

AVCDL Products

- [AVCDL-Design-4.1] [Threat Modeling Report](#)
- [AVCDL-Design-4.2] [Ranked / Risked Threat Report](#)
- [AVCDL-Design-4.3] [Threat Report](#)

ISO 21434 Required Work Products

- [WP-09-02] Threat analysis and risk assessment
- [WP-09-03] Cybersecurity goals
- [WP-09-04] Cybersecurity claims
- [WP-09-05] Verification report
- [WP-15-01] Damage scenarios
- [WP-15-03] Threat scenarios
- [WP-15-04] Impact rating
- [WP-15-05] Attack paths
- [WP-15-06] Attack feasibility rating
- [WP-15-07] Risk values
- [WP-15-08] Risk treatment decision per threat scenario

WP.29 CSMS Requirements

- [7.2.2.1(a)] development phase CSMS
- [7.2.2.1(c)] post-production phase CSMS
- [7.2.2.2(b)] risk identification
- [7.2.2.2(c)] risk treatment
- [7.2.2.2(d)] verification of risk management
- [7.2.2.2(f)] risk assessment kept current
- [7.2.2.2.(g)] adaptable monitoring / response
- [7.2.2.3] timely risk management
- [7.3.3] critical element risk assessment
- [7.3.4] type risk protection
- [7.3.5] type risk countermeasures
- [7.4.1] periodic monitoring report

WP.29 CSMS Supplemental

- [7.2.2.1(b)] production phase CSMS
- [7.3.2] management of type

CMMC Applicable Practices

Level	Practice
1	none
2	RM.2.143
3	AU.3.049, AU.3.052, RM.3.144
4	none
5	AU.5.055