



Task 10: Reference Evaluation

Prepared by

ALI MMADI, PhD student-Midocean University





Research Issues (2)

Task 10

Introduction and link with the previous task

Hello,

For this 10th and final task, I will present a concise evaluation of the bibliographic references of a master's thesis. This analysis is crucial because references constitute the backbone of any scientific research.

Today, I will be evaluating a thesis on a hot current topic: "The security of connected and autonomous vehicles against coordinated cyberattacks." I will focus on two criteria: the clarity and diversity of the references, showing their direct impact on the overall quality of the research.



Presentation of the evaluated thesis

Title: "References: Autonomous Vehicle Safety - Critical Analysis"

Thesis topic: Assessment of systemic risks in autonomous vehicle fleets and development of a framework for detecting coordinated attacks.

Central issue: How to protect against attacks that simultaneously target multiple vehicles through their connected systems?

3: Analysis of the clarity of references

1. Reference Architecture:

Base (30%): Automotive standards (ISO 21434, SAE J3061) and regulations (UNECE R155)

Technical core (40%): Research on CAN bus, embedded systems, V2X communications

Advanced layer (20%): Artificial intelligence for anomaly detection

Top (10%): Sociotechnical studies on risk acceptance

2. Visible logical progression:

The references follow a clear path: standards → technical vulnerabilities → AI solutions → societal implications. This structure allows the reader to perfectly follow the reasoning.

3. Precise citations:

Each technical statement is supported by specific references: CAN bus attacks referenced via the work of Checkoway et al. (2011), anomaly detection via Miller & Valasek (2015).

4: Analysis of the Diversity of Sources

Identified strengths:

Balance of theory/practice:

Theory: IEEE articles on embedded system security

Practice: NHTSA (National Highway Traffic Safety Administration) reports on real incidents

Multidisciplinarity:

Automotive engineering (SAE standards)

Cybersecurity (BlackHat presentations)

Law and regulation (GDPR for vehicle data)

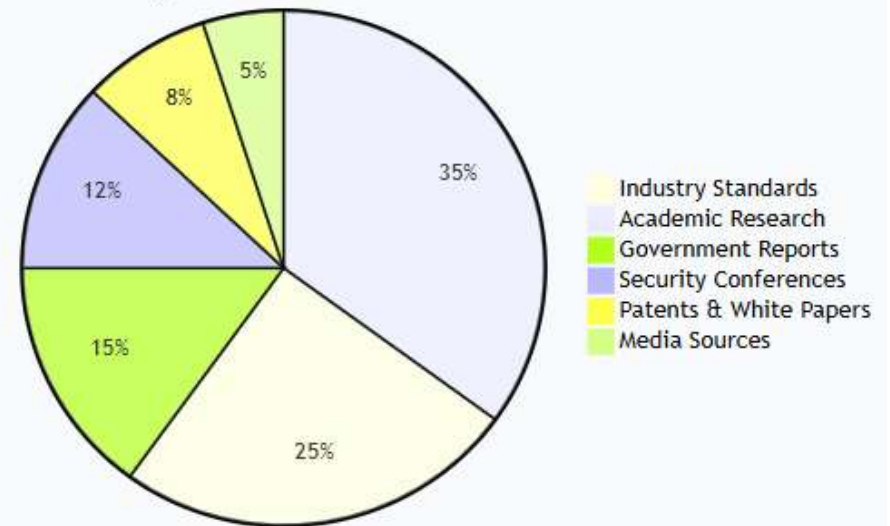
Ethics (European Commission on AI)

Controlled timing:

70% of references are less than 5 years old

But inclusion of foundational papers (e.g., 2010 CAN bus attacks)

Diversity of Referenced Sources



5: Gaps and possible improvements

Appearance	Highlights	Weak points	Impact
Modernity	Good coverage 2020-2023	Missing refs 2024 (very recent)	Limits innovation
Geography	Strong US/EU sources	Few Asian research studies	Incomplete vision
Types of sources	Academic and industrial	Insufficient open source	Lack of practice

Recommendation for improvement:

Add 10-15% of references from:
 GitHub repositories of open-source automotive projects (comma.ai, OpenPilot)
 Technical blogs from industry experts
 Databases of specific vulnerabilities (CVE related to automobiles)

