

ASSURANCE

Le bon livrable, pas seulement un livrable

Cible, réalisation, divergence et acceptation dans Sawbill

Comment Sawbill établit qu'un résultat correspond à l'intention, à la cible, aux politiques et aux preuves attendues.

LECTEURS

Directeurs et responsables d'ingénierie / Architectes / Responsables qualité et sécurité / Responsables risque et conformité

Sommaire

L'enjeu en une minute	3
Ce que « conformité » signifie ici	3
Trois artefacts qui ne doivent pas être confondus	3
Le graphe cible	4
Le graphe réel	4
Le rapport de divergence	4
L'alignement ne se déduit pas d'un nom	4
Observer est une activité gouvernée	5
L'assurance traverse la chaîne existante	6
UNKNOWN est une information, pas un échec cosmétique	6
Les tests sont des preuves bornées	7
Mécanique et sémantique : deux formes d'évaluation	8
De la divergence au prochain travail	8
L'acceptation lie des versions exactes	8
La conformité normative est un profil, pas le moteur entier	9
Scénario : l'export de données est-il réellement conforme à la cible ?	9
Valeur pour l'entreprise	9
Moins de faux positifs de livraison	9
Une qualité explicable	9
Une conformité réglementaire intégrable	10
Une gestion continue du drift	10
Références officielles	10

Le bon livrable, pas seulement un livrable

L'enjeu en une minute

Un agent peut terminer sa tâche, produire du code valide et faire passer tous les tests disponibles sans livrer ce qui avait réellement été demandé. Une exigence peut manquer. L'architecture cible peut être contournée. Une configuration peut ne pas avoir été observée. Un résultat de test peut appartenir à une ancienne version.

Sawbill appelle **assurance du livrable** la capacité de relier :

une intention autorisée, une cible versionnée, une réalisation observée, des politiques applicables et les preuves exigées pour l'acceptation.

La conformité réglementaire peut participer à cette assurance, mais elle n'en est qu'une dimension possible.

Ce que « conformité » signifie ici

Dans le langage courant, conformité évoque d'abord les lois, règlements et normes. Pour un produit d'ingénierie, la première question est pourtant plus large : le livrable correspond-il au contrat que l'organisation a décidé de lui appliquer ?

Ce contrat peut contenir :

- des comportements fonctionnels ;
- une architecture, des interfaces et des contraintes de dépendances ;
- des invariants de sécurité ;
- des objectifs de qualité ou de performance ;
- un processus de vérification et une séparation des devoirs ;
- des obligations contractuelles ;
- des contrôles issus de standards ou de réglementations applicables ;
- des preuves et conditions d'acceptation.

Sawbill ne mesure donc pas une qualité universelle. Il évalue une correspondance relative à une cible et à un profil d'assurance identifiés.

Trois artefacts qui ne doivent pas être confondus

Le cœur de l'approche repose sur trois objets distincts et versionnés.

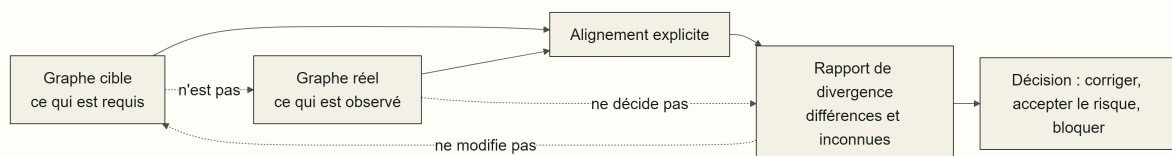


Figure 1 - Sawbill

Le graphe cible

Le graphe cible représente ce qui est requis ou intentionnel : capacités, composants, interfaces, règles, exigences et relations. Il est lié aux versions des sources, des politiques, des packs et des profils utilisés pour l'interpréter.

Une intention ou un document source n'est pas automatiquement une cible admise. Sawbill conserve la différence entre une proposition de cible et la version qui sert effectivement de contrat d'évaluation.

Le graphe réel

Le graphe réel décrit ce qui a été observé à un cutoff donné. Il peut intégrer :

- structures de code et dépendances ;
- interfaces et configurations ;
- topologie et artefacts de déploiement ;
- comportements observés par tests ou traces ;
- affirmations fonctionnelles attribuées ;
- éléments non accessibles, non tentés ou inconnus.

