Designing a Maritime Cybersecurity Risk Intelligence Model with Generative AI and Real-Time Interviews

Jake Townsend, Bilge Karabacak, Ulku Clark, Kasey Miller, & Hosam Alamleh

Cameron School of Business

&

College of Science/Engineering

UNC Wilmington

Agenda

- Introduction
- The Why
- Data Sources
- Components and Agency
- Challenges
- Future Path
- Questions/Comments

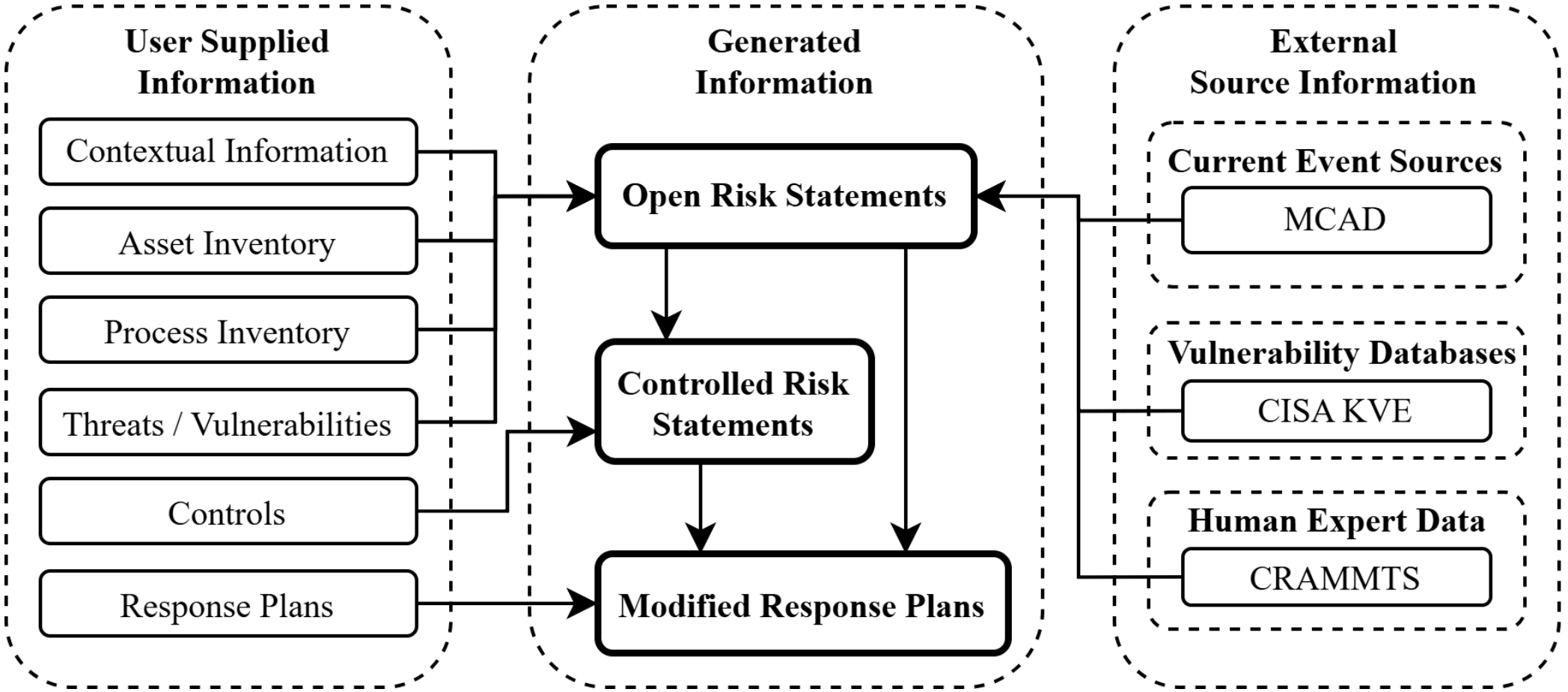
Why?

Maritime Cybersecurity risk assessments require:

- A large upfront time investment
- Expert evaluators and analysts
- Fully knowledgeable staff in the target organization

We seek to streamline one/more portions of the risk assessment process via LLM-powered tools.

