



THE INDUSTRY EDITION / 2 OCTOBER 2026

# Connected cargo. Controlled risk.

Use AI to understand shipment exceptions and draft better updates, without turning emails into cargo-release instructions.

## MARITIME & LOGISTICS

### THE OPPORTUNITY

Begin in the operations inbox, not with a port-sized digital twin.

### THE CYBER QUESTION

Which source is trusted enough to change a shipment?

### THE ACTION

One trade lane, human review and a rehearsed offline fallback.

# In this issue.

Seven sections for the people who run an exception desk, secure it and have to sign off what it is allowed to do.

|    |                                      |                                                                                                                             |
|----|--------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| 01 | <b>The briefing</b>                  | Your first AI port can be an operations inbox. Improve the exception workflow before automating consequential instructions. |
| 02 | <b>AI in practice</b>                | The exception desk, with better evidence. A proposed assistant for one operations team and one trade lane.                  |
| 03 | <b>Cyber front</b>                   | When a message becomes an instruction, stop. Keeping connected partner data from becoming unreviewed authority.             |
| 04 | <b>The 30-day playbook</b>           | One lane. One queue. No automatic release. Operator approval throughout and an independent fallback.                        |
| 05 | <b>The decision desk</b>             | Recover desk time before claiming demurrage savings. Illustrative economics, and the case that breaks even.                 |
| 06 | <b>Monday's agenda</b>               | Give every exception an owner. A conversation for the operations desk, technology team and business sponsor.                |
| 07 | <b>Sources &amp; editorial notes</b> | Six numbered references, each with what it does and does not establish.                                                     |

## HOW TO READ THIS EDITION

Reported examples are attributed to their sources. The SME scenarios, pilot plans and decision questions are original editorial proposals, not verified Agents Stack customer results.

All cost examples use explicit assumptions, not market prices or promised returns. Figures are illustrative planning numbers in Singapore dollars.

Obligations differ between a vessel operator and a shore-only forwarder. Have the responsible maritime, legal or compliance specialist confirm flag, class and contractual requirements for the actual business.

# Your first AI port can be an operations inbox.

For forwarders, ship managers, transport operators and supply-chain SMEs: improve the exception workflow before automating consequential instructions.

## The editor's view

A missed update, an ambiguous document or a conflicting shipment status can demand repeated human checking. Our recommendation is to start by helping the operations team assemble evidence and draft an update. Do not begin by giving an assistant authority over release instructions, banking details or onboard systems.

## Choose a smaller problem

A shipment-exception assistant can compare a defined set of records, identify missing information and prepare a message for an operator. It does not need a complete digital replica of a port. It does need stable identifiers, trusted source systems and a clear distinction between a suggestion and an instruction.

## The pilot question

Can the team produce a correct, source-backed exception update faster, while preserving the existing authorization for shipment changes? This is a more useful target than a broad promise to optimize the entire supply chain.

It is also a question the operations desk can answer with a stopwatch and a sample of real exceptions, which is more than most AI business cases can claim.

---

## WHAT THE ASSISTANT MAY NEVER DO IN THE FIRST PILOT

### 01

#### Release cargo

Owned by the release process.

### 02

#### Change consignee

Owned by verification.

### 03

#### Alter payment details

No payment tool at all.

### 04

#### Reach onboard systems

Kept separate from OT.

# Three signals behind the recommendation.

What the current public evidence supports, and what it does not.

## 01 / A digital twin at port scale

GovTech Singapore describes the MPA and GovTech Maritime Digital Twin as combining vessel, port and environmental data in a virtual representation, including incident simulation. It is an official account of project capabilities, not proof of a smaller operator's return. [1]

---

## 02 / Structured documents come first

DCSA's Bill of Lading standard supports more consistent digital document processes and interoperability. It is a reminder to establish data structure and provenance before asking AI to reconcile records. [2]

---

## 03 / Cyber risk includes safety

IMO's revised maritime cyber guidelines, dated 4 April 2025, link cyber risk with safe and resilient ship operations. They are primarily intended for ships and should be considered alongside the applicable Administration requirements. [3]

---

## 04 / What these signals do not establish

None of the three shows that an exception assistant will pay for itself at a specific forwarder. They establish that the data groundwork matters, that port-scale programs are a different category of investment, and that cyber risk in this sector reaches safety as well as information.

**A suggestion and an instruction are different things. The system, not the model, should be what keeps them apart.**

AGENTS STACK PERSPECTIVE

Research cut-off: 11 September 2026. The publication date is planned in advance; these signals do not claim to be October breaking news.

# The exception desk, with better evidence.

A proposed assistant for one operations team, one trade lane and a limited group of counterparties.