Le réel n'est pas déduit de la cible. Un composant attendu mais non observé ne disparaît pas silencieusement ; il devient une absence établie ou une inconnue, selon la couverture disponible.

Le rapport de divergence

Le rapport compare une cible exacte et une réalisation exacte sous une politique donnée. Il conserve les différences, les mappings ambigus et les inconnues.

Accepter un risque ne transforme pas la divergence en conformité. Sawbill peut conserver à la fois le fait technique - une différence existe - et sa disposition de gouvernance - elle est temporairement acceptée par telle autorité.

L'alignement ne se déduit pas d'un nom

Deux objets qui portent le même nom, chemin ou digest partiel ne jouent pas nécessairement le même rôle. Sawbill rend l'alignement explicite entre les nœuds de la cible et ceux du réel.

Une relation d'alignement peut être :

- établie ;
- candidate ;
- rejetée ;
- ambiguë ;
- inconnue ;
- devenue obsolète.

Seule une relation établie sous le profil applicable peut alimenter les règles déterministes suivantes. Les relations N:M restent possibles : une exigence peut être réalisée par plusieurs composants, et un composant peut contribuer à plusieurs exigences.

Observer est une activité gouvernée

Une analyse n'est fiable que si son périmètre est défini avant de voir le résultat. Sinon, un outil peut simplement réduire le périmètre lorsqu'une partie est difficile à inspecter.

Sawbill utilise un mandat d'observation qui précise :

- la population attendue ;
- les sources et méthodes ;
- les dimensions à examiner ;
- les droits d'accès nécessaires ;
- le cutoff et les contraintes de données ;
- les résultats attendus et les limites de couverture.

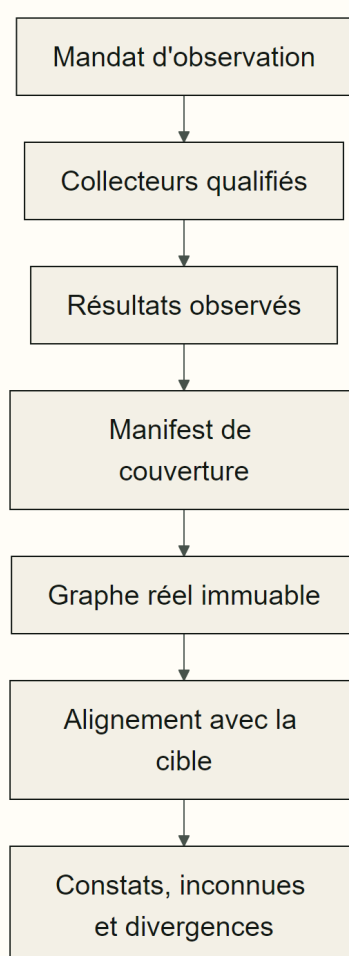


Figure 2 - Sawbill

Un timeout, une source inaccessible, une partition partielle ou une méthode incapable de détecter une classe de défaut reste visible dans le manifest.

L'assurance traverse la chaîne existante

Sawbill ne remplace pas les tests, scanners, CI, dépôts d'artefacts ou plateformes d'observabilité. Il leur donne une place explicite dans un dossier d'assurance : chaque outil observe un sujet défini ; Sawbill relie cette observation à la cible, à la couverture et à la décision qui peut réellement l'utiliser.

