ROB-104 — SYSTÈMES AUTONOMES ET NAVIGATION AVANCÉE

Leçon 8 — Navigation robuste, résilience aux pannes et sûreté de fonctionnement

Manuel universitaire illustré • Formation à distance • Théorie, simulations, exercices corrigés et film pédagogique



Figure 8.1 — Robot mobile doté de capteurs complémentaires : la fiabilité exige surveillance, redondance et vérification.

Objectifs et compétences

- Distinguer robustesse, résilience, fiabilité et sûreté de fonctionnement.
- Détecter une panne franche, une dérive, un retard et une donnée incohérente.
- Définir des états normal, prudent, dégradé et arrêt sûr.
- Dimensionner une distance d'arrêt et interpréter les incertitudes.
- Évaluer un scénario ROS 2/Nav2 par des preuves expérimentales.

1. Concepts fondamentaux

Robustesse : maintien de performances acceptables malgré des perturbations prévues. Résilience : aptitude à détecter un problème, réorganiser le fonctionnement et récupérer. Fiabilité : probabilité d’assurer une fonction pendant une durée et dans des conditions définies. Sûreté de fonctionnement : ensemble des propriétés permettant d’accorder une confiance justifiée au service rendu, notamment la sécurité des personnes.

Un robot peut être robuste face au bruit d’un capteur tout en étant non résilient à une panne complète. Inversement, un robot qui détecte une perte LiDAR et s’arrête de manière contrôlée démontre une propriété de sécurité, même s’il ne termine pas sa mission.

2. Architecture de surveillance

L’architecture sépare la mission de navigation, l’estimation d’état, la surveillance des capteurs et une couche indépendante de limitation ou d’arrêt. La surveillance doit examiner la fraîcheur des données, leur plausibilité, leur cohérence avec les autres capteurs et la qualité de communication.

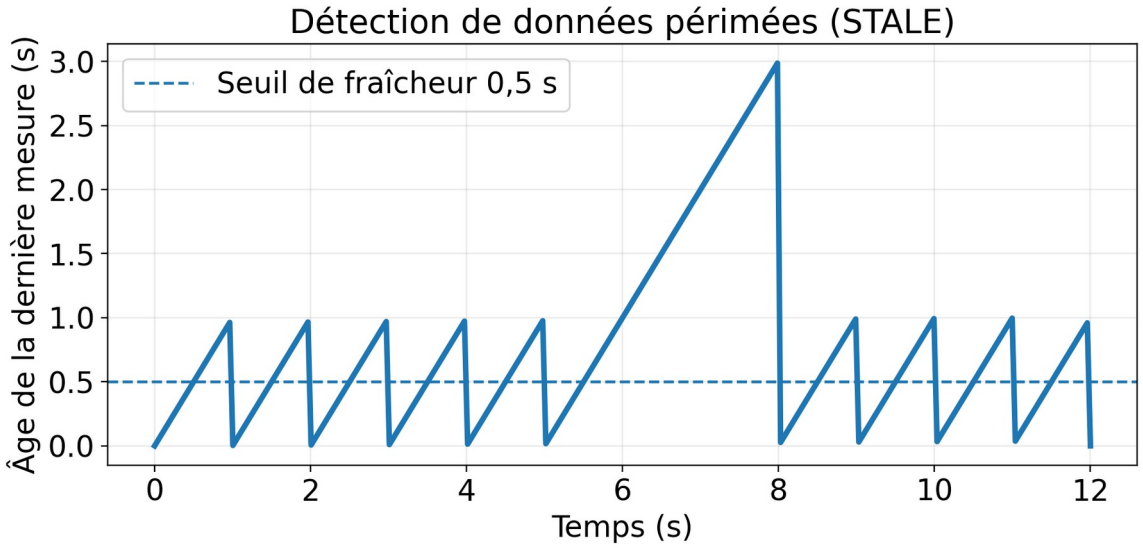


Figure 8.2 — Détection d'une mesure périmée par un timeout défini selon le capteur et la mission.

Contrat de santé de chaque capteur

- OK : mesure récente, plausible et cohérente.
- NOISY : variance ou dispersion excessive.
- BIASED : décalage systématique estimé.
- STALE : mesure trop ancienne pour guider la navigation.
- ABSENT : aucune mesure reçue.
- INVALID : valeur hors domaine ou format incorrect.

3. Analyse des défaillances et FMEA

Une analyse des modes de défaillance et de leurs effets (FMEA/AMDEC) part du composant, de son mode de panne, des effets locaux et système, des moyens de détection et des mesures de maîtrise. Les valeurs de criticité dépendent du contexte d'emploi et doivent être justifiées.

