List of Approved Tools and Components

Revision

Version 5
11/15/21 9:05 AM

SME

Charles Wilson

Abstract

This document describes the methodology to create tracking information for the software used in the creation of an autonomous vehicle.

Group / Owner

devops / Information Systems Security Developer

Motivation

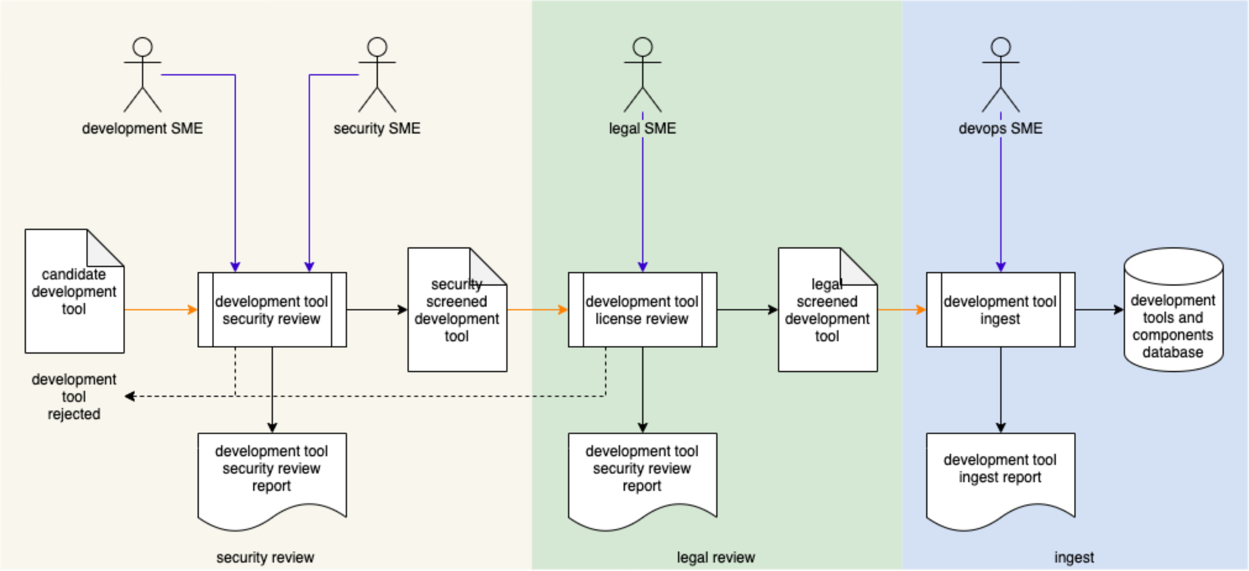
This document is motivated by the need to have formal processes in place tracking the tools and components used in creation of safety-critical, cyber-physical systems for certification of compliance to standards such as ISO 21434 and 26262. The case is made in the referenced document [1].

License

Overview

In order to ensure the security of the software to be produced, it is necessary to validate and enumerate the software used in its creation.

Below is the overview of the process leading to development tool / component ingest.