Data Sources



Structure Planning

- We need to define a balance:
  - Flexibility for variance in user-defined and external source data.
  - Rigidity/Structure for consistent risk assessments to be conducted.
- LLMs are still not very good at tasks which require many sub-tasks:
  - How to break down the process of gathering, analyzing, and documenting risk?
  - How to minimize need for human-in-the-loop?

Structure Planning

- Three Main Components:
  - Interview Node
  - Analysis Node
  - Documentation Node

- Keep the tasks small and manageable
- Allow for addition/subtraction of components
- Reflect an already established process

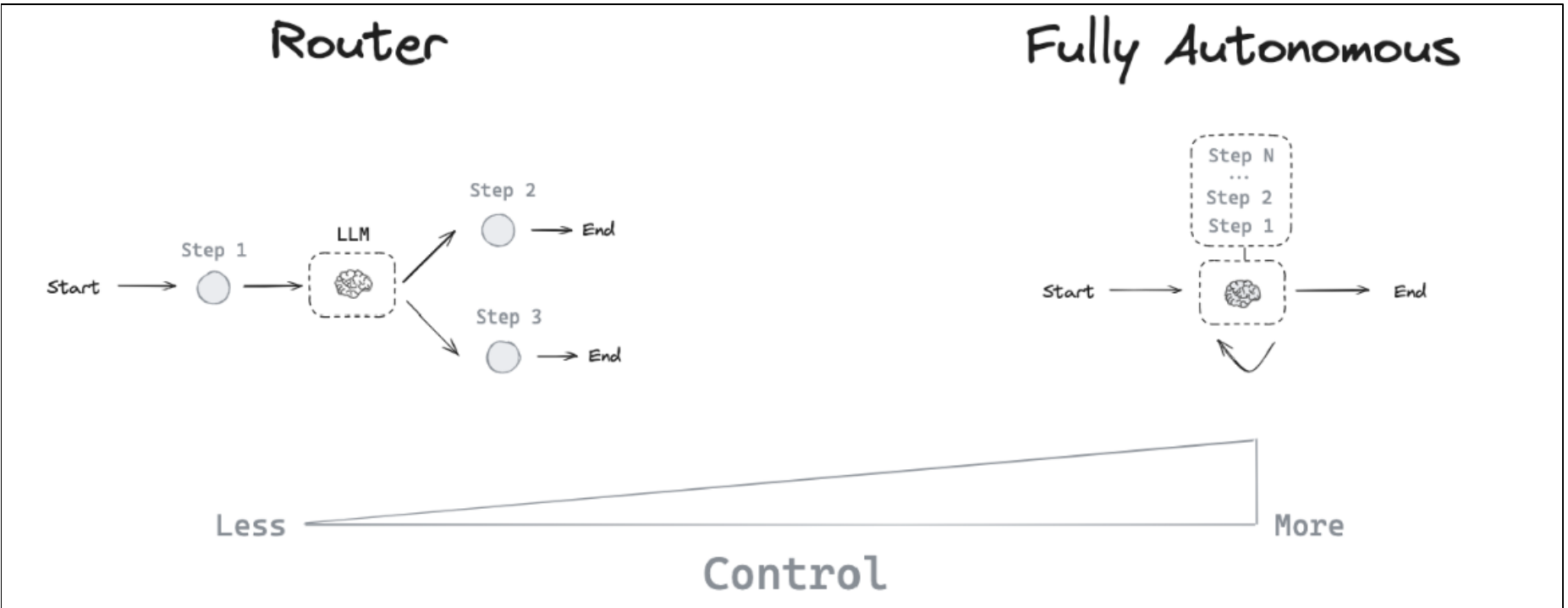
A Note on Components

- Components/Workflows/Agents can be used interchangeably.
  - It is acknowledged that definitions are still debated, although clearer definitions are emerging.

- Is this just an LLM wrapper?
  - The components leverage LLMs for the main functionality.
  - Multiple LLMs are chained together to allow for decision-driven routing.

