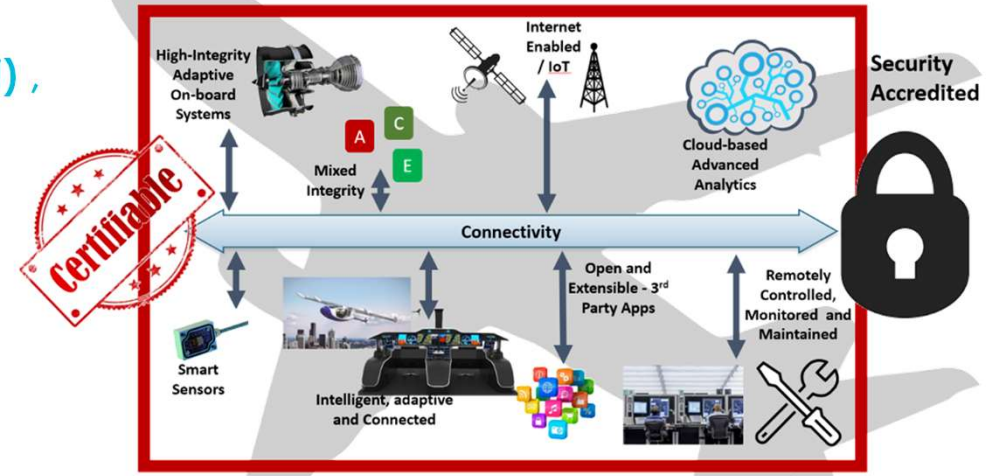
> This work was performed as part of the 'HICLASS' Project

> Innovate UK/ATI co-funded project from 2019-2023

> Lead Partner: Rolls-Royce

> Funded Partners: **AdaCore**, Altran UK (now Cap-Gemini) , BAE Systems, Callen-Lenz, Cobham, Cocotec, D-RisQ, **General Dynamics UK**, **GE Aerospace**, University of Oxford, Rapita Systems, Rolls-Royce, **University of Southampton**, **Thales**, Ultra-CEMS, University of York

UK industry to lead in the build and support of the most complex, connected, cyber-secure avionic systems in the world...



....a pan-industry effort involving UK industry and academic leaders in safety-critical aerospace systems development

{OPEN}

Context – Security Assurance in Aviation

> Safety assurance standards are mature and well understood in aviation

- e.g. DO-178C for "Software Considerations in Airborne Systems and Equipment Certification"

> Security assurance standards have been developed in the last ~10 years but are only recently starting to be applied and have only recently become an acceptable means of compliance

- Focus of this talk is on the design standards:
  - ED-202A/DO-326A ("Airworthiness Security Process Specification")
  - **ED-203A/DO-356A ("Airworthiness Security Methods and Considerations")**
- Focus of this talk also on software security assurance aspects of these standards, but we will consider more general issues

{OPEN}

Context – Security Assurance in Aviation

> **As companies are starting to apply these security standards in practice, difficulties in understanding or meeting these are being identified**

> **HICLASS project performed a cross-industry assessment of areas where more clarity is needed**

> **One area identified is requirements related to having and demonstrating 'independence, diversity and isolation' of Security Measures:**

- Independence: "Able to provide full functionality and effectiveness without inputs or other support from another Security Measure"
- Diversity: "Security Measures are more diverse if they have less functionality, technology and code in common."
- Isolation: "Isolation is the existence of physical and/or logical boundaries between Security Measures that prevent compromise or failures from propagating."

> **Diversity in particular was perceived as difficult to understand and apply**

- Focus of this talk
- Focus is also on use of diversity in certification of a specific product according to the aviation standards. Other uses of diversity (e.g. population diversity for resilience) are not covered, and subject to different assessment

Why Diversity?