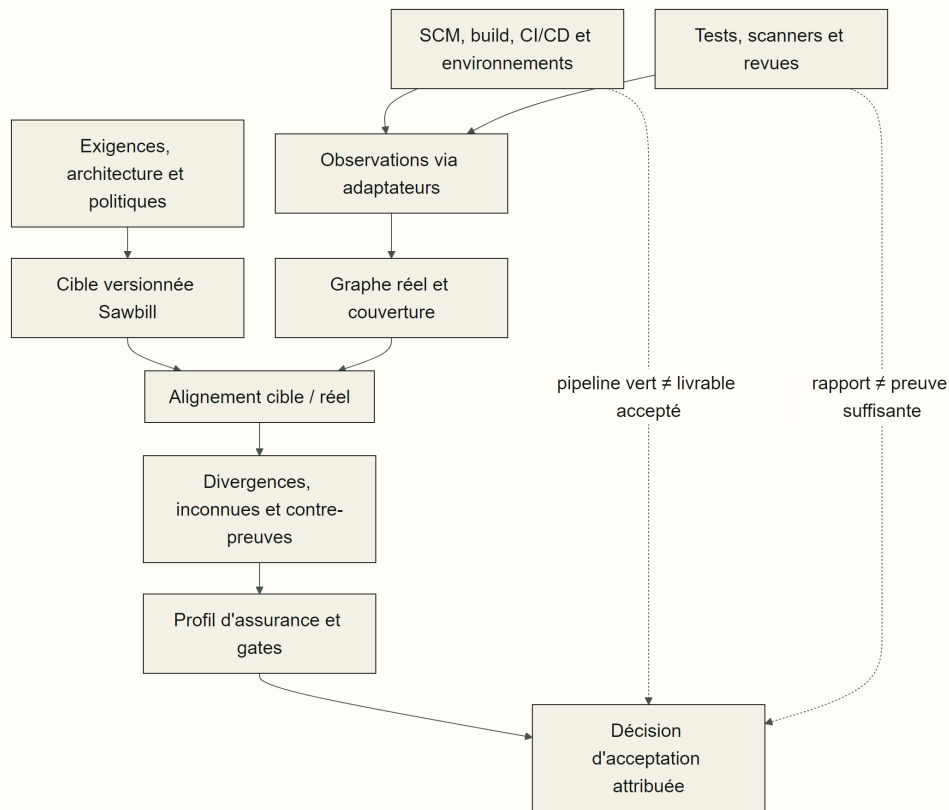


Figure 3 - Sawbill

La frontière se déplace du statut de l'outil vers la relation démontrée entre une cible et un état observé. Les outils conservent leur spécialité ; aucun ne peut conclure seul que le livrable entier est acceptable.

UNKNOWN est une information, pas un échec cosmétique

Une grande partie du risque logiciel vient de conclusions positives obtenues à partir d'une population incomplète. Un scanner qui ne trouve rien peut avoir couvert 100 % des fichiers qu'il a reçus tout en ignorant un runtime, une configuration ou un dépôt voisin.

Sawbill distingue donc la couverture du processus et l'adéquation de l'univers :

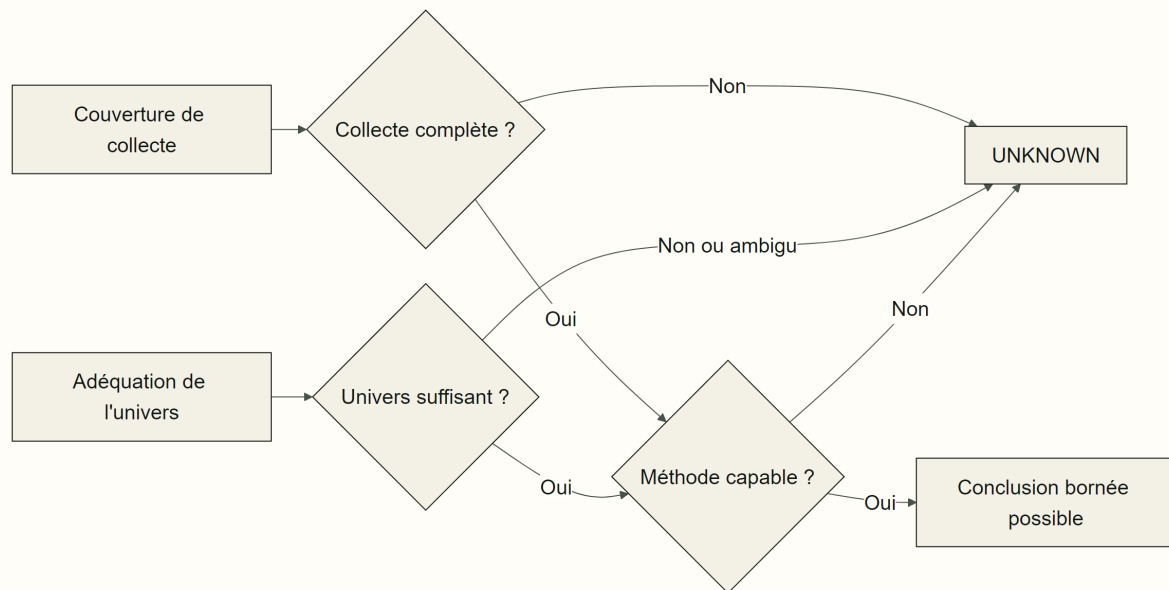


Figure 4 - Sawbill

Une conclusion d'absence exige une population fermée, une méthode capable, une traversée complète et un résultat négatif explicite. Sans ces éléments, Sawbill conserve UNKNOWN au lieu de produire un score rassurant.