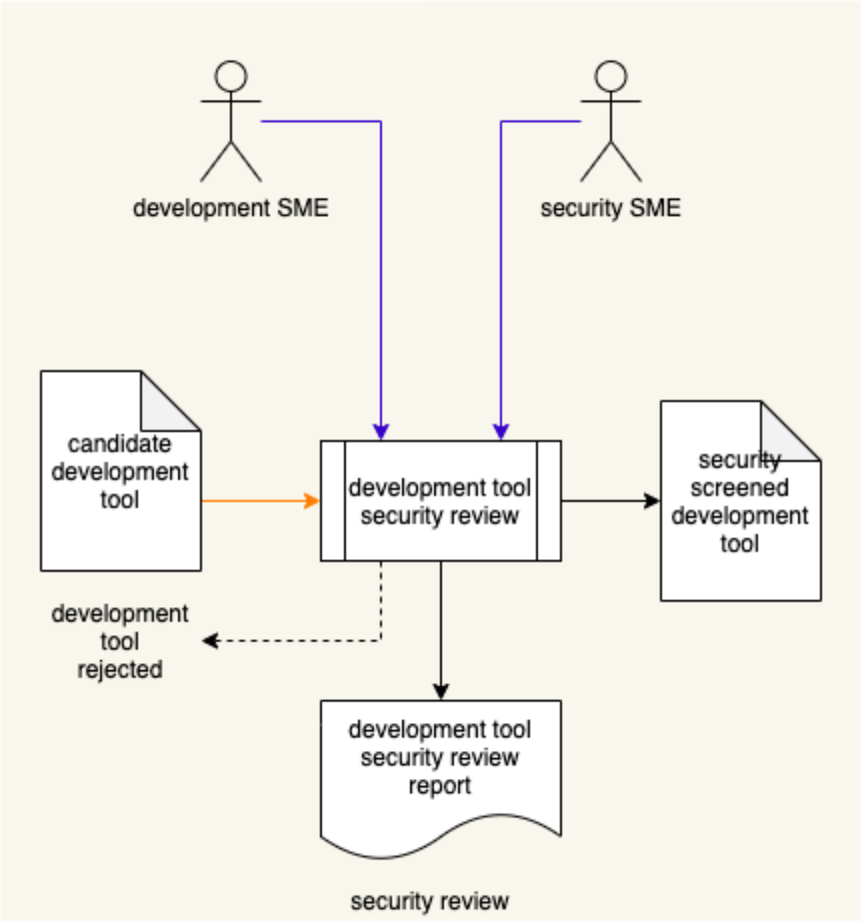

development SME
security SME
legal SME
devops SME
candidate development tool
development tool security review
security screened development tool
development tool license review
legal screened development tool
development tool ingest
development tools and components database
development tool rejected
development tool security review report
development tool security review report
development tool ingest report
security review
legal review
ingest

Note: In order to avoid constantly repeating the phrase "tool / component," **tool** is used to refer to either a **tool** or a **component**.

Process

Security Review

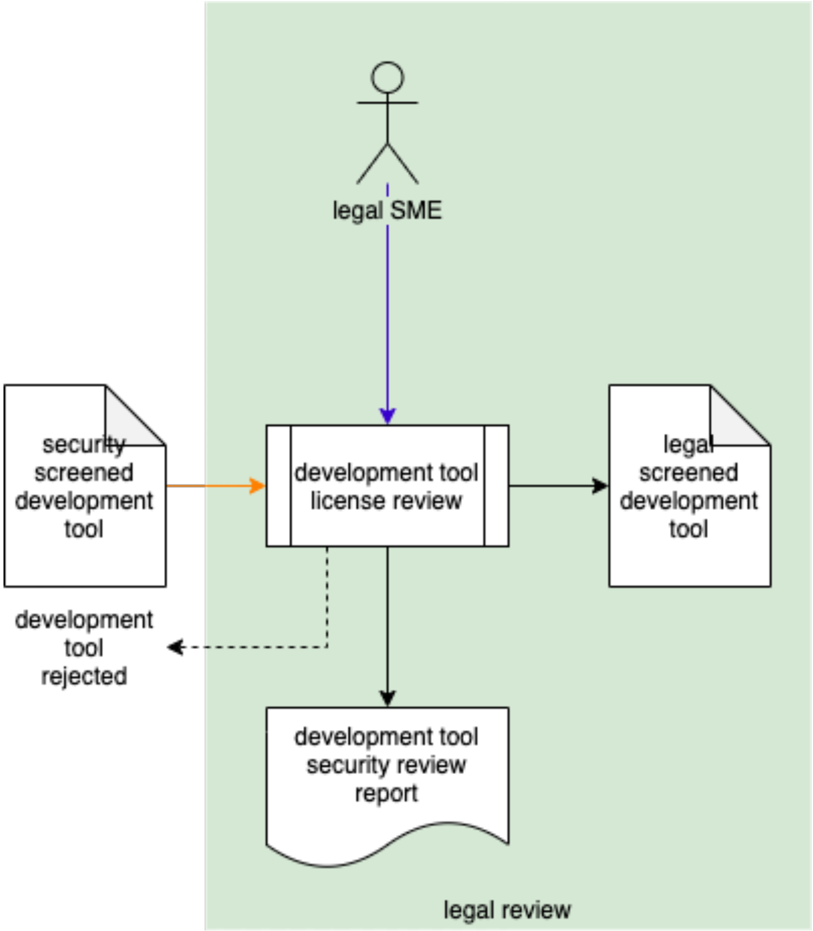
Inputs	Candidate development tool
Outputs	Security screened development tool, security review report
Participants	Security SME, Development SME


development SME
security SME
candidate development tool
development tool security review
security screened development tool
development tool rejected
development tool security review report
security review

The Security SME, together with Development SME(s), review the candidate development tool to determine whether it has acceptable security controls in place. The specifics of “acceptable” is based on the tool and its application. If the tool is deemed unacceptable, it is rejected and may not be used. A report documenting the nature and outcome of the review will be generated.