## Give the assistant a concrete job

For each selected shipment, assemble the approved reference, latest status, relevant cut-off and outstanding question. Draft a concise customer update with source timestamps. Ask the operator to review it before sending. The assistant should not quietly convert an inferred arrival time into a confirmed commitment.

## Preserve where each fact came from

Distinguish a carrier event from a forwarded email and from an internal estimate. Show the event time, time zone and when the information was retrieved. Retain the original value where normalization changes date or location format. Conflicting sources should trigger a review queue, not an invented compromise.

## Start with imperfect data on purpose

Include a shipment with two identifiers, an old attachment, a revised schedule and a missing event. A pilot built only on clean records will not reveal whether the team can use it when work becomes difficult. Use historical or synthetic data before introducing live customer information.

---

### THE FOUR THINGS EVERY DRAFTED STATUS MUST CARRY

#### 01

##### The source

Carrier event, email or estimate.

#### 02

##### The event time

With its time zone stated.

#### 03

##### The retrieval time

How fresh the information is.

#### 04

##### The open question

What is still unknown.

# A draft is not a document, and speed is not the measure.

The two places this pilot is most likely to be oversold inside your own business.

## **Do not confuse document extraction with legal effect**

Extracting fields from a PDF can support checking, but an AI-generated document is not automatically a legally effective electronic bill of lading. DCSA distinguishes technical and legal interoperability in its work. **[2]** Confirm the instrument, carrier, platform and applicable law with qualified advisers before changing a document process.

## **Keep the first model away from release authority**

The proposed assistant may highlight a discrepancy or prepare a draft. It may not change consignee details, release cargo, alter payment instructions or navigate a vessel. Those exclusions should be enforced by the available tools and identities, not left to the model's interpretation.

## **Measure the work that remains**

Track time from an exception arriving to a correct, approved update. Include reading, source verification and message correction. Record missed exceptions and unnecessary alerts separately. A shorter draft is not useful if an operator must still open every source to discover that its conclusion is wrong.

## **Sample the drafts that were accepted**

Re-check a fixed number of sent updates against their cited events each week. Acceptance rate measures convenience. Re-checking measures whether the cited event was the right one, and whether it was still current when the message went out.

**A shipment status needs a source and a time, not just a confident sentence.**

AGENTS STACK PERSPECTIVE

# When a message becomes an instruction, stop.

Connected partners create useful information flows. The pilot must not turn those flows into unreviewed authority.

## An illustrative failure

An operations assistant reads a forwarded message that appears to update a delivery arrangement. A connected tool can also edit release details. If the system treats the message itself as sufficient approval, a drafting workflow becomes an execution workflow. This is a hypothetical control scenario, not a reported incident.

## Separate reading from acting

OWASP's excessive-agency guidance identifies risk from unnecessary tools, privileges and autonomy. [5] Our proposed logistics assistant therefore receives read access to approved shipment information and a draft-writing function only. Cargo-release or payment changes remain in the established systems and approval process.

## Know the connector identity

Use named service identities and narrow scopes for carrier, customer and internal connections. The team should know who owns each credential, how it is rotated and how access is revoked. Do not share an operator's broad account simply because it makes the initial integration quicker.

---

### PERMISSIONS TO WITHHOLD FROM A DRAFTING ASSISTANT

#### 01

##### Cargo release

It drafts the update, it does not act on it.

#### 02

##### Payment and banking edits

Changes stay in the established system.

#### 03

##### Onboard and OT access

No route from shore-side documents to the vessel.

# Keep the ship, and the fallback, out of scope.

Two boundaries that are easier to draw now than to reconstruct after an incident.

## Keep vessel systems distinct

IMO's guidance explicitly recognizes IT and OT, with the latter capable of affecting ship safety, and it recommends separating OT from IT and Internet-facing systems. [3] A shore-side document assistant should not gain a route into navigation, propulsion or cargo-control systems as a side effect of integration.

## Design the communications fallback

For this pilot, rehearse a loss of the assistant and its status feeds. Operators should know the approved alternative sources, who verifies exceptional instructions and how pending work is recorded. When systems return, reconcile actions before replaying queued messages or drafts.

## Do not confuse guidance with universal scope

IMO's cyber-risk material includes the integration of cyber considerations into safety management. [4] The precise obligations for a vessel operator differ from those for a shore-only forwarder. Have the responsible maritime, legal or compliance specialist confirm flag, class and contractual requirements for the actual business.

## Log enough to reconstruct a decision

Record which records were retrieved, which identity requested them and what the assistant proposed. Logs should support review without copying unnecessary customer or commercial data into a second store that then needs its own controls.

