Implementable Approach for SWIM Message Exchange over CRV

Xiaodong Lu
Surveillance and Communications Department
Electronic Navigation Research Institute, Japan

January 14~17, 2025

Agenda

1. Current Status

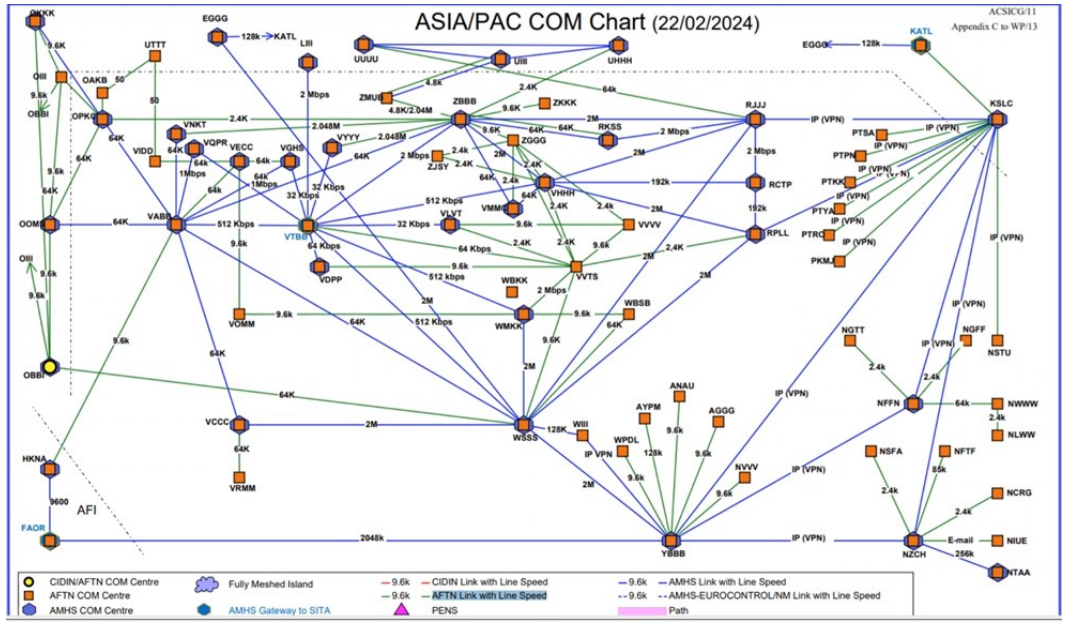
2. Implementable Approach

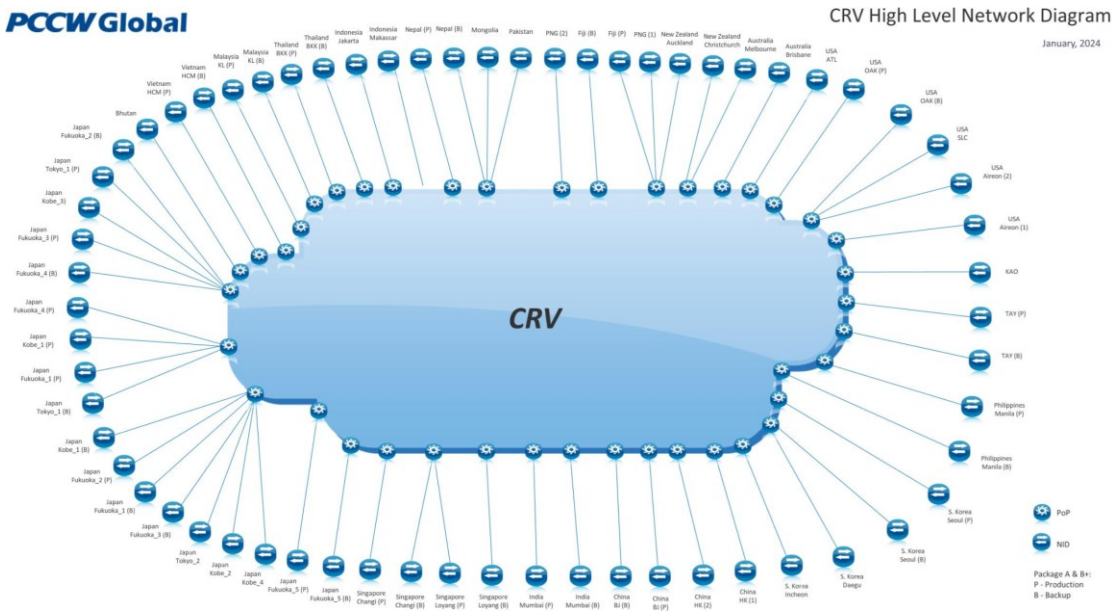
3. Technical Problems

4. Summary