Legal Review

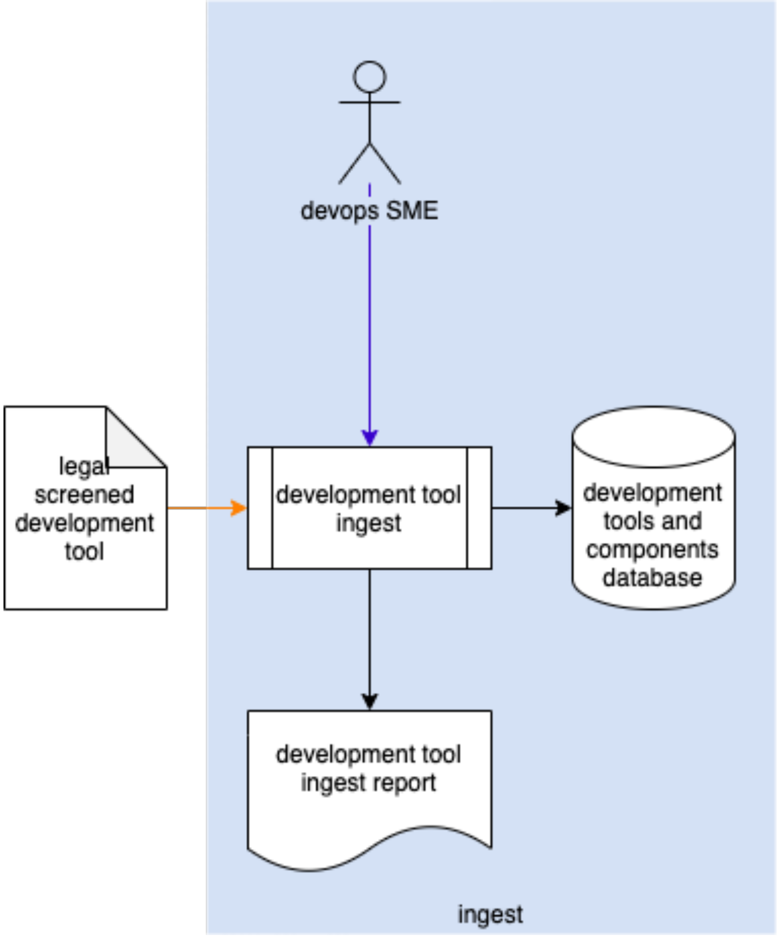
Inputs	Security screened development tool
Outputs	Legal screened development tool, legal review report
Participants	Legal SME


legal SME
security screened development tool
development tool license review
legal screened development tool
development tool rejected
development tool security review report
legal review

The Legal SME reviews the security screened tool's license to assess its acceptability. The specifics of "acceptability" is based on the tool and its deployment. If the tool's license is deemed unacceptable, it is rejected and may not be used. A report documenting the nature and outcome of the review will be generated.

Ingest

Inputs	Legal screened development tool
Outputs	Development tools database (entry)
Participants	Devops SME


devops SME
legal screened development tool
development tool ingest
development tools and components database
development tool ingest report
ingest

The Devops SME takes (or creates, if necessary) the metadata associated with the tool and creates an entry for it in the development tools database. The tool itself is then managed using standard best practices. A report documenting the tool ingest will be generated.

Metadata Detail

The preferred form of tool metadata is SPDX encoded JSON for software components (raw source / libraries) and SWID encoded JSON for executables.

All software (tools and components) used in the development process will be tracked using a database containing the information necessary to generate ISO 19770-2:2015 [2] (SWID [3]) documents. When software libraries are ingested their SPDX information is used.

For each project, a database table will be created forming a collection of project-specific SWID entries.

References

1. **The Case for Software Bill of Materials** [video 37m]
   http://video.sonatype.com/watch/k1q2hYfAussHmetReM3Jbm
2. **Software Package Data Exchange® (SPDX®)**
   https://spdx.dev/wp-content/uploads/sites/41/2017/12/spdxversion2.1.pdf
3. ISO 19770-2:2015 **Information technology - IT asset management - Part 2: Software identification tag**
   https://www.iso.org/standard/65666.html
4. NIST IR 8060 **Guidelines for the Creation of Interoperable Software Identification (SWID) Tags**
   https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8060.pdf