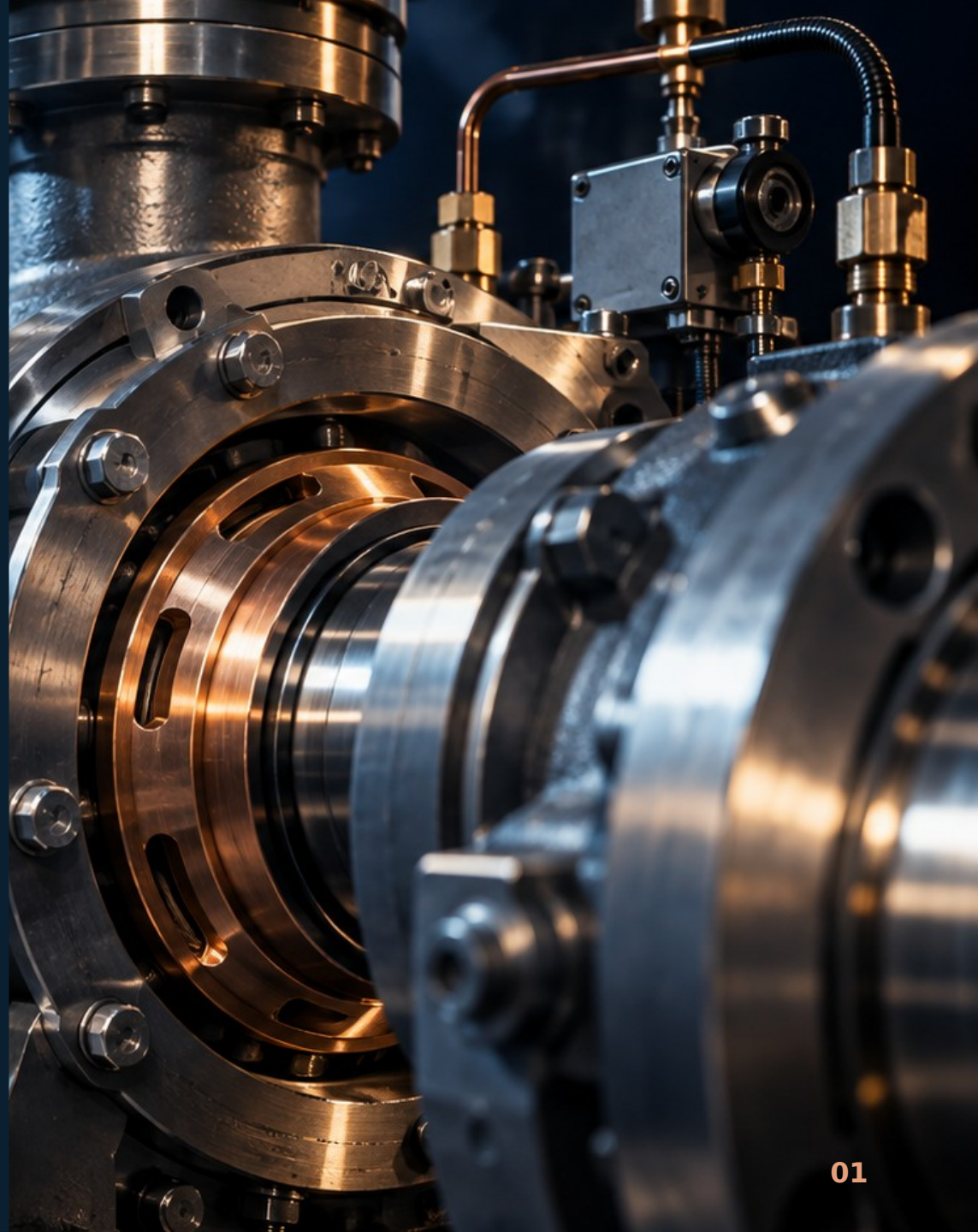
HISTOIRE DE LA DISCIPLINE

Sûreté de fonctionnement

Six périodes pour comprendre son évolution

XIXe siècle à 2026



La sûreté de fonctionnement

Un cadre commun pour évaluer la confiance dans un système

Assurer la fonction requise dans des conditions définies

Quatre propriétés complémentaires

F — **Fiabilité**

Fonctionner sans défaillance pendant une durée donnée.

M — **Maintenabilité**

Permettre la maintenance dans des conditions fixées.

D — **Disponibilité**

Être en état de fonctionner au moment requis.

S — **Sécurité**

Maîtriser le risque de dommages aux personnes et à l’environnement.