Élément	Panne	Détection	Réaction prévue
LiDAR	Flux absent	Timeout /scan	Ralentir ou arrêter

IMU	Biais croissant	Innovation et cohérence	Augmenter covariance
Encodeur	Valeur figée	Incohérence mouvement	Limiter la commande
Réseau	Perte de messages	Heartbeat / délai	État sûr local
Alimentation	Sous-tension	Mesure bus / alarme	Arrêt contrôlé

4. Machine à états et modes dégradés

Une machine à états rend les décisions traçables. NORMAL : perception et localisation conformes. PRUDENT : baisse temporaire de confiance; vitesse limitée. DÉGRADÉ : une source critique est perdue mais une solution de repli validée existe. ARRÊT_SÛR : la marge de sécurité ne peut plus être démontrée. RÉCUPÉRATION : tests de retour à l'état nominal.

Les transitions doivent comporter des conditions explicites et une hystérésis pour éviter les oscillations rapides entre états. Une récupération ne doit pas relancer automatiquement une commande dangereuse.



Figure 8.3 — Exemple visuel de panne de perception et d'adaptation du robot; la poursuite n'est permise que si les marges restent démontrées.

5. Calcul de distance d'arrêt

Dans un modèle pédagogique à décélération constante, $d_{arrêt} = v \cdot \tau + v^2/(2a)$, avec v la vitesse initiale, τ la latence totale et $a>0$ la décélération disponible. On ajoute ensuite une marge tenant compte de la précision des capteurs, de l'adhérence et du gabarit.

Exemple résolu : $v = 1{,}2$ m/s, $\tau = 0{,}30$ s et $a = 1{,}8$ m/s². Distance pendant la latence : $1{,}2 \times 0{,}30 = 0{,}36$ m. Distance de freinage : $1{,}2^2/(2 \times 1{,}8) = 0{,}40$ m. Total : 0,76 m avant marge. Avec 0,25 m de marge, il faut au moins 1,01 m.

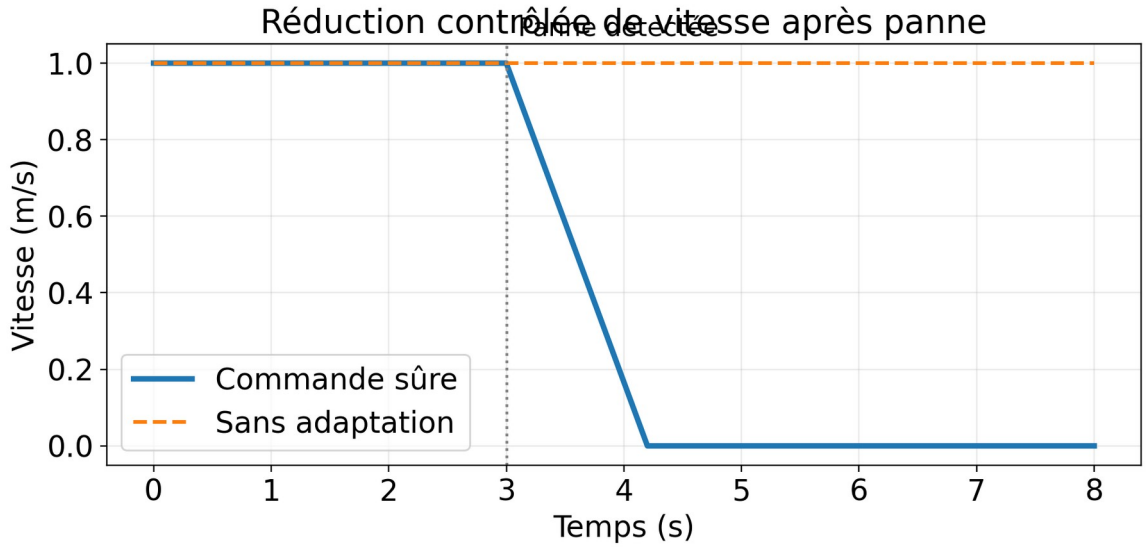


Figure 8.4 — Exemple de réduction contrôlée de vitesse après détection d'une panne.

6. Redondance et fusion prudente

La redondance peut être matérielle (deux capteurs indépendants), fonctionnelle (caméra et LiDAR) ou analytique (modèle de mouvement et observation). Deux capteurs de même technologie peuvent partager une panne commune : poussière, alimentation, horloge ou logiciel. La fusion

ne doit pas accorder une confiance élevée à une mesure manifestement incohérente.

En présence d'une perte LiDAR, l'odométrie et la caméra peuvent conserver une estimation temporaire, mais l'incertitude augmente. Selon l'environnement, la bonne réponse peut être de réduire la vitesse ou de s'arrêter, plutôt que de continuer coûte que coûte.

7. Intégration dans ROS 2 / Nav2

ROS 2 fournit des topics, diagnostics, paramètres et mécanismes de communication. Nav2 dispose de composants de planification, contrôle, comportements et supervision du cycle de vie. L'intégration sûre dépend de la version installée, du matériel, de la configuration et de la surveillance indépendante de la commande moteur.

Commandes d'observation sous Ubuntu

```
ros2 node list

ros2 topic list

ros2 topic hz /scan

ros2 topic echo /diagnostics --once

ros2 topic echo /odom --once

ros2 action list
```

Ces commandes sont destinées à l'observation; leur fonctionnement dépend des topics réellement publiés. La sécurité physique exige des protections et un arrêt d'urgence adaptés, indépendamment du logiciel de navigation.

