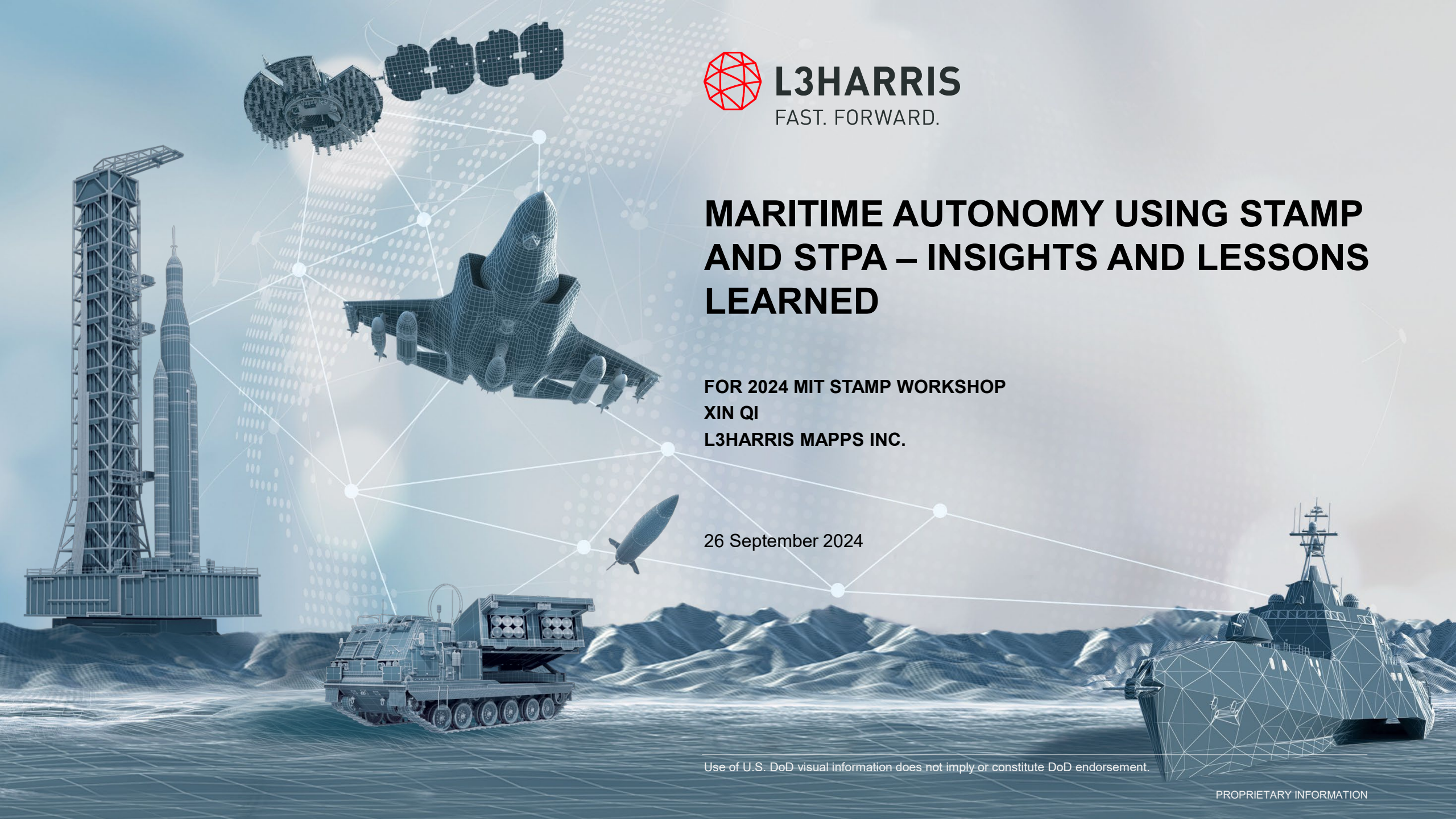


L3HARRIS
FAST. FORWARD.

MARITIME AUTONOMY USING STAMP AND STPA – INSIGHTS AND LESSONS LEARNED

FOR 2024 MIT STAMP WORKSHOP
XIN QI
L3HARRIS MAPPS INC.