A Note on Agency

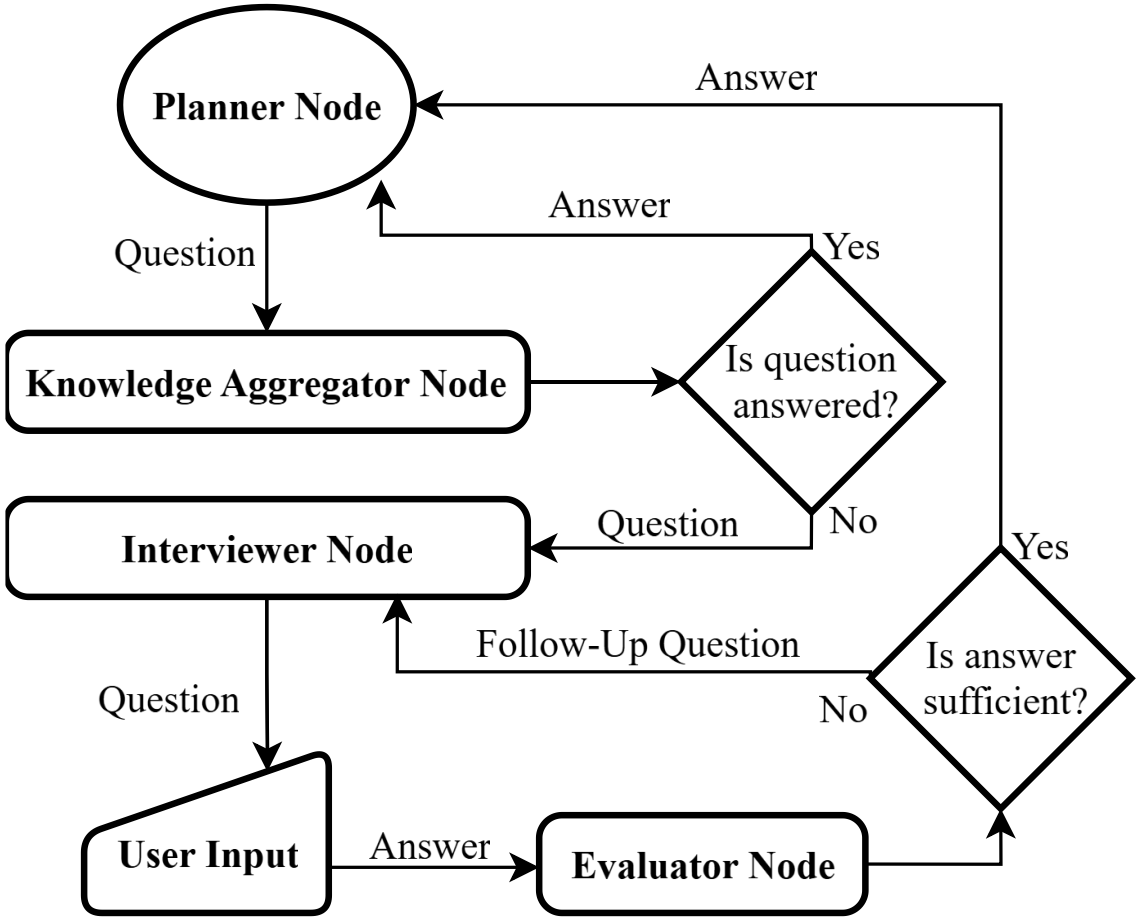
- AI Agency != AI Omnipotence
- Agency for us is simply making a decision based on observation(s).
- ReAct – Reason & Act
- https://blog.langchain.com/what-is-a-cognitive-architecture/



Source: https://langchain-ai.github.io/langgraph/concepts/agentic_concepts/

Interview Component

- How do you prompt an LLM to gather information from the user?
- “Prompt engineering” isn’t enough.
- Relying on one LLM alone is like relying on one human solely relying on memory.
- We need a reliable process that prompts for and stores information from the user.