Les tests sont des preuves bornées

Un test unitaire, un test d'intégration et une régression ne répondent pas à la même question. Sawbill lie chaque test à un profil qui déclare son environnement, ses données, son sujet, sa population attendue et son oracle.

Pour un bloc logique, un ensemble de vérification regroupe les paquets exacts concernés :

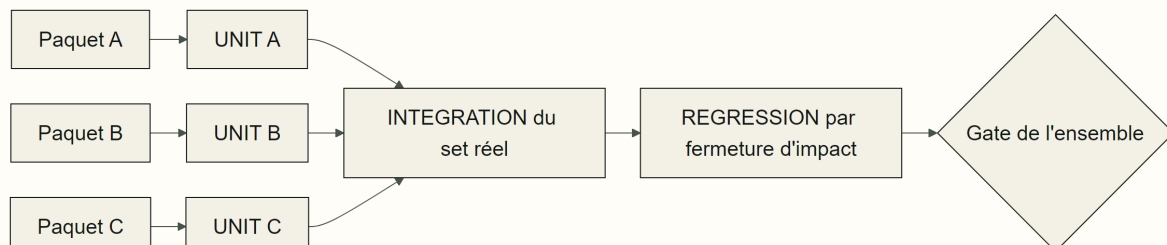


Figure 5 - Sawbill

Une étape terminale ne compense pas une étape absente. Un test unitaire vert ne prouve pas l'intégration. Un test d'intégration ne couvre pas automatiquement les consommateurs affectés. Une exemption N/A doit elle-même être justifiée, bornée et autorisée.

Les mocks et simulateurs restent utiles, mais ils prouvent seulement un comportement sous substitution. Ils ne démontrent pas le comportement du vrai fournisseur ou d'un effet externe.

Mécanique et sémantique : deux formes d'évaluation

Certaines questions possèdent un oracle déterministe :

- ces octets ont-ils ce digest ?
- le schéma est-il valide ?
- cette dépendance interdite est-elle présente ?
- la signature correspond-elle aux octets attendus ?

D'autres nécessitent une appréciation sémantique :

- l'implémentation réalise-t-elle réellement l'intention métier ?
- l'univers d'observation est-il suffisamment complet ?
- l'architecture répond-elle au risque dans son contexte ?
- une exigence réglementaire est-elle applicable à cette organisation ?

Sawbill automatise les prédicats mécaniques et attribue les jugements sémantiques. Un agent peut lire, comparer et rechercher des contre-exemples, mais son score de confiance ne devient pas une preuve mathématique. Les décisions matérielles peuvent exiger une revue indépendante ou humaine.

De la divergence au prochain travail

Le rapport de divergence ne modifie pas directement le système. Il alimente une analyse d'impact, puis une base de planification et un DAG d'exécution distinct.

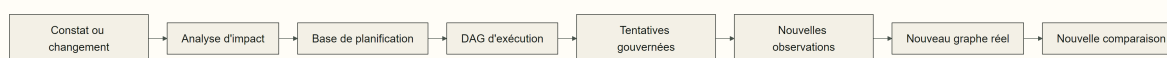


Figure 6 - Sawbill

Ce cycle évite deux raccourcis : transformer automatiquement toute divergence en tâche, ou considérer une tâche terminée comme preuve de réalisation.

L'acceptation lie des versions exactes

Une décision d'acceptation porte sur un sujet précis et un ensemble précis d'entrées : cible, réalisation, politiques, gates et preuves. Elle n'est pas un booléen durable attaché au nom d'un projet.

Si le code, la politique, le profil de preuve ou la couverture change, le système ne réutilise pas silencieusement l'ancienne acceptation. Il réévalue son utilisabilité et ouvre un successeur lorsque nécessaire.

Les outcomes restent distincts :

Outcome	Signification
ACCEPTED	L'autorité compétente accepte ce sujet exact avec ces entrées exactes
REJECTED	La décision est explicitement négative
BLOCKED	Une condition obligatoire empêche de progresser
UNKNOWN	Le dossier est valide mais insuffisant pour conclure

UNKNOWN ne signifie pas risque faible. Il signifie que le système refuse de fabriquer une certitude.