26 September 2024

Introduction

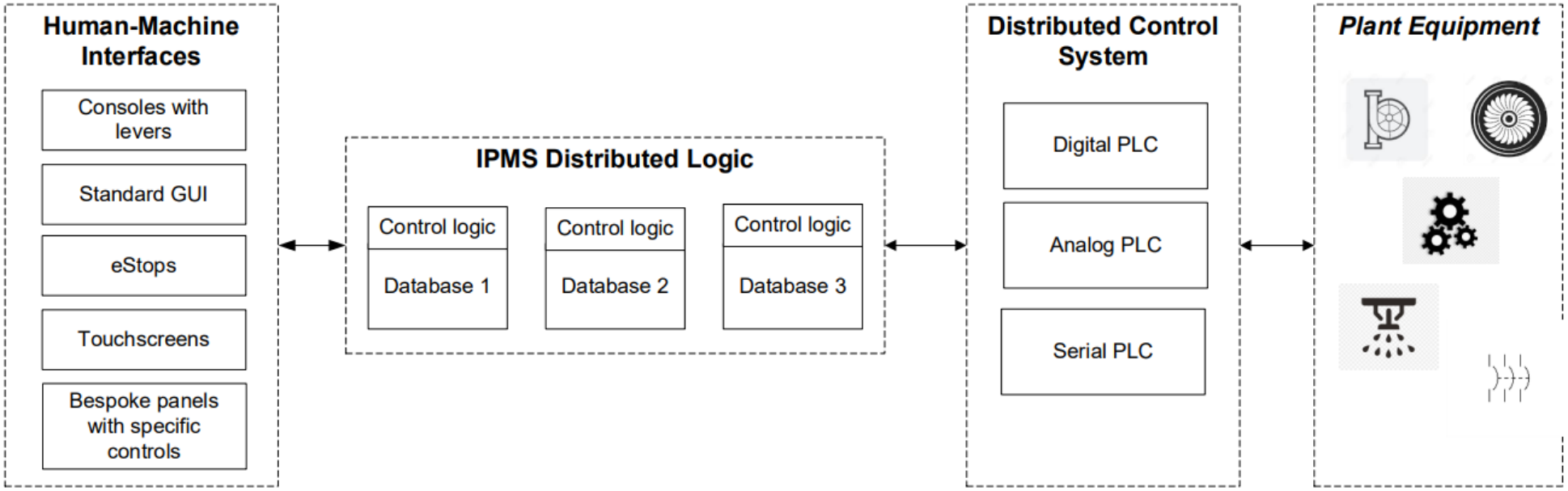
Presenter Background

- My name is Xin Qi.
- I work at L3Harris MAPPS Inc. (a subsidiary of L3Harris Technologies Inc.) as Senior Systems Safety Architect.
- Professional focus in design and development of safety-related (and safety-critical) software systems.
- TUV-Certified Functional Safety Expert.
- UL-Certified Autonomy Safety Professional.
- Email contact: Xin.Qi@can.l3harris.com

About L3Harris MAPPS Inc.

- Based in Montreal, Canada.
- Specializes in integrated control systems and simulation solutions for naval vessels.
- Integrated Platform Management System (IPMS)
- IPMS is a very successful product that has been exported and delivered to many navies around the world and used onboard hundreds of vessels.

What is an Integrated Platform Management System (IPMS)



IPMS usually consists of three major layers:

1. A Distributed Control System (DCS) layer, interfacing to a variety of ship machinery / plant equipment via Remote Terminal Units (RTUs).
2. A logic layer, based around a distributed, failure-tolerant database which synchronizes and can undertake automatic functionality in response to changes in data received via the DCS layer.
3. A Human-Machine Interface (HMI) layer, consisting of both bespoke control interfaces (levers, buttons) and standardized GUI interfaces (via keyboard / mouse / touchscreen).

IPMS has been interfaced to a wide range of systems, from firefighting / damage control to power and propulsion machinery.

This slide is taken from “Assuring Maritime Autonomy Through STPA and STAMP”, Slide 4, by Dr. Giles Howard, presented at the 2020 MIT STAMP Workshop on 20 July 2020.

Motivation - Why STPA?

To date, we have managed to justify our safety arguments mainly with traditional safety analyses, but it is becoming evident that there may be potential gaps when applying traditional safety analyses on the IPMS system. Therefore we have explored the use of STPA as an improvement to our development process.

Some factors that motivate the use of STPA:

- increasing complexity in modern warships.
- better adaptability with emerging technologies.
- to improve Safety Culture within the organization.

Simple example of using STPA[1] [2]

Take an example of a ship control and monitoring system for this analysis. This system requires human and automated control coordination. System performs automated controls depending on sensors' inputs, and operator can choose to interact with the system by monitoring ship status on console displays and visual environment to make control decisions.

- The objective is to perform STPA on interaction between automated controls and operator actions. For this example, the focus is on conflicting commands issued by the system and what is wanted by human operator.

Scenario description:

System automation provides command to increase turbine speed command when it detects turbine speed drops during heavy sea conditions. It does this because sensor inputs indicate a drop in turbine speed and more power is required to maintain speed. However, the operator may want to command a reduction in ship propulsion as ship approaches an unexpected congested area. The operator does this based on experience and believe reducing propulsion is necessary to safely navigate through the congested area. Another conflicting command scenario is when operator wants to command a reduction of turbine speed to prevent excessive strain on system during heavy sea conditions based on understanding of the limits of propulsion system.

Without appropriate mitigation measures, the conflicting actions could lead to hazardous conditions.

Loss:
- Loss of life or injuries
- Equipment damage
- Loss of mission capability (operational downtime)

Hazard:
- Ship does not maintain safe distance from other vessels
- Ship enters dangerous/shallow water area
- Ship exceeds safe operating envelope for environment

1. While the STPA analysis was performed for the design of the IPMS, findings presented in this presentation have been generalized, this is to make sure no confidential information of the IPMS is made public through this presentation.
2. At this stage, there is no formal requirement to adopt the STPA method in the current process at L3Harris MAPPS Inc.. As such, STPA is being applied as an informal analysis, results and findings from STPA are being used as supplementary to the primary design analysis.