Current Status

➢ Current Structures



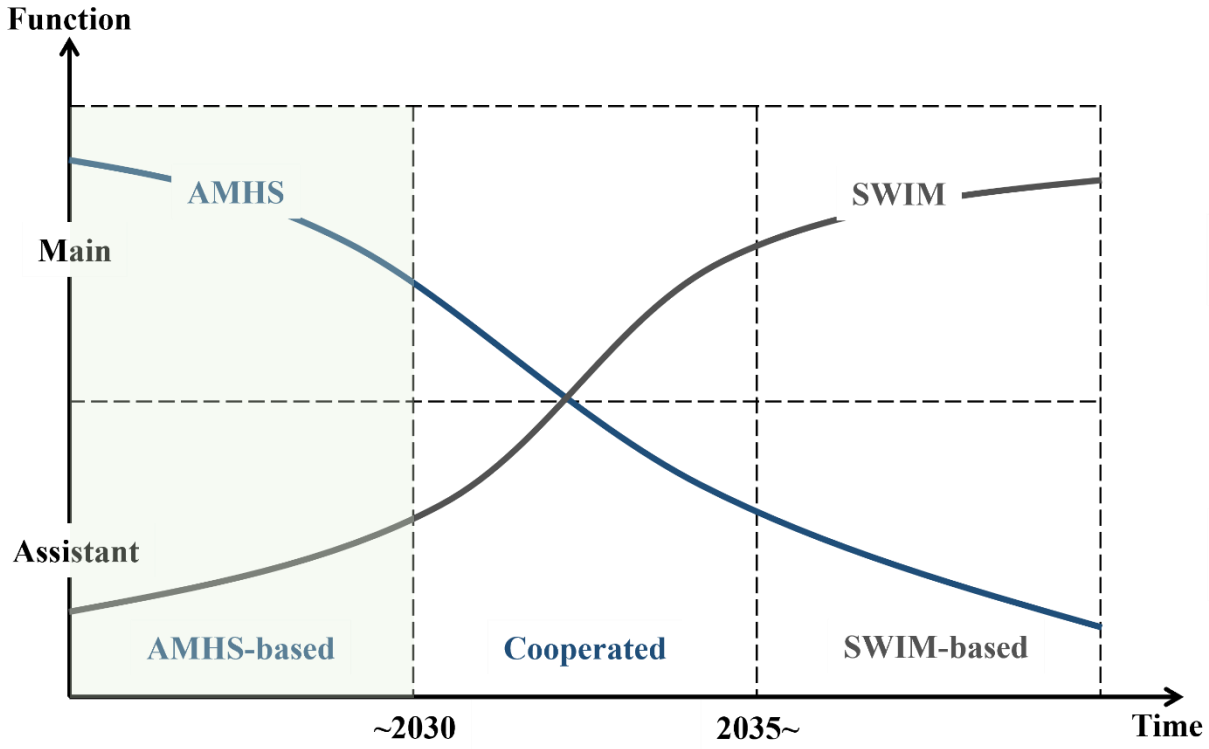


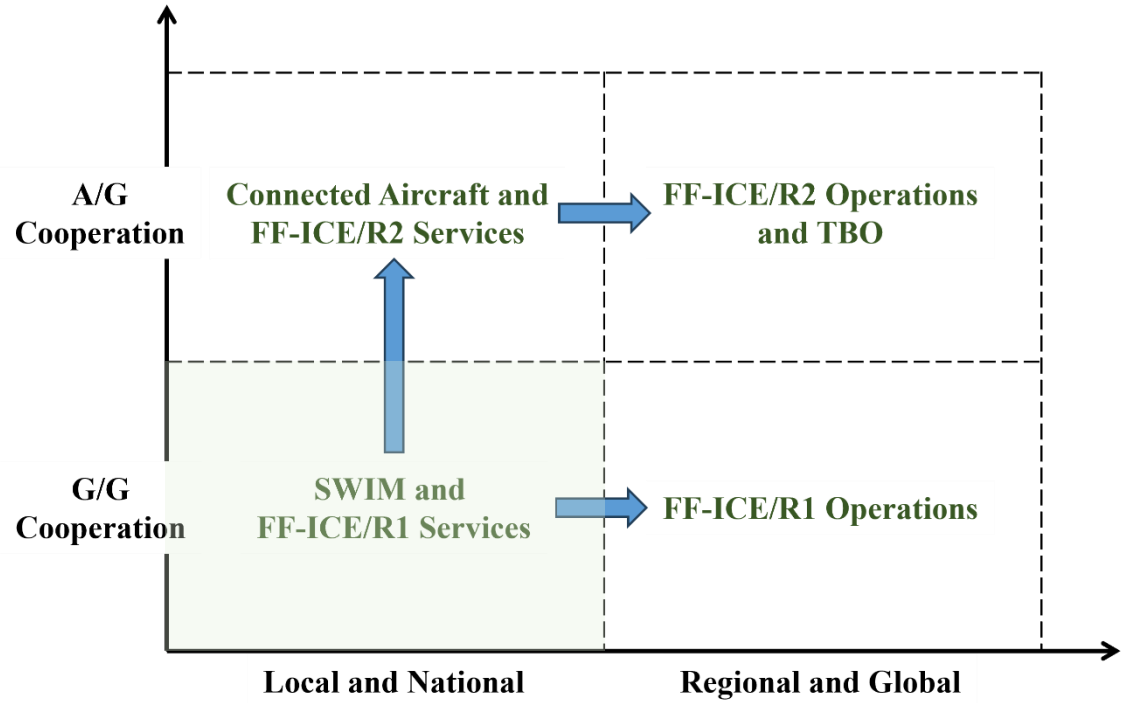
- Static IP address
- Static connections
- Static bandwidth