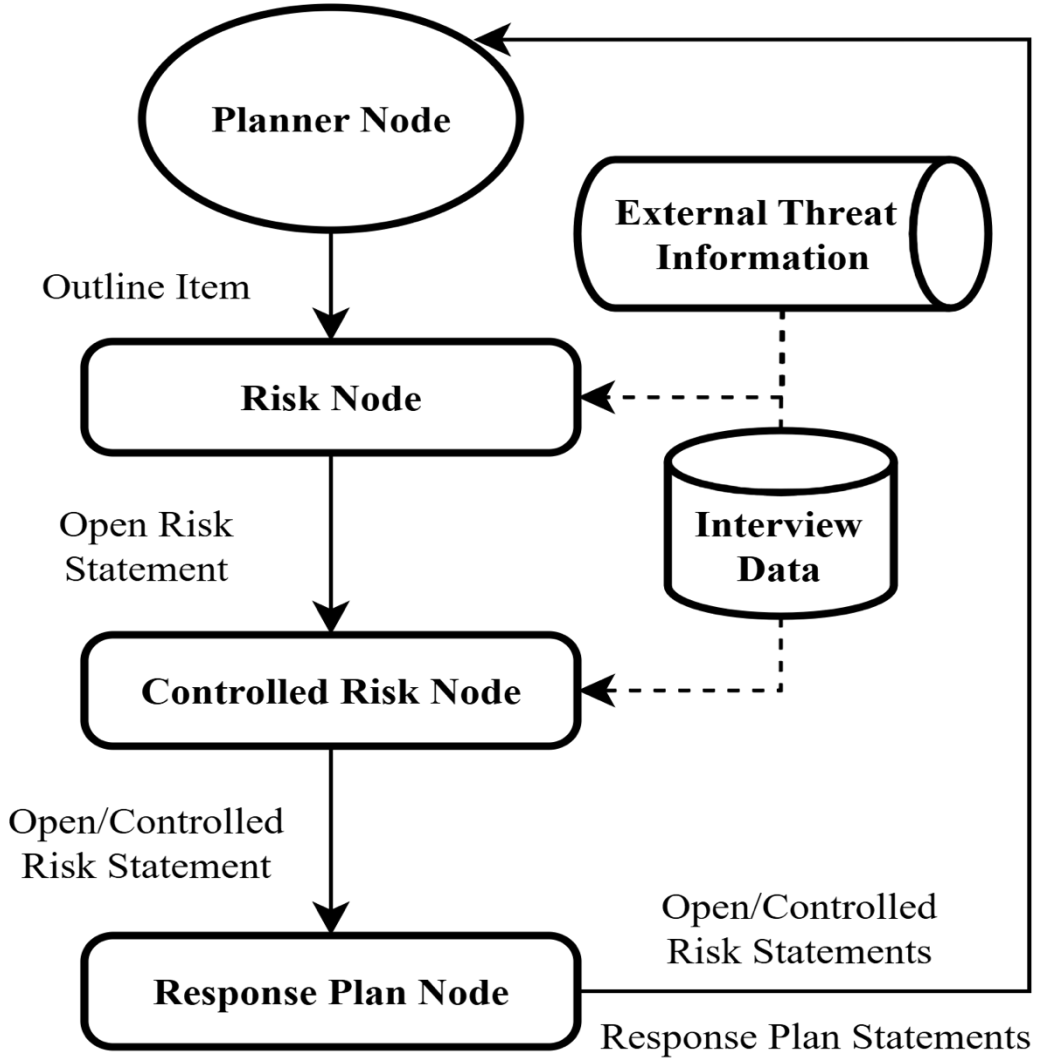
Interview Component

Behaviors we want to avoid:

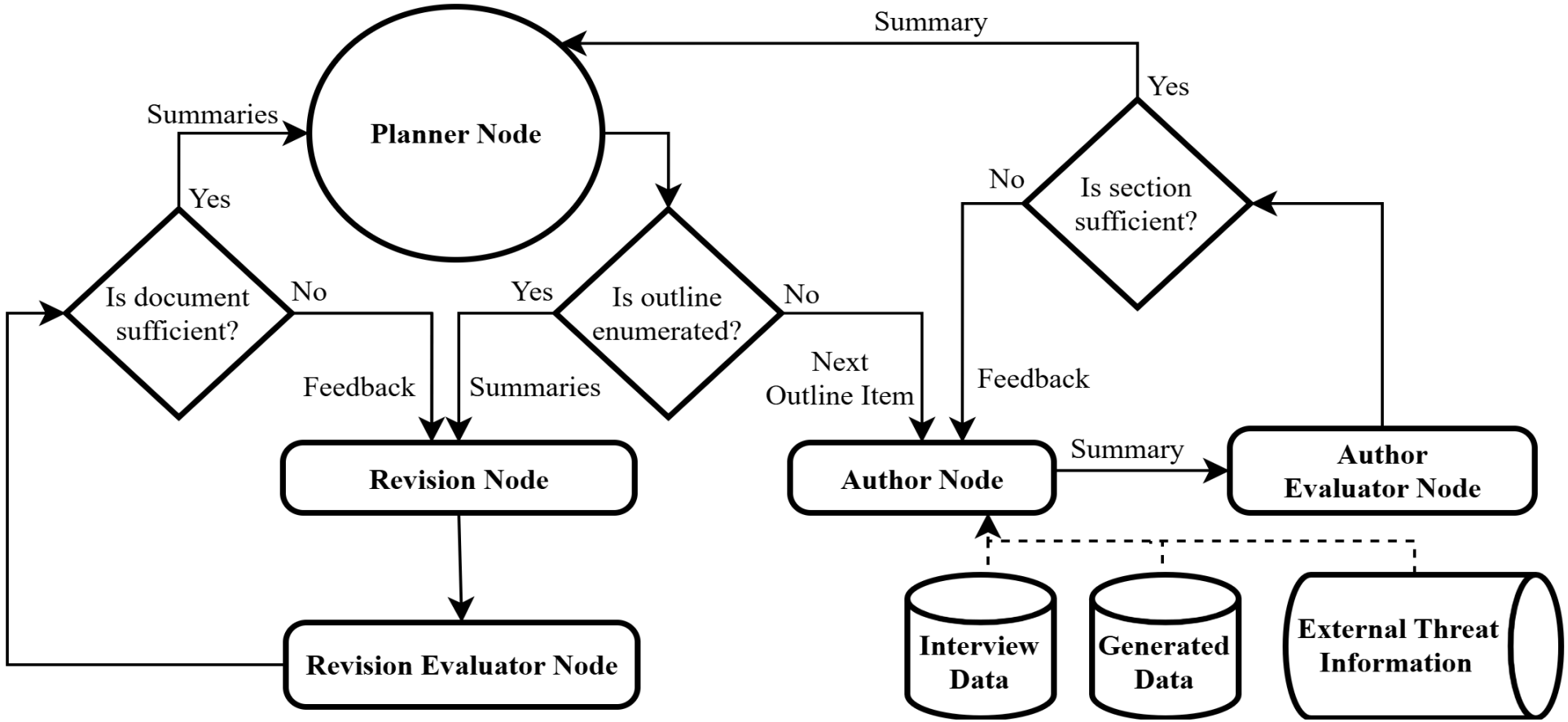
- Redundant questions
  - Q: Do you currently have anything to monitor your AIS systems?
  - A: Yes, we have system XYZ which monitors for AIS spoofing as well as geofences…
  - Q: Do you monitor for AIS spoofing?
- Vague answers
  - Q: Do you currently have anything to monitor your AIS systems?
  - A: Yes
- The “six-year-old” interviewer
  - Q: Do you currently have anything to monitor your AIS systems?
  - A: No, we do not.
  - Q: Why not?

Analysis Component

- How do we analyze the information provided to determine risk?
- External data sources become extremely important here.
- Open risk items should first be generated to influence controlled risk statements or response plan recommendations.