La conformité normative est un profil, pas le moteur entier

Les obligations externes entrent dans Sawbill sous forme de sources identifiées et versionnées. Un mapping relie une exigence externe à des contrôles, sujets et preuves Sawbill sans recopier ni remplacer le texte normatif.

Le parcours standards-first est :

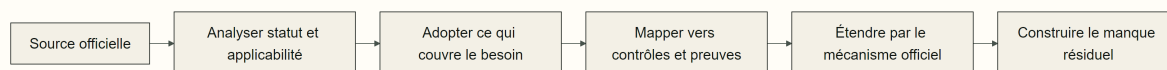


Figure 7 - Sawbill

L'applicabilité, le tailoring et les jugements juridiques restent attribués. Un pack réussi peut contribuer à un dossier de conformité ; il ne constitue pas à lui seul une certification.

Scénario : l'export de données est-il réellement conforme à la cible ?

La cible exige :

- un export accessible uniquement au propriétaire des données ;
- une journalisation sans contenu sensible ;
- un traitement dans l'environnement autorisé ;
- une expiration du lien de téléchargement ;
- des tests unitaires, une intégration avec le stockage réel et une régression sur les parcours d'accès existants.

L'observation trouve l'endpoint, les contrôles d'accès et les tests unitaires. Elle ne peut toutefois pas accéder à la configuration de l'environnement de staging. Le stockage réel n'a pas été exercé.

Sawbill ne conclut ni « conforme » parce que le CI est vert, ni « non conforme » par intuition. Il produit :

- des alignements établis pour l'endpoint et le contrôle d'accès ;
- une divergence si la journalisation expose des données ;
- UNKNOWN pour l'environnement inaccessible ;
- une obligation d'intégration non satisfaite pour le stockage réel ;
- une analyse d'impact sur les anciens parcours d'accès.

Le décideur sait exactement ce qui est démontré, contredit ou encore inconnu.

Valeur pour l'entreprise

Moins de faux positifs de livraison

La fin d'une tâche, un commit ou un pipeline vert ne remplace pas la comparaison entre intention et réalisation.

Une qualité explicable

Chaque conclusion conserve sa cible, son périmètre, sa méthode, sa couverture et ses limites. Les équipes peuvent débattre du bon profil plutôt que d'un score opaque.

Une conformité réglementaire intégrable

Les obligations normatives deviennent des sources et mappings versionnés dans le même parcours d'assurance, sans contaminer le moteur avec une interprétation juridique implicite.

Une gestion continue du drift

La cible, le réel et les divergences étant distincts, Sawbill peut détecter les changements et réévaluer l'acceptation sans réécrire l'histoire.

Références officielles

Source	Statut externe	Apport utilisé	Limite conservée par Sawbill
ISO/IEC/IEEE 29148:2018 - Requirements engineering	Standard publié, confirmé en 2024 et en cours de révision	Référence pour l'ingénierie des exigences et ses éléments d'information	Le texte sous licence n'est pas reproduit ; l'applicabilité reste explicite
ISO/IEC 25010:2023 - Product quality model	Standard international publié	Vocabulaire de caractéristiques de qualité et de critères d'évaluation	Un modèle de qualité ne décide pas de l'acceptation Sawbill
ISO/IEC/IEEE 29119-2:2021 - Test processes	Standard international publié	Référence pour la gouvernance et l'organisation des processus de test	Sawbill conserve ses bindings de sujet, version, couverture et preuve
NIST SP 800-218 - SSDF 1.1	Publication NIST finale	Pratiques de développement sécurisé intégrables au cycle de vie	Le respect d'une pratique ne prouve pas seul la conformité du livrable
JSON Schema Draft 2020-12	Spécification publiée	Validation de formes et contrats JSON	La validité de schéma ne prouve pas la sémantique métier
NIST OSCAL	Initiative NIST et formats ouverts	Échange machine-readable de catalogues, profils, implémentations et évaluations de contrôles	OSCAL transporte des données de contrôle ; Sawbill conserve applicabilité, preuve et décision
NASA NPR 7150.2D	Directive NASA effective du 8 mars 2022 au 8 mars 2027 ; obligatoire dans son périmètre NASA	Exemple public d'exigences de cycle de vie, de classification et de tailoring	Aucun projet non NASA n'hérite de son applicabilité par simple mapping

Les références ISO sont citées par identifiant, version, titre et statut public. Leur texte reste soumis aux droits de l'éditeur. Les mappings Sawbill ne sont ni le texte normatif, ni une certification, ni un avis juridique.