> In safety, adopting multiple, diverse systems to protect against a single point of failure is well known and understood (in general…)

- …however, software diversity is less well understood and applied
- The aim is that the same failure is unlikely to occur in the diverse systems at the same time

> The security standards specify similar diversity requirements to safety, but note that we also need to consider deliberate attacks as well as faults leading to failures

- Aim to reduce the risk of the same zero day vulnerability being exercised by an attacker on multiple Security Measures used to protect against a given Threat Scenario
- Indeed, it would be beneficial to be able to quantify the reduction of risk through introducing diversity

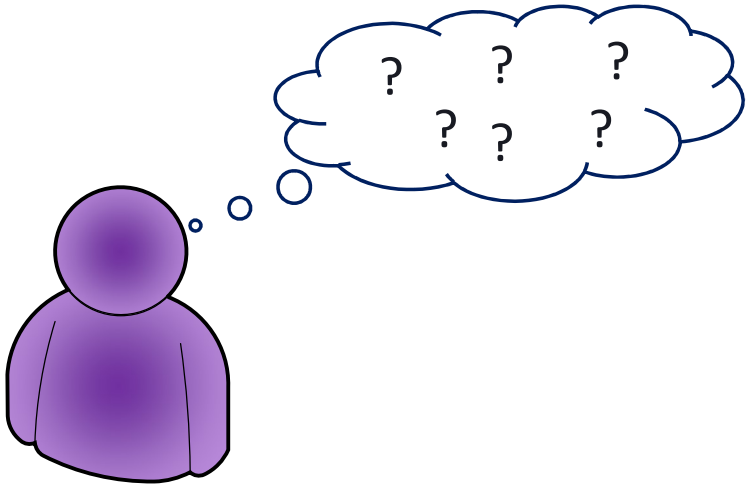
{OPEN}

Details from Standards

> From ED-203A/DO-356A:

- Two Independent, Diverse and Isolated Security Measures are required for any Threat Scenario that leads to a Threat Condition effect of severity Catastrophic (section 4.4.1 of ED-203A/DO-356A)
- Requirement to analyse the degree of Independence, Diversity and Isolation in any Security Measures as part of a "Security Measure Common Mode Analysis" (section 3.5.1 of ED-203A/DO-356A)

> ED-203A/DO-356A provides only limited guidance on how to do this



{OPEN}

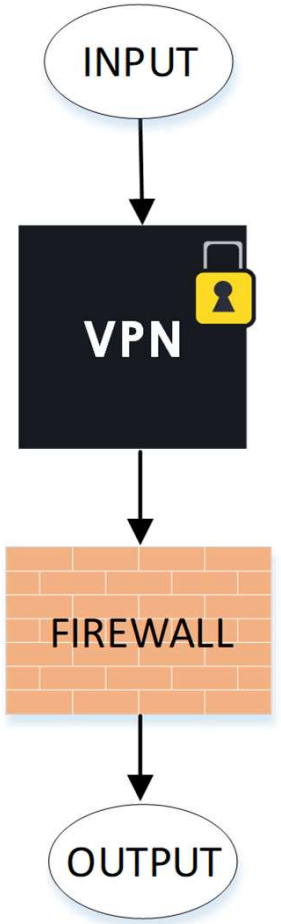
When does diversity apply in ED-203A?

1. Diversity in Security Measures adopted for 'defence in depth'

- If multiple Security Measures exist on an attack path in a Threat Scenario, then according the ED-203A, the degree of diversity between these should be used in determining the level of threat as part of the security risk assessment
- Intuition: If the degree of diversity between the Security Measures is high, then…
  - Risk of unknown vulnerability being discovered in each Security Measure should be relatively low
  - All Security Measures would need to be compromised independently to lead to a successful attack

> Open Questions:

- How can the required level of diversity between Security Measures be specified?
- How can the level of diversity be measured?