- Static IP address
- Changeable connections
- Changeable bandwidth

Current Status

➢ **Where we are, Where we need to go, How we can get there**





From AMHS to SWIM

From Local to Global

Agenda

1. Current Status

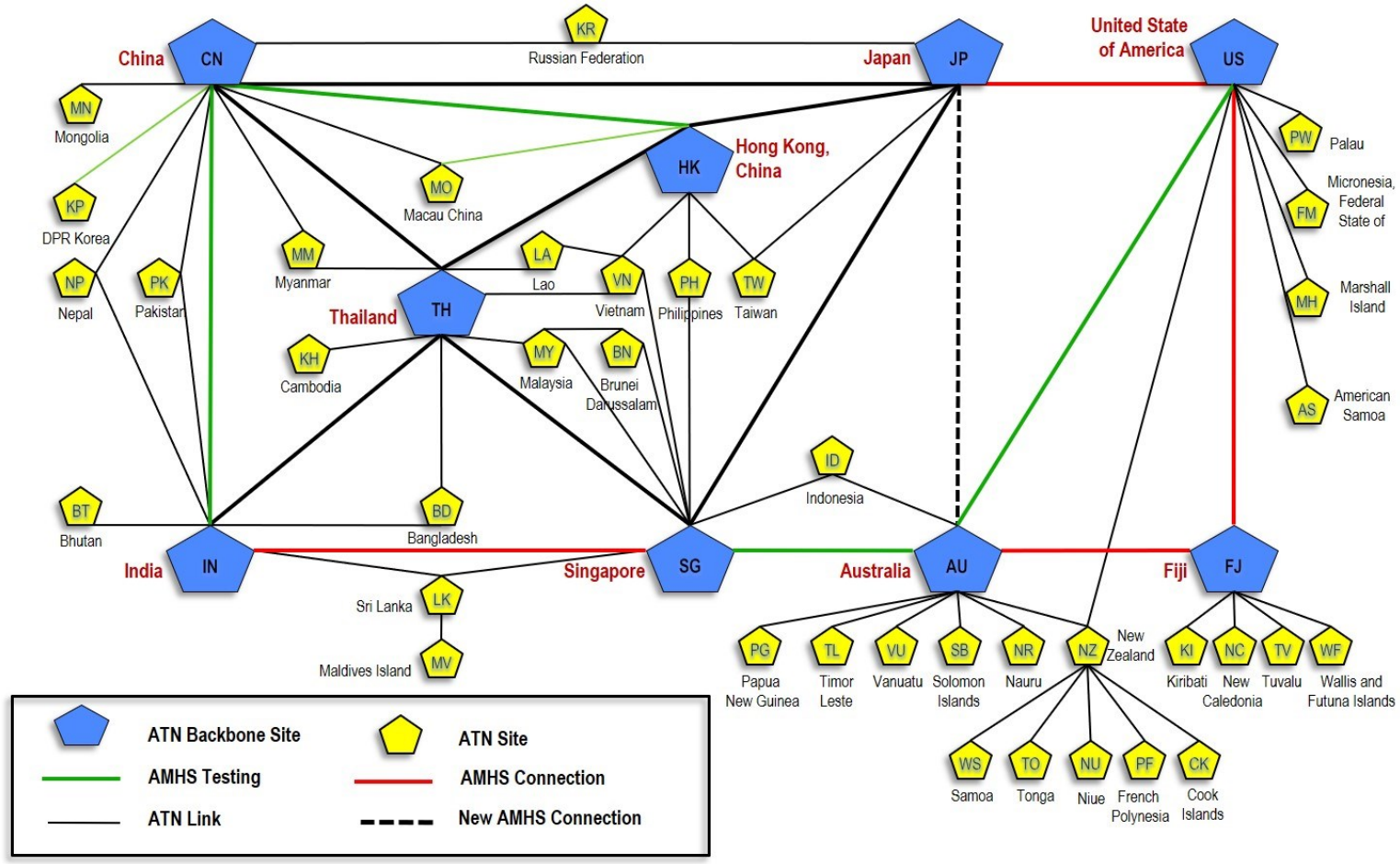
2. Implementable Approach

3. Technical Problems