Six périodes de l’évolution

Un découpage fondé sur le périmètre de l’analyse

01 XIXe siècle–1939

Prévention industrielle

02 1940–1959

Fiabilité quantitative

03 1960–1979

Analyse des systèmes

04 1980–1999

Facteurs humains et logiciel

05 2000–2009

Cycle de vie et normes

06 2010–2026

Systèmes connectés

Prévention industrielle

Limiter les ruptures et les accidents

Les chaudières et les équipements sous pression font émerger des règles d’essai et de construction.

1884

Norme ASME d’essais des chaudières

1914 / 1915

Premier code ASME : édition 1914, publication 1915



Priorité : résistance et conformité de l’équipement

Fiabilité quantitative



La défaillance devient une grandeur à mesurer

L’électronique militaire stimule les études de durée de vie et la qualification des composants.

1951

Weibull : une loi de distribution statistique

1957

Rapport AGREE : fiabilité des équipements électroniques

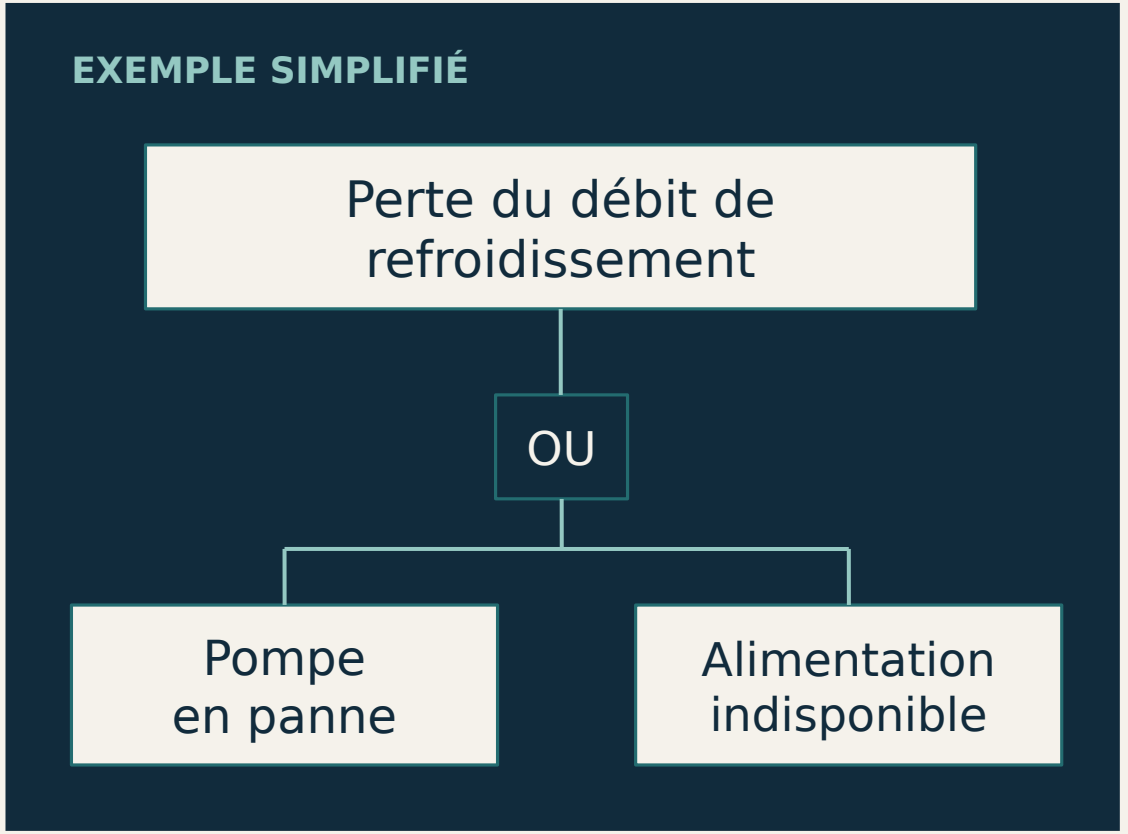
Lyonnet : approches prévisionnelle, expérimentale et opérationnelle

Analyse des systèmes

Les pannes se combinent à l’échelle du système

1961 Arbres de défaillances à Bell Labs

1975 WASH-1400 : évaluation probabiliste des risques nucléaires



Facteurs humains et logiciel

1988

Villemeur documente un périmètre élargi

Le sommaire associe déjà le matériel, les personnes et le logiciel.

CHAPITRES DU SOMMAIRE

15 Défaillances dépendantes et de cause commune

16 Facteurs humains

18 Logiciel

La technique et les personnes interagissent dans les défaillances

Cycle de vie et normes

1998

IEC 61508-1 amorce le cadre de sécurité fonctionnelle

2003

IEC 61511-1 adapte ce cadre aux industries de procédé



Cycle simplifié. La sécurité se construit et se vérifie au fil de la vie du système.