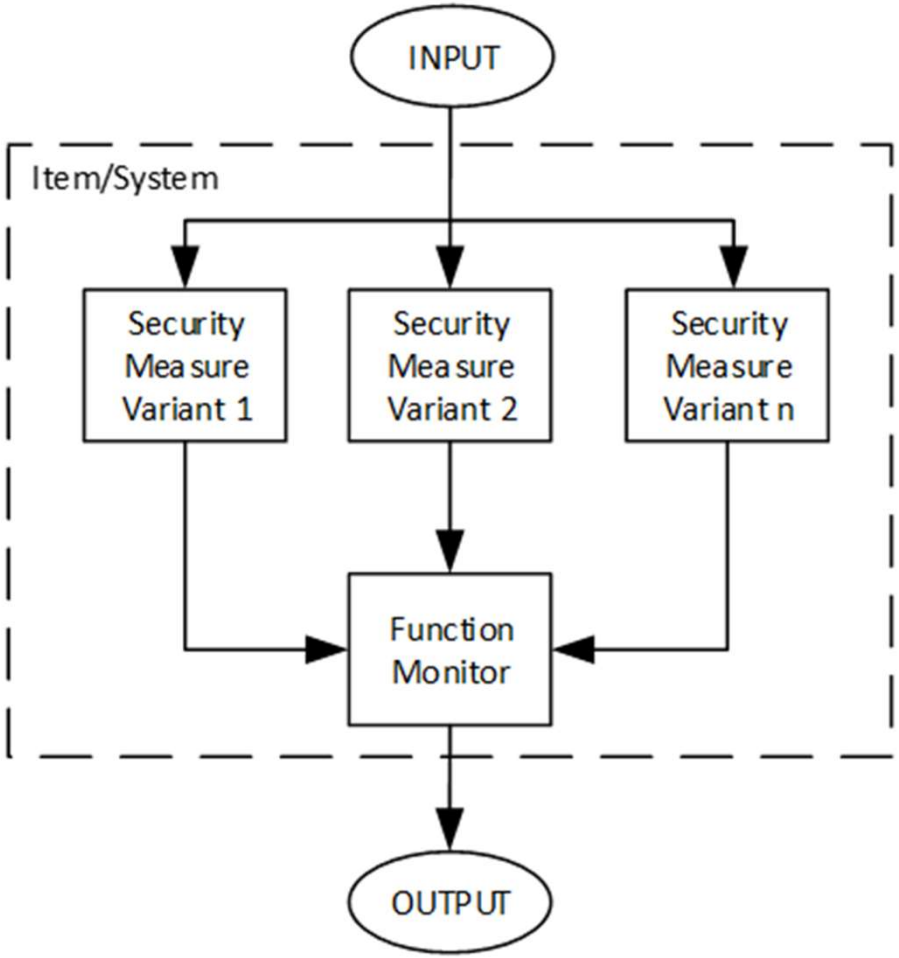
{OPEN}

When does diversity apply in ED-203A?

2. Deliberately introduce redundancy

- Additional, redundant, diverse Security Measures may be added to a given Threat Scenario if the risk is too high

> **Leads to questions: 'how and where should I add redundant, diverse, Security Measures to enhance security?'**



{OPEN}

Programme and practicality aspects

> Cost of applying diversity is a major consideration

- Where to apply diversity may thus be more focussed around critical security functionality and where compromise or failure is least acceptable

> Because of concerns around cost and practicality, diversity at system or aircraft level is unlikely.

> Diversity should not be added for diversity's sake as this can lead to more threats (e.g. greater attack surface – complexity is the enemy of security)

> Given the above, diversity may be best targeted at areas such as:

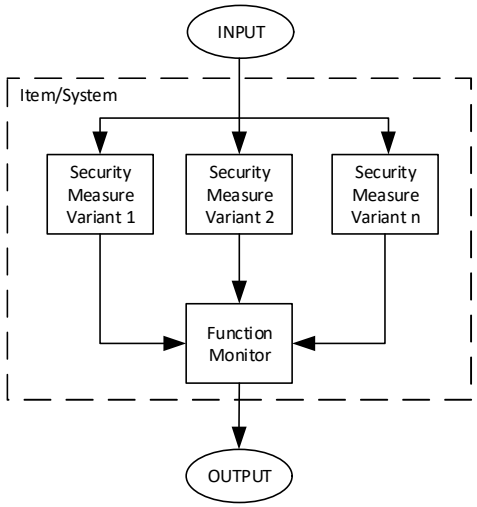
- Critical software functions and supporting infrastructure
- During system building and testing (e.g. use of different configurations and test tooling/approaches).

{OPEN}

Architectures using Diversity to Enhance Security

> Diversity can be targeted in different architectures adopting multiple Security Measures.