**An operations copilot must not become an undocumented control system.**

AGENTS STACK PERSPECTIVE

# One lane. One queue. No automatic release.

An Agents Stack proposed pilot: a shipment-exception drafting assistant with operator approval and an independent fallback.

## DAYS 1 TO 7

### Define the operational boundary

Choose one trade lane and a manageable set of carriers or counterparties. Specify the approved shipment identifiers, source systems and event types. Record how long staff spend assembling a correct update today. Name the operations owner and the authority for exceptional instructions.

## DAYS 8 TO 14

### Build a historical test

Prepare records with missing events, conflicting times, duplicate references and revised documents. Use minimized, authorized data. Configure a read-only comparison workflow and draft output. Every factual status must retain its source and timestamp. Unknown information must remain unknown.

## DAYS 15 TO 21

### Run beside operators

Use the assistant on the selected queue while the existing workflow remains authoritative. Operators review every update before it is sent. Record corrected statuses, misleading inferences, missed exceptions and review time. Watch for an attractive draft concealing an old event or the wrong shipment reference.

## DAYS 22 TO 30

### Rehearse and decide

Practice an outage and recovery with a safe test scenario. Confirm how manually completed work is reconciled when the assistant returns. Compare completed-task time and quality with the baseline. Continue only when operations and security can explain the results and accept the tested scope.

**Review group:** operations · customer data · IT and security · maritime or compliance specialist as applicable.

# Two conditions decide whether the pilot continues.

Write both of them down before the first operator sends an assisted update, not after the first wrong one.

## GATE ONE

### Control gate

Confirm the assistant cannot release cargo, edit consignee or banking details, or reach onboard systems. Check that a user cannot retrieve another customer's restricted shipment information. Keep a record of each test and of the configuration being evaluated.

## GATE TWO

### Pause conditions

Stop after unauthorized access, an unapproved consequential change, repeated wrong-shipment matching or loss of source traceability. Route the event through the organization's incident process. Restoring a model version is not enough if a message was already sent or a human action must be reconciled.

## Why rollback is harder here

In most pilots, reverting means switching a system off. In this one, an incorrect update may already be with a customer and may already have changed what someone else did. The recovery plan has to cover the messages, not only the software.

## What a pause should look like

A named person, reachable during operating hours, with the authority and the access to switch the assistant off without a committee. The manual queue should already have been rehearsed, so reverting is routine rather than disruptive.

**Rollback means restoring a trustworthy workflow, not merely selecting an older model.**

AGENTS STACK PERSPECTIVE

# Recover desk time before claiming demurrage savings.

Illustrative economics in Singapore dollars. These assumptions show how to test value, not how much any operator will save.

## ILLUSTRATIVE CAPACITY-VALUE EXAMPLE

# S\$1,375

Monthly net capacity value

# 5.1 months

Approximate setup recovery on a capacity-value basis

Planning assumptions in Singapore dollars; not necessarily cash savings.

### The base case

Assume 1,500 eligible exception updates each month and five minutes of net time saved on each, after source checking and correction. This creates 125 hours of gross capacity. At 65% useful redeployment, that becomes 81.25 hours. Value the time at an assumed S\$28 an hour.

### Make the cost visible

Monthly capacity value is S\$2,275. Deduct an assumed S\$900 for operation, data access, evaluation and routine support to get S\$1,375 net capacity value. An assumed S\$7,000 setup cost has a simple capacity-value recovery period of about 5.1 months.

## THE FOUR ASSUMPTIONS BEHIND THE FIGURE

### 1,500

Exception updates a month

Assumed volume.

### 5 min

Net time saved on each

After review.

### 65%

Usefully redeployed  
Not all of it is recovered.

### S\$28

Fully loaded hourly cost  
Assumed, not a quote.

# At two minutes saved, the case is gone.

The downside here is not a longer payback. It is break-even before you have paid for setup.

## The lower-value case

At two minutes saved per update and the same redeployment factor, monthly capacity value falls to S\$910. After S\$900 cost, only S\$10 remains. The model is effectively at break-even before setup cost, so a purchase would need better evidence or a different use case.

## Keep avoided fees out until proven

Do not add a speculative demurrage, detention or missed-departure benefit to make the case attractive. Establish what was actually paid, which event could have been prevented and whether the assistant caused a different outcome. Avoid double-counting time savings and the same operational benefit.

## Questions for a supplier

Can every status be traced to the original source and time? Which carrier feeds and document formats are actually supported? How are customer boundaries enforced? What happens when a feed is stale or unavailable? Can we export pending work without the vendor? Ask for the exception path as well as the ideal path.