8. Laboratoire à distance — cinq séances

Séance 1 — Référence nominale

Construire un parcours de 12 m, définir des obstacles et enregistrer trajectoire, vitesse, âge des données et distance minimale.

Séance 2 — Panne LiDAR

Interrompre /scan pendant 2 s dans la simulation; vérifier timeout, journal et transition d'état.

Séance 3 — Dérive IMU

Ajouter un biais gyroscopique progressif; mesurer l'innovation et l'augmentation de covariance.

Séance 4 — Perte réseau

Interrompre les messages de supervision; vérifier que le contrôleur local conserve un comportement sûr.

Séance 5 — Validation statistique

Exécuter 20 essais, comparer taux de réussite, distances minimales, arrêts sûrs et délais de détection.

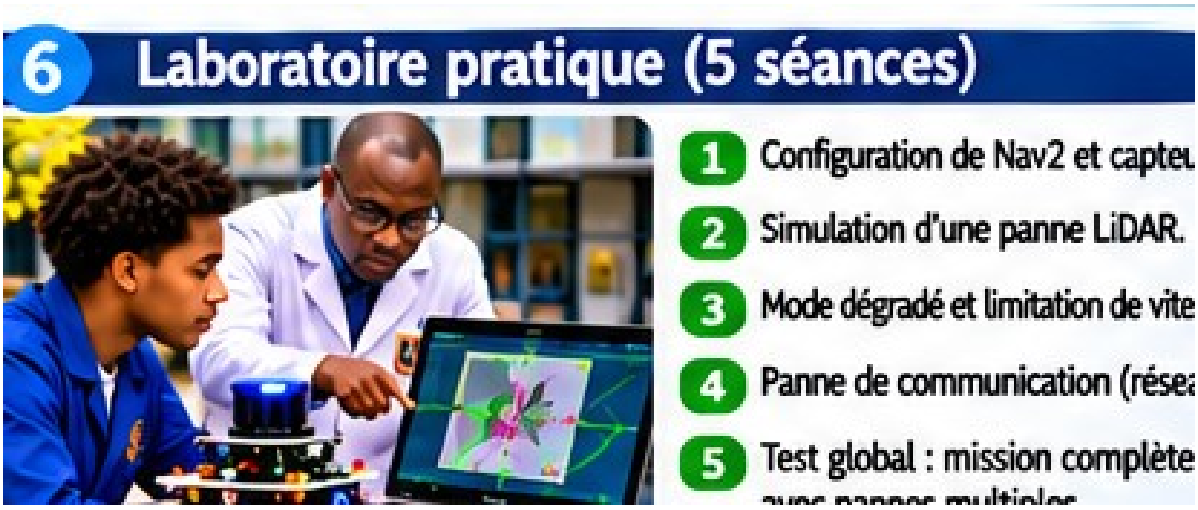


Figure 8.5 — Laboratoire simulé : comparer comportement nominal, panne et récupération.

9. Évaluation et preuves

Le rapport doit comprendre : scénario et paramètres; chronologie horodatée; état des capteurs; transitions de la machine à états; commandes et vitesses; distances minimales; résultat de sécurité; conclusion et mesures correctives.

Exercices corrigés

Question — Pourquoi la robustesse n'est-elle pas identique à la résilience ?

Corrigé — La première concerne la tolérance aux perturbations; la seconde inclut détection, adaptation et récupération après défaillance.

Question — Quelle distance d'arrêt à $v=1{,}5$ m/s, $\tau=0{,}4$ s et $a=2{,}0$ m/s² ?

Corrigé — $1{,}5\times0{,}4 + 2{,}25/4 = 1{,}1625$ m avant marge.

Question — Une caméra peut-elle remplacer systématiquement un LiDAR perdu ?

Corrigé — Non; la décision dépend des capacités de la caméra, de la lumière, des distances et de l'incertitude.

Question — Pourquoi un arrêt sûr peut-il être une réussite ?

Corrigé — Il empêche une exposition au risque lorsque la mission ne peut plus être menée avec les garanties nécessaires.

Question — Que vérifier avant de revenir à NORMAL ?

Corrigé — Fraîcheur, cohérence, localisation, absence de panne persistante et validation des conditions de reprise.

10. Film pédagogique dialogué

Scène 1 : le professeur présente un robot autonome en laboratoire. Scène 2 : une étudiante surveille les capteurs sur écran. Scène 3 : un LiDAR cesse de publier; une alerte apparaît. Scène 4 : le robot réduit sa vitesse puis s’arrête devant une zone incertaine. Scène 5 : l’équipe analyse les journaux, rétablit le capteur et vérifie la reprise. Scène 6 : les étudiants exposent les différences entre robustesse, résilience et sécurité.

Livrables : simulation, données horodatées, tableaux de résultats, réponses corrigées, rapport de laboratoire et storyboard du film.