4. Summary

Implementable Approach

➢ AMHS-based Operations with SWIM



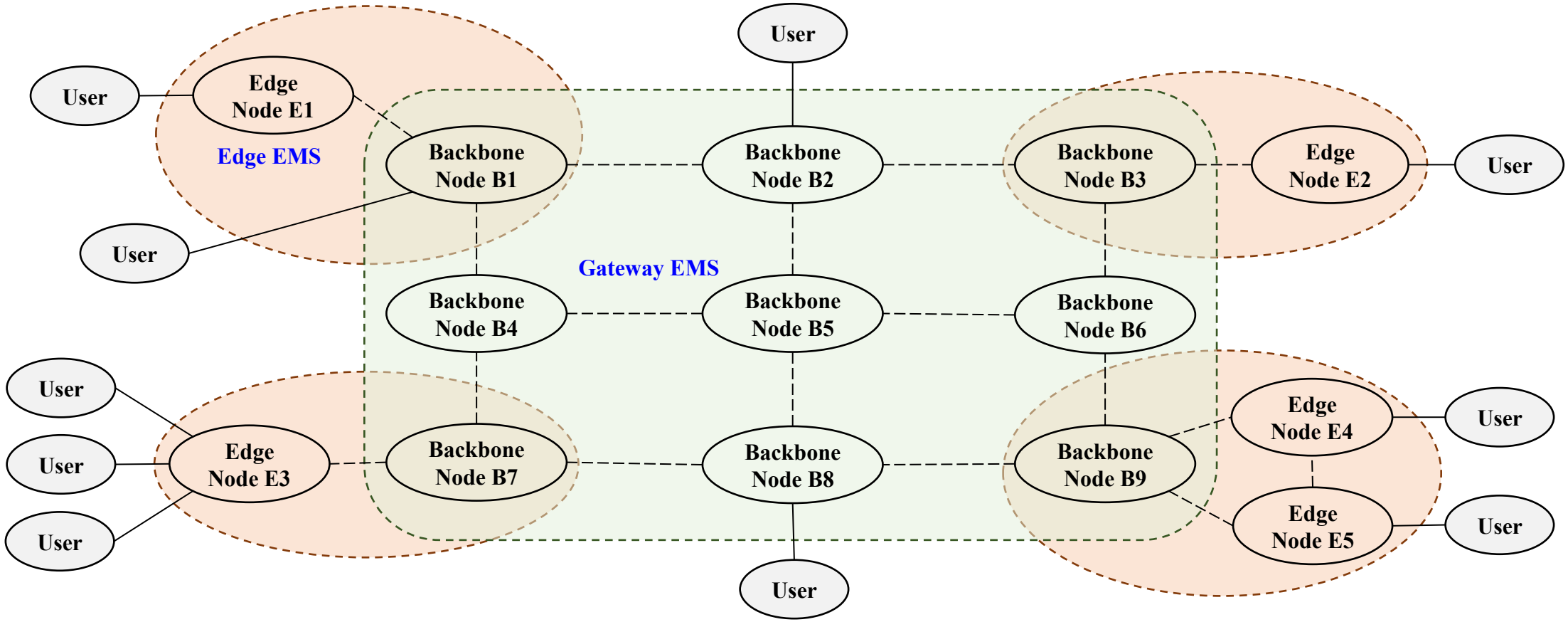
Requirements:

- **No impact on current AMHS based message exchange**
- **Easy to implement SWIM based information sharing**
- **Low cost to maintain and manage both systems**