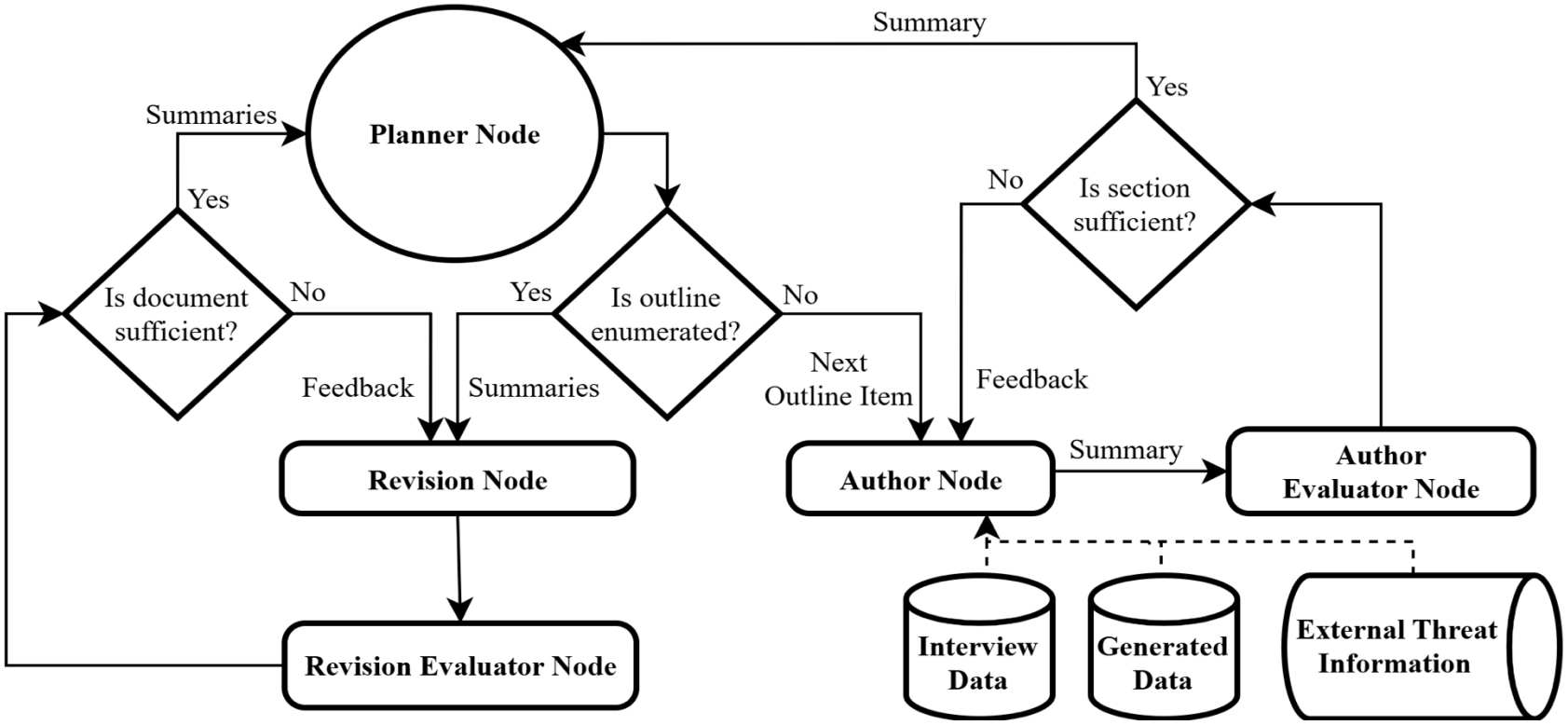


Documentation Component



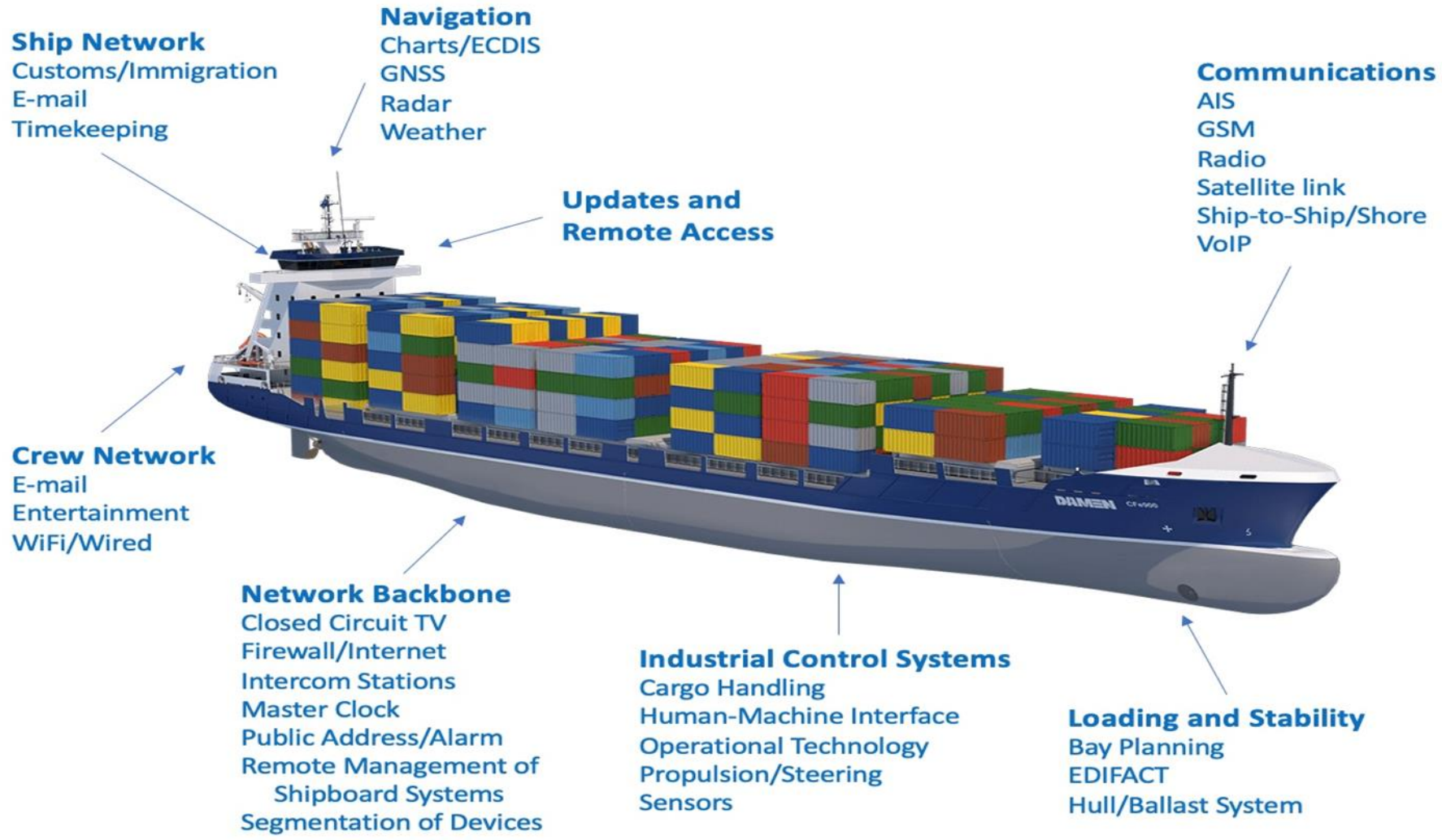
Documentation Component

- The last piece is to generate a document.
- We can take all the data collected and generated to make the final document.



Use Case for Cybersecurity Risk Intelligence

- Explore Chip to Ship Vulnerabilities
- Explore Port Vulnerabilities
- Assist in Zero Day (Unknown attacks).



Source: Gary Kessler and Steven D. Shepard. 2025. *Maritime Cybersecurity: A Guide for Leaders and Managers*. Ormond Beach, FL: Independently published

Challenges

- LLMs are not good at saying, “I don’t know”
  - This is of course by nature since LLMs don’t actually “think”.
  - This causes hallucinations.
- Early agents can be unpredictable in their tool calls
  - Sometimes they seek answers via RAG, and other times they don’t.
  - This is one reason we’ve looked more heavily into constrained workflows.

Future Path

- More data to ingest more Maritime Data:
  - Current events
  - Threat databases
  - Internal reports
  - Physical/Virtual Naval Asset Manifests
- Exploration of new frameworks/packages
  - Deep Research
  - Swarm
  - Etc.

Questions and Comments

Contact info:
jmt9454@uncw.edu
karabacakb@uncw.edu
clarku@uncw.edu
millerkc@uncw.edu
alamlehh@uncw.edu