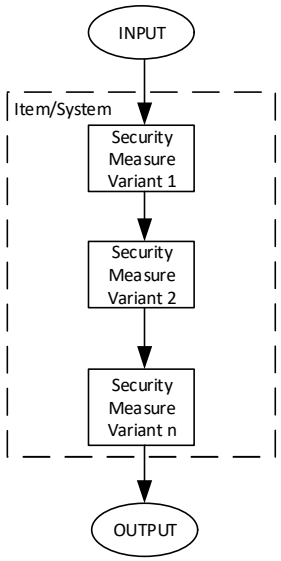
Security Measures in Parallel (e.g. for availability and integrity assurance)



Diversity of:

- Implementation
  - e.g. different software libraries used

Security Measures in Series (e.g. for integrity assurance, 'defence in depth')

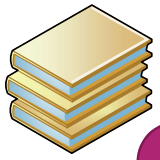


Diversity of:

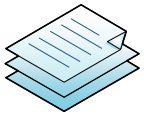
- Algorithm
  - e.g. ECDSA vs. RSA for digital signatures
- Implementation
  - e.g. two different software libraries
- Measure, with same goal
  - e.g. for integrity, content check function vs. hash check
- Measure and goal
  - E.g. content check function for integrity and digital signature for authentication

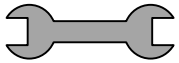
{OPEN}

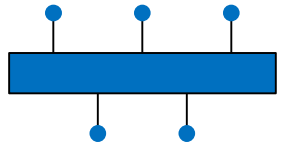
Methods for Diversity



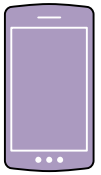
Software

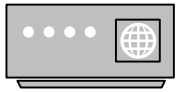


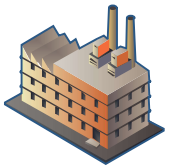




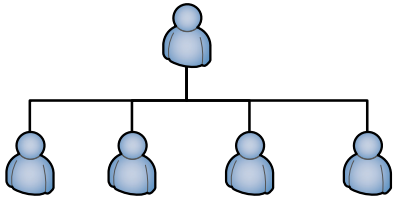
Hardware





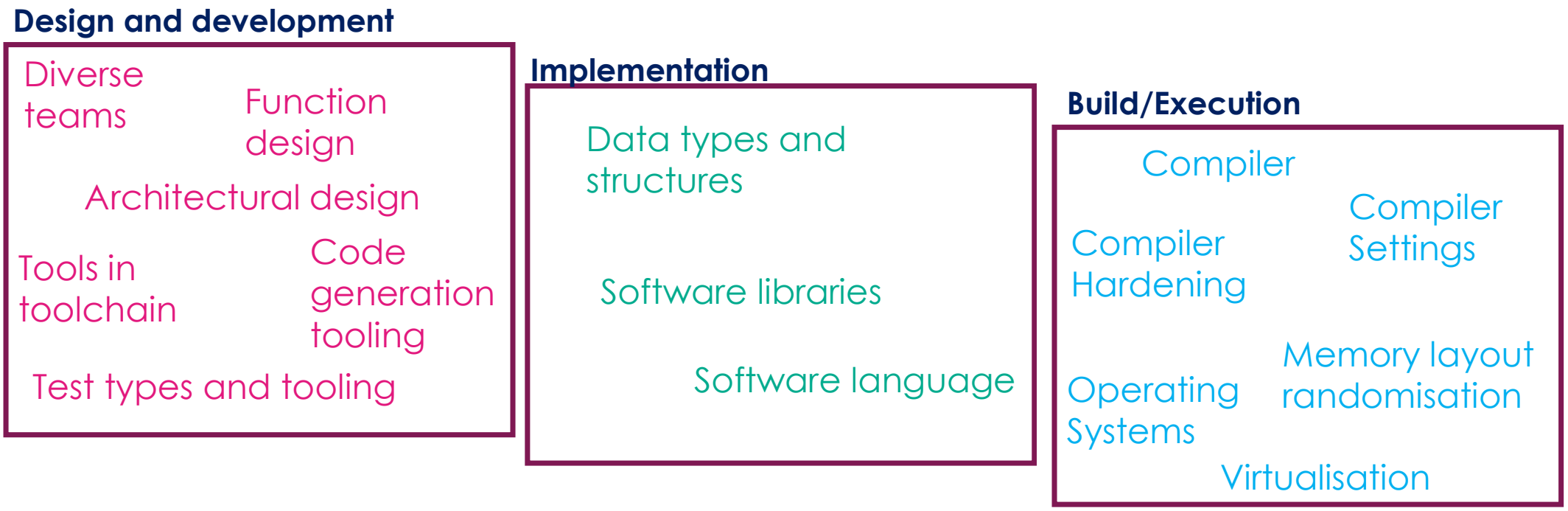


Other Aspects



Methods for Diversity (Software)

> **Examples of potential areas to apply diversity for software are shown below:**