Same Structure with various Interface Bindings

Implementable Approach

➢ Backbone Nodes serve as Gateway EMS



Agenda

1. Current Status

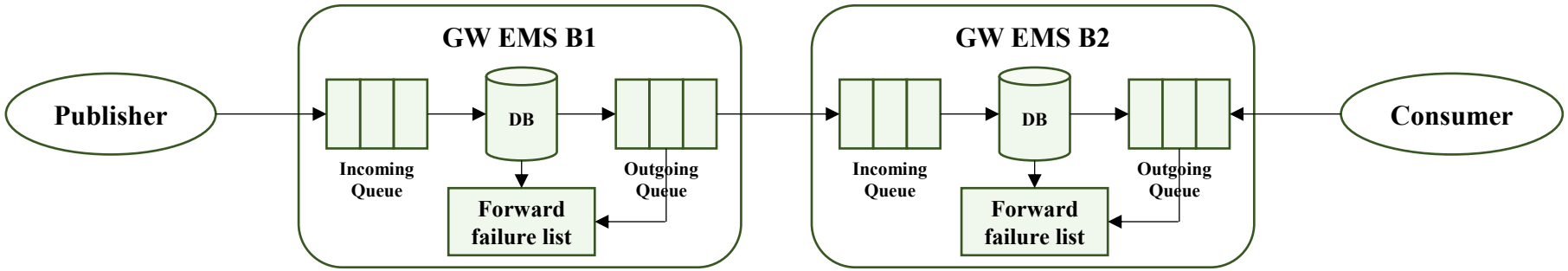
2. Implementable Approach

3. Technical Problems

4. Summary

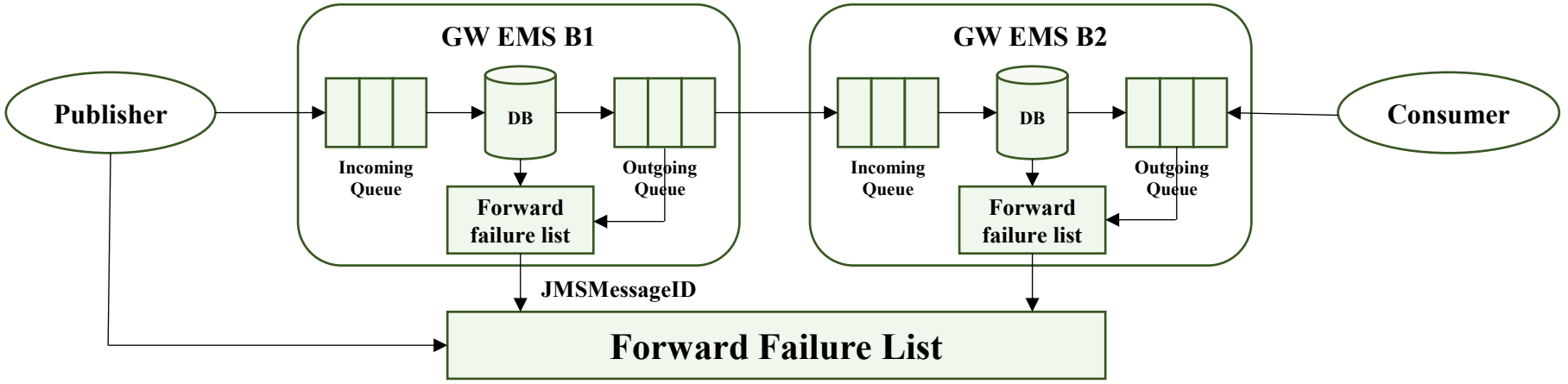
Technical Problems

Problem	Use case	Solution
1. Priority messaging is not possible depending on the importance of the information	Surveillance messages caused queue overflow and loss of FF-ICE messages.	• Deliver surveillance messages using a separate queue and logical network • Set a message TTL for surveillance messages
2. Guaranteed message delivery is destroyed when malfunctioning of a message broker occurs in the message delivery chain	When the message broker reaches the maximum number of messages, it drops subsequent messages.	• Set up a staging DB between incoming queue and outgoing queue • Peek & Lock, Receive & delete
3. Compensation transactions cannot be performed to compensate transaction failure in the message delivery chain	The publisher is not aware of failures that occurred in the EMS afterwards.	• Implement retry logic for failed message deliveries • Record Forward Failure List for traceability



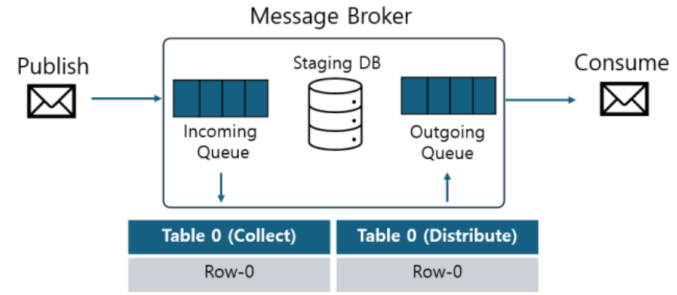
Technical Problems

Problem	Use case	Solution
4. Detouring cannot be performed if a failure occurs in the message delivery chain	The publisher is not able to change delivery responsibility even if the publisher recognizes a failure in the message delivery chain.	• Set a backup EMS for each publisher and Edge EMS • Each Gateway EMS has at least two connections to other Gateway EMS
5. The edge node does not know which message to resend when message loss occurs	In the case of a missing message that occurs in a subsequent EMS, the publisher cannot specify the message and try to resend it.	• Publish the Forward Failure List, making it accessible to publishers • Subscriber responds “Submission Response” to the publisher