Systèmes connectés

Les interactions numériques élargissent les scénarios étudiés

2010 Deuxième édition d’IEC 61508-1

2023 NIST : cybersécurité industrielle
EASA : confiance dans l’IA



Une intrusion ou une donnée incorrecte peuvent affecter une fonction industrielle.

La logique des bornes

Chaque transition correspond à un élargissement de la question étudiée

Borne	Évolution retenue	Repère documentaire
1940	La fiabilité devient quantitative	Rapport AGREE, 1957 [H3]
1960	L’analyse porte sur le système	Arbres de défaillances, 1961 [H5]
1980	Poids de l’humain et du logiciel	Villemeur, ouvrage de 1988 [V]
2000	Preuves sur le cycle de vie	IEC 61508, 1998 / IEC 61511, 2003 [N1, N2]
2010	Connexions numériques	IEC, 2010 / NIST et EASA, 2023 [N1, N3, N4]

Une pompe, six regards successifs

Exemple pédagogique : une pompe alimente le refroidissement d’une machine

Période	Point d’attention	Question à poser
XIXe–1939	Résistance	La pompe résiste-t-elle à la pression ?
1940–1959	Durée de vie	Quelle durée de fonctionnement sans panne ?
1960–1979	Scénario de panne	Quelles pannes peuvent supprimer le débit ?
1980–1999	Intervention et logiciel	Une erreur de commande peut-elle l’arrêter ?
2000–2009	Cycle de vie	Comment vérifier la fonction à chaque étape ?
2010–2026	Interaction numérique	Une intrusion peut-elle perturber la commande ?

Un périmètre qui s’élargit

Les méthodes se complètent au fil des besoins industriels

Une même finalité

Assurer la fonction requise avec un risque maîtrisé

XIXe–1939	Prévention industrielle
1940–1959	Fiabilité quantitative
1960–1979	Analyse des systèmes
1980–1999	Humain et logiciel
2000–2009	Cycle de vie et normes
2010–2026	Systèmes connectés

Références des deux ouvrages

Repères de lecture pour approfondir le découpage

[V] Alain Villemeur

Sûreté de fonctionnement des systèmes industriels

Fiabilité, facteurs humains, informatisation
Eyrolles, collection EDF n° 67, 1988
ISBN 978-2-21201-615-4

Ch. 1 : historique
Ch. 15, 16, 18 : dépendances, humain, logiciel
Sommaire et préfaces publics consultés

Sommaire de l’auteur

[L] Patrick Lyonnet

Ingénierie de la fiabilité

Tec & Doc, Lavoisier, 2006
ISBN 978-2-7430-0823-9

Ch. 1–2 : historique, taux de défaillances
Ch. 5–8 : systèmes, REX, essais, méthodes
Présentation et sommaire publics consultés

Notice et présentation

Sources des jalons historiques

Références complémentaires aux deux ouvrages

[H1] **ASME. History of ASME Standards**

Norme d’essais de 1884. Code, édition 1914 et publication 1915.

[H2] **W. Weibull. A Statistical Distribution Function of Wide Applicability**

Journal of Applied Mechanics, 18(3), 1951, p. 293–297.

[H3] **AGREE. Reliability of Military Electronic Equipment**

US Government Printing Office, 1957.

[H4] **NRC. Reactor Safety Study, WASH-1400**

NUREG-75/014, octobre 1975.

[H5] **J.-P. Katoen et M. Stoelinga. Boosting Fault Tree Analysis by Formal Methods**

2017, introduction p. 1. Repère historique des arbres en 1961.

Sources de l’histoire récente

Concepts, normes et publications institutionnelles

[Q] **Avizienis, Laprie, Randell et Landwehr. Basic Concepts and Taxonomy**

IEEE TDSC, 1(1), 2004, p. 11–33. DOI 10.1109/TDSC.2004.2.

[N1] **IEC 61508-1:2010 et Overview of IEC 61508 & Functional Safety**

Édition 2 de 2010, après 1998. Aperçu public IEC de 2022.

[N2] **IEC 61511-1**

Première édition 2003. Sécurité instrumentée des industries de procédé.

[N3] **NIST. Guide to Operational Technology (OT) Security**

SP 800-82 Rev. 3, 2023. DOI 10.6028/NIST.SP.800-82r3.

[N4] **EASA. Artificial Intelligence Roadmap 2.0**

2023. Approche de l’IA en aviation centrée sur l’humain.