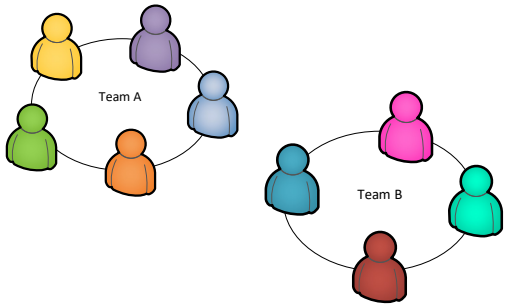


{OPEN}

Methods for Diversity (Software)

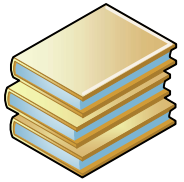
> Diverse Teams

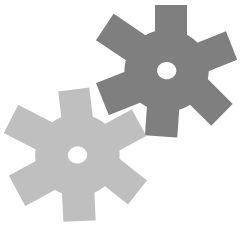
- Cost of using and managing multiple teams can be prohibitive
- Do they actually produce diverse software?



> Software Libraries

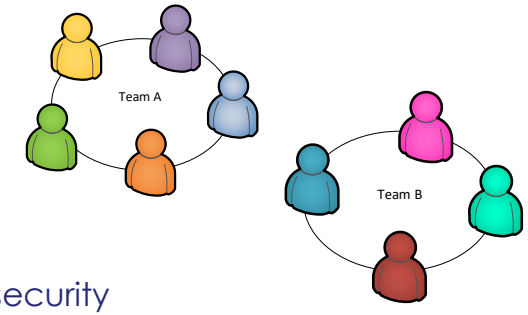
- Diversity could reduce the risk of the same vulnerability impacting multiple Security Measures
- However, how diverse in practice?
- Use of diverse libraries is discouraged if a lack of reputable/assured options exist





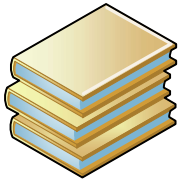
{OPEN}

Methods for Diversity (Software)



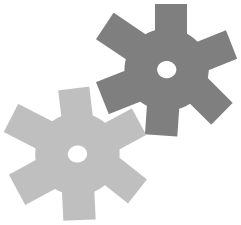
> Software Languages

- Need to consider how diverse these are in practice, i.e. whether these may be vulnerable to same/similar vulnerabilities in practice (e.g. memory faults)
- Using multiple languages may lead to greater complexity and thus have a negative impact on security assurance
- Selecting to use language(s) that are memory safe (e.g. Rust), formally verifiable (e.g. Spark) may be preferred from a security assurance aspect



> Compiler/Compiler Settings

- Reduce risk of vulnerabilities in a compiler impacting multiple Security Measures
- Different options can lead to very different implementations
- Need to ensure options do not have a negative impact on safety or security



{OPEN}

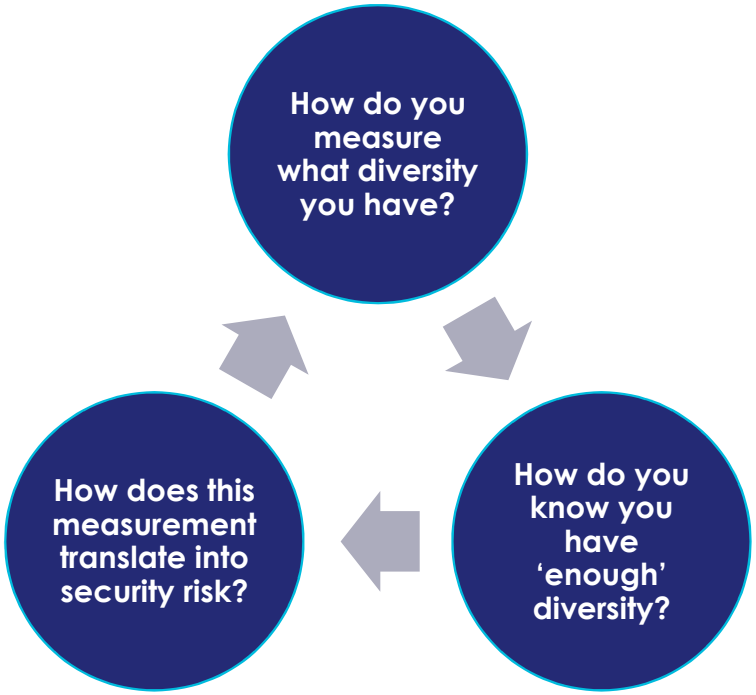
Methods for Diversity (Hardware)