Technical Problems

➢ Discussions

Vulnerabilities	Troubleshooting	
Priority messaging is not possible depending on the importance of the information	OSI 3rd Layer (Network)	Queueing algorithms in the OSI 3rd layer typically prioritize packets based on various factors, including Quality of Service (QoS) requirements, packet type, and destination. Queueing plays a crucial role in managing packet traffic, minimizing delays, and maintaining the quality of service.
	OSI 7th Layer (Application)	Message brokers (e.g., RabbitMQ) support message prioritization through the use of message priorities. Prioritized messaging allows to ensure that messages with higher priorities are consumed before messages with lower priorities.
Guaranteed message delivery is destroyed when malfunctioning of a message broker occurs in the message delivery chain	OSI 3rd Layer (Network)	Leaky bucket algorithm serves as a method to control the rate of data flow into the buffer, thereby managing congestion and ensuring a consistent data transfer rate.
	OSI 7th Layer (Application)	JMS Server with staging DB is one of the de-facto architectural patterns for reliable messaging. Incoming queue is only to receive message from publisher and out coming queue is only to send message to consumer. There is staging DB between incoming queue and outgoing queue, so it acts like an buffer. 

Technical Problems

➢ Discussions

Vulnerabilities	Troubleshooting	
Compensation transactions cannot be performed to compensate transaction failure in the message delivery chain	OSI 7th Layer (Application)	Saga pattern is a design pattern used in distributed systems to maintain data consistency across multiple microservices or transactions. It's particularly relevant in the context of Event-Driven Messaging (EDM) architectures, where services communicate asynchronously through events. This consistency is achieved by executing conservative transactions for failover such as pivot, compensable, retriable transaction.
Detouring cannot be performed if a failure occurs in the message delivery chain	OSI 3rd Layer (Network)	OSPF (Open Shortest Path First) is a dynamic routing protocol commonly used in large-scale enterprise and service provider networks. OSPF provides several mechanisms for creating detour routes within a network to optimize traffic flow, enhance network resilience, and mitigate congestion or failures.
The edge node does not know which message to resend when message loss occurs	OSI 3rd Layer (Network)	Automatic Repeat reQuest (ARQ) is a communication protocol technique used to ensure the reliable delivery of data packets over unreliable communication channels. One of the primary functions of ARQ is to detect and resend lost or corrupted packets
	OSI 7th Layer (Application)	In the FF-ICE, the message type “SUB_RESP” is generated by recipients enlisted in the FF-ICE message to notify if the message is received to message originator

Agenda

1. Current Status

2. Implementable Approach

3. Technical Problems

4. Summary

Summary

➢ New Considerations

Operation Concept	▪ TBO (Trajectory Based Operations) - 4-Dimentional Trajectory	ICAO ATM Requirements and Performance Panel (ATMRPP): Operation Approach
	▪ FF-ICE (Flight and Flow Information for Collaborative Environment)	
Information Infrastructure	▪ SWIM (System Wide Information Management) - Messaging Infrastructure - Information Exchange Models - Information Services	ICAO Trust Framework Panel (TFP): Information Security ICAO Information Management Panel (IMP), APAC SWIM Task Force: SWIM Implementation
Communication Infrastructure	▪ IP based Connectivity - Ground-to-Ground Communication Network - Air-to-Ground Data Link	ICAO Cybersecurity Panel (CYSECP): Comms. Security ICAO Communication Panel (CP): IP-based Communication Network


Thank You!