What considerations apply when using a software tool in a safety-related development process if its behavior has not been previously evaluated?

When using a software tool in a safety-related development process where its behavior has not been previously evaluated, the ISO 26262 series of standards requires specific considerations to ensure functional safety. Such software tools shall comply with the requirements outlined in ISO 26262-8, Clause 11 (ISO 26262-8:2018, Clause 11.4.1).

The confidence in the use of software tools involves two main groups of activities: tool usage aspects and tool qualification aspects (ISO 26262-8:2018, Clause 11.2).

Key considerations include:

1. **General Requirement:** If activities or tasks required by ISO 26262 rely on the correct functioning of a software tool, and its relevant outputs are not examined or verified for the applicable process step(s), the tool shall comply with ISO 26262-8, Clause 11 (ISO 26262-8:2018, Clause 11.4.1).
2. **Planning of Usage:** The usage of the software tool shall be planned, including the determination of (ISO 26262-8:2018, Clause 11.4.4.1):
   - The identification and version number of the software tool (ISO 26262-8:2018, Clause 11.4.4.1 a)).
   - The configuration of the software tool (ISO 26262-8:2018, Clause 11.4.4.1 b)).
   - The use cases of the software tool, which describe user interactions and the subset of functionality applied (ISO 26262-8:2018, Clause 11.4.4.1 c)).
   - The environment in which the software tool is executed (ISO 26262-8:2018, Clause 11.4.4.1 d)).
   - The maximum ASIL of all safety requirements allocated to the item or element that could be directly violated if the software tool malfunctions and produces erroneous output (ISO 26262-8:2018, Clause 11.4.4.1 e)).
   - The methods to qualify the software tool, if required, based on the determined level of confidence and ASIL (ISO 26262-8:2018, Clause 11.4.4.1 f)).
3. **Information Availability:** To ensure proper evaluation and usage, the following information shall be available (ISO 26262-8:2018, Clause 11.4.4.2):
   - A description of the features, functions, and technical properties of the software tool (ISO 26262-8:2018, Clause 11.4.4.2).
   - The user manual or other usage guides (ISO 26262-8:2018, Clause 11.4.4.2).
   - A description of the environment required for its operation (ISO 26262-8:2018, Clause 11.4.4.2).
   - A description of the expected behavior of the software tool under anomalous operating conditions (ISO 26262-8:2018, Clause 11.4.4.2).
   - A description of known software tool malfunctions and appropriate safeguards, avoidance, or workaround measures (ISO 26262-8:2018, Clause 11.4.4.2).
   - Measures for the prevention or detection of malfunctions and corresponding erroneous output identified during confidence level determination (ISO 26262-8:2018, Clause 11.4.4.2).
4. **Evaluation of a Software Tool by Analysis:** The intended usage of the software tool shall be analyzed and evaluated to determine the Tool Confidence Level (TCL) based on two analysis classes (ISO 26262-8:2018, Clause 11.2, a); ISO 26262-8:2018, Clause 11.4.5.2; ISO 26262-10:2018, Clause 13):
   - **Tool Impact (TI):** The possibility that a malfunction of the tool can introduce or fail to detect errors in a safety-related item or element being developed (ISO 26262-8:2018, Clause 11.4.5.2). TI1 is selected if there is no such possibility, and TI2 in all other cases

(ISO 26262-8:2018, Clause 11.4.5.2).
    - **Tool error Detection (TD):** The confidence in measures that prevent the tool from malfunctioning and producing erroneous output, or that detect such malfunctions (ISO 26262-8:2018, Clause 11.4.5.2). TD1 is for high confidence, TD2 for medium confidence, and TD3 in all other cases (ISO 26262-8:2018, Clause 11.4.5.2).
5. **Tool Qualification:** If indicated by the determined Tool Confidence Level (TCL), appropriate qualification methods shall be applied to comply with both the TCL and the maximum ASIL of the safety requirements (ISO 26262-8:2018, Clause 11.2, b)). The rigor of requirements for the tool depends on its role, the risks related to tool failures, and the maximum ASIL of the item or element (ISO 26262-8:2018, Clause 11.2, b)). The qualification process and its documentation include specific information like unique identification, maximum TCL, predetermined maximum ASIL for use cases, configuration, and methods applied (ISO 26262-8:2018, Clause 11.4.6.2).
6. **Integration and Verification:** The software tool should be integrated into the user's environment according to the evaluation and qualification results. It must then be verified that the tool is working appropriately in the user environment, checking the validity of the predetermined TCL or qualification (ISO 26262-8:2018, Clause 11.2, a)).
7. **Prerequisites:** Before initiating tool usage, certain prerequisites must be available, including a safety plan (ISO 26262-2:2018, Clause 6.5.3), organization-specific rules and processes for functional safety (ISO 26262-2:2018, Clause 5.5.1), and applicable prerequisites of the phases of the safety lifecycle where the software tool is used (ISO 26262-8:2018, Clause 11.3.1).

Additional list of clauses:

- ISO 26262-2:2018, Clause 5.5.1
- ISO 26262-2:2018, Clause 6.5.3
- ISO 26262-8:2018, Clause 11.1
- ISO 26262-8:2018, Clause 11.2
- ISO 26262-8:2018, Clause 11.3.1
- ISO 26262-8:2018, Clause 11.4.1
- ISO 26262-8:2018, Clause 11.4.4.1
- ISO 26262-8:2018, Clause 11.4.4.1 a)
- ISO 26262-8:2018, Clause 11.4.4.1 b)
- ISO 26262-8:2018, Clause 11.4.4.1 c)
- ISO 26262-8:2018, Clause 11.4.4.1 d)
- ISO 26262-8:2018, Clause 11.4.4.1 e)
- ISO 26262-8:2018, Clause 11.4.4.1 f)
- ISO 26262-8:2018, Clause 11.4.4.2
- ISO 26262-8:2018, Clause 11.4.5.2
- ISO 26262-8:2018, Clause 11.4.6.2
- ISO 26262-10:2018, Clause 13

Correctness = 5P
Completness = 4P, -1P No mention of Change managment