> Key areas where hardware diversity may be considered are:

- Diversity of processor (e.g. type, manufacturer) and instruction sets used
- Multi-processor vs. Multi-core processor
- Diversity of choice of peripherals, interface devices, drivers
- Diversity of memory/storage type (e.g. SRAM, Flash, Hard Disk Drives etc.)
- Diversity of circuit-level designs (including layouts) and timings

{OPEN}

Quantifying Diversity



> A hard problem to do this objectively

> Best practice, patterns, guidelines etc. could be needed instead, but how do we develop these?

{OPEN}

Quantifying Diversity

- Requirement to demonstrate diversity motivates the need for a framework to support decision making process (e.g. on where to add diversity)
- Initial exercise performed as part of HICLASS project to understand what the framework should capture, but significant further work needed to mature this!

Ref. No.	Level	Diverse Aspect	Diversity Grading (Low to High/1-10)	Mitigates (Security)	Security Risk Severity (Low to High/1-10)	Difficulty to exploit (Low to High/1-10)	Remarks	Diversity Factor (For example, could be ((Grade / Severity) x Difficulty)
1	Item	Software language	6	Code weaknesses, coding errors	8	3	Depends how dissimilar the languages are	2.25
2	System / Item	Software compliers	4	Compiler defects Different object code	6	4		2.6
3	All	Development environment	7	Subversive attacks, undetected malware infection	8	4		3.5
4	All	Verification tools (automated)	6	Verification errors	8	N/A?		And so on…
5	All	Human developers	6	erroneous design assumptions	7	5	Independent development teams	

{OPEN}

Example of Poor Use of Diversity – Back to Back Firewalls

> In the shown example, diversity has been added through adopting two diverse firewalls: a network layer firewall and a Web Application Firewall (WAF)

- Note however that this is unlikely the best area to target diversity in this example and is likely to be costly to get right and effectively manage

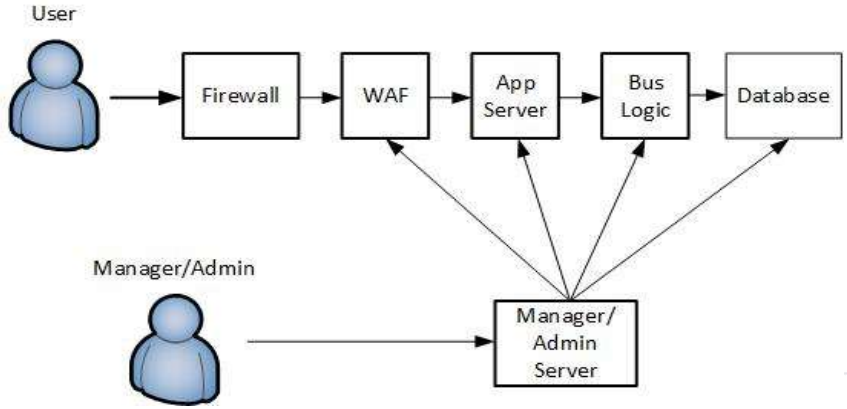
> An attacker who can compromise the Manager/Admin Server can get around any additional protection this brings.

- Thus, cost of adding diversity has not reduced this threat.
- Effort is best spent on getting policy/management right at a single firewall than on implementing diversity in these
- All attack paths (and risks of these) should be considered as to identify where to prioritise efforts.

Reference:

NCSC, Security architecture anti-patterns,

https://www.ncsc.gov.uk/whitepaper/security-architecture-anti-patterns



{OPEN}

Alternative arguments to Diversity

- In practice, it may be impractical (e.g. due to cost) or undesirable to apply diversity (e.g. negative, unknown, or no impact on security or safety)
- Hence, alternative arguments when diversity is not applied may be considered, e.g.:

Additional assurance achieved for existing, non-diverse measures

Adopt additional mechanisms to detect faults

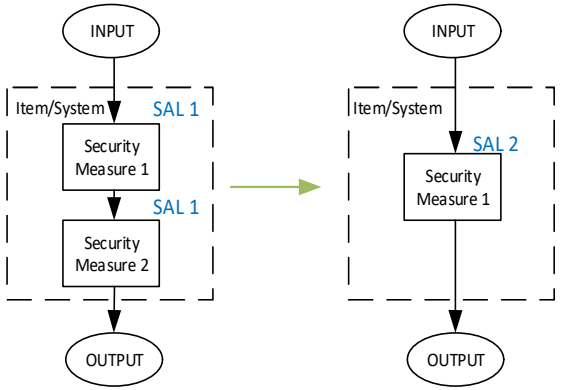
Enhanced arguments that the risk of a threat/attack is acceptable

{OPEN}

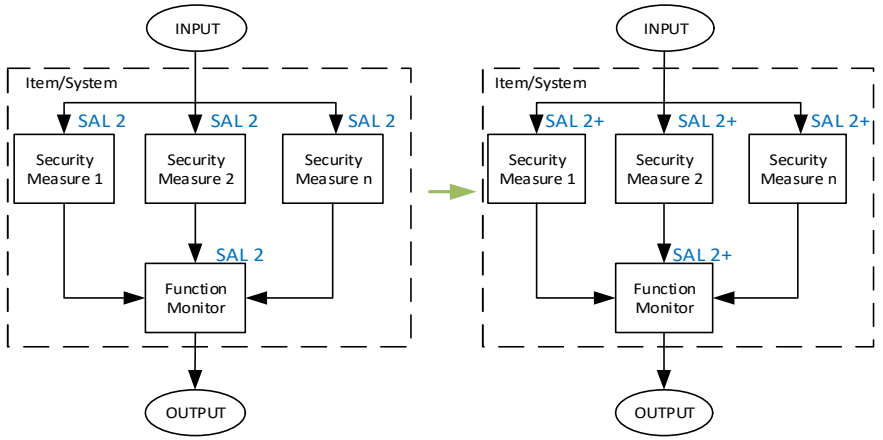
Alternative arguments to Diversity

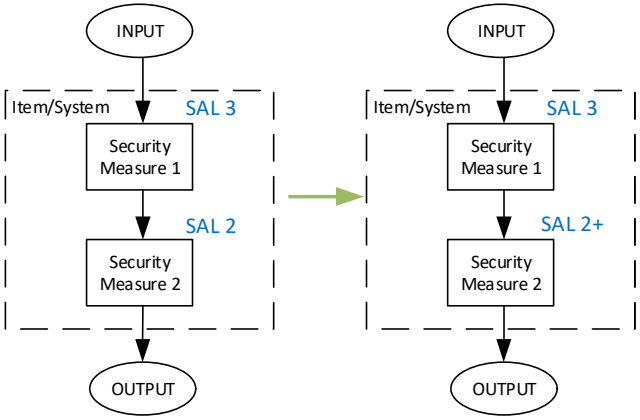
> Additional assurance for non-diverse measures

- Single Security Measure with a higher security assurance level
  - Could be a more assurable, cost-effective way of achieving resistance to zero-day vulnerabilities than applying two measures with lower assurance.



- Add additional security requirements of higher Security Assurance Levels. E.g. through demonstrating the use of formal methods, security refutation tests, etc.





{OPEN}

Alternative arguments to Diversity

> Additional mechanisms to reduce the presence of vulnerabilities

- E.g. use of software and/or compiler hardening techniques, adoption of memory safe software/hardware

> Classes of vulnerabilities (e.g. Common Weakness Enumeration) such as memory-based faults and/or common attack patterns (CAPECs) have been protected against

- E.g. through adoption of memory safe software/hardware

> Techniques have been adopted to detect potential attacks

- E.g. fault detection mechanisms, monitoring technologies
  - (Note: these mechanisms are likely to be Security Measures in their own right and would need to be secured and assessed appropriately)

> Enhanced analysis of identified risks to demonstrate they are acceptable

{OPEN}

Conclusions

> Diversity is extremely subjective

- It is hard to provide a reliable way to quantify Diversity.
- A useful framework to support the diversity assessment is highly desired.

> Diversity is something that deserves thought and consideration when developing such systems, to determine if it can reduce level of risk and provide additional security assurances

> Evidence of consideration and subsequent justification either way (to apply diversity or not) should be provided to show all aspects have been considered

> Ongoing conversation in standards groups about how to provide better guidance

{OPEN}