

Inspection Certificate

Certificate Number:	8123001551-002 V01, 26.09.2024
Inspection Item:	PCERT 1.4 a component of the tool suite PROVER CERTIFIER, including its documentation.
Manufacturer:	Prover Technology AB, Krukmakargatan 21, 118 51 Stockholm, Sweden Purchase order 2024-08-12.
Inspection Criteria:	EN 50128:2011 and EN 50716:2023, Tool class T2, applications up to SIL4
Objective of inspection:	Inspection of PCERT 1.4 regarding to the fulfillment of the tools-related requirements of EN 50128:2011 and EN 50716:2023, tool class T2, for application in projects up to SIL4. Assessment results are documented in following report*:
Inspection Reports:	Inspection Report about the Tool PCERT 1.4 according to the Requirements of EN 50128:2011 and EN 50716:2023, Chapter 6.7, for a Tool that is used for Verification (Tool Class T2) of Software with high Safety Criticality (up to SIL4), Report number 8123001551-001 V01, 26.09.2024, by TÜV NORD Systems GmbH & Co. KG
Inspection Result:	PCERT 1.4 is an offline software tool, i.e. it has no direct safety function like a control system, however, it could have influence on safety functions: The tool gets as input the specification (model) of a system and of its safety requirements, specified as proof obligations, in HLL (high level language). Based upon that input, a proof engine (not part of PCERT) is used by PCERT to get a correctness proof, confirming that the safety requirements are met by the system. In case of a successful proof by the proof engine, PCERT then checks the correctness of that proof by analyzing a proof log file. A wrong-side failure of PCERT (confirming that the proof obligations are fulfilled despite they are not fulfilled) could prevent detection of a dangerous error in the analyzed system. Due to the complexity of the system, that systematic error might not be detected by other means in the development process of the system. Based on the analyses documented in the above-mentioned report, the assessor confirms, that PCERT 1.4 fulfils the applicable requirements of EN 50128:2011 and EN 50716:2023 for tool class T2 and use for applications up to SIL4.
Terms of use and restrictions:	This certificate confirms that the tool is - with respect to the tool's own specification - sufficiently trustworthy to be used in a development process for software with integrity level up to SIL4 of EN 50128:2011 / EN 50716:2023. Using the inspection results as a generic foundation, the tool user must evaluate on its own whether the tool is appropriate for his specific development process and in particular for the needs of the specific application, including the safety integrity level.
* This certificate of assessment is valid only in combination with the complete report mentioned above and must not be contemplated isolated.	

TÜV NORD Systems GmbH & Co. KG

Große Bahnstraße 31, 22525 Hamburg, Germany

Business Field Rail
Control Systems

G. Krage