6: Impact on research quality

How these references influence research:

On conclusions (Task 9 link):

Diverse references allow for nuanced conclusions

Example: Understanding that a technical solution must also be legally viable

On credibility:

Including ISO standards adds weight to the recommendations

Industry references ensure practical realism

On innovation:

The academic/industry mix stimulates innovative solutions

Cross-disciplinary references (law, ethics) enrich the analysis

7: Summary Evaluation Grid

Final thesis evaluation:

Clarity of references: 4.5/5

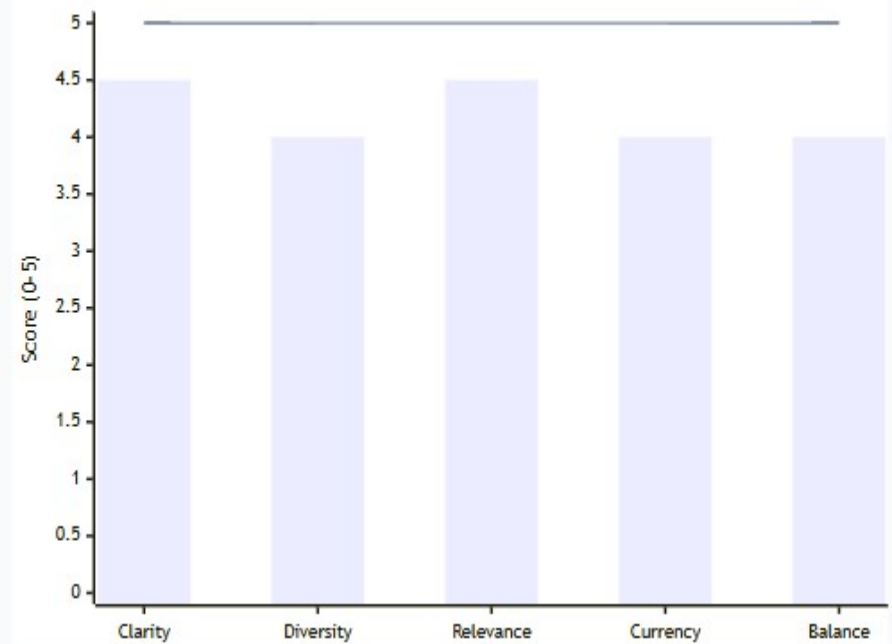
- ✓ Logical and hierarchical structure
- ✓ Accurate and relevant citations
- ✓ Progression from general to specific
- ~ A few poorly contextualized references

Diversity of references: 4/5

- ✓ Good academic/industry balance
- ✓ Multidisciplinary sources
- ✓ Generally good timing
- ✗ Lack of recent open-source references
- ✗ Geographic limitation (few sources from Asia)

Overall score: 8.5/10

Evaluation Metrics Across Categories



Conclusion

In conclusion, this assessment demonstrates that:
The quality of references is an amplifier of research quality. Clear and diverse references not only allow for the construction of a solid argument, but also open up innovative perspectives.

Essential skill: Knowing how to evaluate and select references is a fundamental skill for any cybersecurity researcher. It is what distinguishes an opinion from an evidence-based conclusion.

Final link to our course: Task 10 synthesizes our entire approach, as each previous step—from the theoretical framework to the recommendations—ultimately relies on the strength of the references used.

Thank you for your attention throughout these 10 research tasks.

Bibliographic References

1. APA Manual (2020) for formatting; Booth et al. (2016) for logical integration; Creswell (2018) for framework coherence.
2. Bennett & Checkel (2015) on triangulation; MITRE Sources list as a benchmark; Balance of NIST (authoritative), Academic (Knight & Nurse), Operational (CISA), and Community (OpenSSF) sources.
3. UC Berkeley CRAAP Test (Currency); Inclusion of recent conference briefings (Black Hat) and threat advisories (CISA).
4. Evaluation of whether sources like NIST SPs, academic papers, and open-source tools are used in a logically connected way to tell a complete story, as advocated in *The Craft of Research*.



مجموعة جامعة
الجميع الذكية
للتعليم القابضة

MIDOCEAN
UNIVERSITY



Thank You