## The responsible decision

An operations owner should replace each assumption with measured data. Compare with improved templates, existing transport-management-system features and rules-based alerts. Recovered capacity has value only when it is actually useful; it is not automatically a reduction in cash expenditure.

Original calculation:  $1,500 \times 5 \div 60 \times 65\% \times \text{S\$}28 - \text{S\$}900 = \text{S\$}1,375$  per month. Downside case: **S\$10** per month, before setup cost. Tax, financing and discounting are excluded.

# Give every exception an owner.

A conversation for the operations desk, technology team and business sponsor.

## Ask operations for five difficult cases

Choose examples involving a stale event, a revised document, conflicting dates, a wrong identifier and an instruction that required independent confirmation. Explain how the team resolved them. Those examples are more useful to a pilot than a large set of routine shipments with no uncertainty.

## Ask the data owner what is authoritative

Name the source of each key field and the rule for conflicts. Agree a time-zone convention and display the freshness of each event. Document when an operator must stop and check with a counterparty rather than accept the assistant's inference.

## Ask security where the boundary is

Can the assistant create drafts without the right to issue consequential instructions? Is customer access enforced outside the model? Who can revoke a connector? How would the team notice that a source or identity had changed?

---

### WHO HAS TO BE IN THE ROOM

#### 01

##### Operations owner

Brings the five difficult cases.

#### 02

##### Data owner

Names what is authoritative.

#### 03

##### Security

Owns access, logging and the pause.

#### 04

##### Resilience owner

Runs the outage rehearsal.

# Rehearse the outage in the same meeting.

Recovery discipline belongs in the acceptance test, not in a document nobody opens.

## Ask the resilience owner to pull the plug

Rehearse loss of the assistant in a controlled setting. Make sure the manual queue, trusted contacts and reconciliation process work. NIST's small-business CSF resources include response and recovery alongside preventive controls. [6] Our recommendation is to make that recovery discipline part of the pilot acceptance test.

## Ask the sponsor for one outcome

Choose the task the team wants to improve, the minimum meaningful benefit and the non-negotiable quality conditions. Do not mix a shore-side operations pilot with promises of vessel autonomy or port-wide optimization. Those are different programs with different evidence needs.

## The question to take to your team

Which repeated shipment exception could be resolved faster if the right evidence were assembled automatically, while every instruction that changes cargo, money or safety still follows the approved process?

## What to leave the meeting with

One trade lane, a named operations owner, an agreed pause condition and a date for the outage rehearsal. If any of the four is missing, the proposal is not yet testable.

**Useful automation reduces uncertainty. It does not hide it.**

AGENTS STACK PERSPECTIVE

**Planned next edition:** healthcare and life sciences. Internal knowledge, sensitive data and evidence-led AI adoption. Not yet written or researched in this pack.

# Evidence you can inspect.

Numbered references match the articles. All sources were checked on 11 September 2026.

---

## [1] Singapore's first Maritime Digital Twin is live

GovTech Singapore · official LinkedIn account · Exact publication date not displayed

First-party government project account. Describes MPA and GovTech capabilities; benefits are not independently measured here.

---

## [2] Bill of Lading standard

Digital Container Shipping Association · Living standards page; accessed at cut-off

Industry standards body. Technical and legal interoperability work; not universal legal recognition of every electronic document.

---

## [3] MSC-FAL.1/Circ.3/Rev.3: Guidelines on maritime cyber risk management

International Maritime Organization · 4 April 2025

Official maritime guidance. Primarily intended for ships; consult applicable flag Administration requirements and relevant standards.

---

## [4] Maritime cyber risk

International Maritime Organization · Living guidance page; accessed at cut-off

Official guidance index. Provides context on cyber risk and safety-management-system integration.

---

## [5] LLM06:2025 Excessive Agency

OWASP GenAI Security Project · 2025 risk taxonomy

Community security guidance. Highlights excessive functionality, permissions and autonomy.

---

## [6] NIST Cybersecurity Framework 2.0 for Small Business

NIST · Page updated 17 April 2026

Small-business guidance. A framework and quick-start resources, not a compliance certification.

---

### EDITORIAL NOTES

Reported examples are attributed to their sources. The SME scenarios, pilot plans and decision questions are original editorial proposals, not verified Agents Stack customer results. All cost examples use explicit assumptions, not market prices or promised returns.

This magazine does not provide legal, financial or safety certification. Publication requires a named editor's approval and a final source check. No affiliation or endorsement by cited organizations is implied.



NEXT IN THE SERIES

# 9 October • Healthcare & life sciences

Internal knowledge, sensitive data and evidence-led AI adoption. Planned, and not yet written or researched.



**Agents Stack**

One industry. Useful AI. Accountable cybersecurity.

[agentsstack.com](https://agentsstack.com)