Simple example of using STPA[1] [2]

Unsafe control actions (UCAs) include automated system issues conflicting commands while operator is trying to perform safe maneuver to control the ship. Operator does not provide correct override (control mode change) procedure when there are conflicts in command.

Causal factors include inadequate training for operator to operate the system, poor/confusing HMI interface design, overwhelming alert and warning display on console monitor.

Mitigation strategies from analysis:

- ✓ Implementing an alarm processing technique that reduce operator loading by filtering out nuisance alarms and providing well prioritized and context-sensitive displays (i.e. operation mode).
- ✓ Implementing audible and visual annunciation to alert operator of critical alarms and warnings and requiring operator acknowledgement for critical alarms and warnings.
- ✓ Improvements to operator training and operator guide on critical operations.

Conclusion: STPA helps to reveal potential limitations by not only considering the system design but also the operational interactions between human operator and system automation. With the findings from STPA, we can implement targeted mitigations to enhance safety.

1. While the STPA analysis was performed for the design of the IPMS, findings presented in this presentation have been generalized, this is to make sure no confidential information of the IPMS is made public through this presentation.
2. At this stage, there is no formal requirement to adopt the STPA method in the current process at L3Harris MAPPS Inc.. As such, STPA is being applied as an informal analysis, results and findings from STPA are being used as supplementary to the primary design analysis.

Lessons learned

Lesson Learned: STPA has been helpful in designing system around control actions and interactions

- This has been very effective for IPMS or any system that interact extensively with other systems.
- STPA can be used to analyze the interaction between human operator and the automated system.
- Findings are used to derive operational requirements required for operator to safely operate a system.
- STPA allows all stakeholders to contribute to the analysis as it does not require a thorough understanding of the design to start STPA analysis.

Lesson Learned: STPA has been effective to derive design requirements for human machine interfaces.

- STPA findings highlighted the importance of human factors in design analysis.
- The assessment of human interactions with IPMS has been identified as an important element for design considerations.
- Well-designed HMI interface with great clarity and well prioritized display of information help operators to respond more effectively during unexpected conditions and therefore improving safety.

Insights: Benefits of STPA

The following are benefits we observed from applying STPA:

1. Effective for complex system analysis.
   - STPA is effective in analyzing interactions between various subsystems in complex systems.

2. Reduce operational risk and enhance design safety.
   - STPA goes beyond hardware and software failures to consider organizational, human and environmental factors, which helps to identify risks from operational procedures.

3. Applicable throughout the development lifecycle.
   - STPA can be implemented anytime in the development lifecycle and even for in-operational systems.

4. Improves communications among all stakeholders.
   - STPA offers a common framework of analysis for all stakeholders.

Insights: Current Limitations of STPA

The following are current limitations we observed from applying STPA:

1. Time and resource intensive for proven systems with legacy development without STPA.
   - High initial learning curve for training and culture shift within organization.
   - Impractical to conduct training for everyone on STPA (time and resource issues).

2. Requires Expertise in Systems Theory
   - STPA's core concepts are built on principles of how complex systems behave, interact and controlled. It is difficult to fully utilize STPA without solid understanding of systems theory.
   - Difficult to hire professionals with expertise in systems theory and STPA.

3. Automation tools for STPA are limited
   - There are only a limited number of automation tools tailored for STPA.
   - STAMP Tools | MIT Partnership for Systems Approaches to Safety and Security (PSASS)

4. Difficult to translate STPA findings into specific evidence for certification purpose
   - Although findings from STPA can be used to support safety argument for certification purpose, there is a lack of clear requirement from certification organizations to adopt STPA as formal analysis.

Insights: Evaluation and Comparative Studies with Traditional Approaches

1. In-depth focus on system interactions rather than focusing on individual component.
    - From analysis we identified potential hazards that are from unintended interactions between subsystems. Traditional approaches (i.e. FMEA and FTA) tend to focus more on individual components or individual failure modes which will miss accidents and failures due to system-wide interactions.

2. Accounts for Emergent Behavior of Complex Systems
    - Complex systems (for example the IPMS system) often exhibit emergent behaviors, where the collective operation of different subsystems may lead to outcome that cannot be accurately analyzed by analyzing individual parts in isolation. Traditional approaches tend to miss emergent behaviors as they focus on linear cause-effect relationships of specific subsystems and not the entire system as a whole.

3. Potential Time- and Cost-Efficient in the long run for Complex Systems
    - From experience, safety issues from system interactions and emergent behavior are usually detected late in the development lifecycle, mostly from integration tests. Late-stage rework to fix these issues are costly and contributes to project delays.

Conclusion

- STPA in this context has been valuable and effective.
- STPA is effective in uncovering potential hazards that other methods might have missed.
- Findings and results from STPA are valuable for system designers to have a deeper understanding of system vulnerabilities and to make necessary modifications to improve design.
- I recommend system designers to include STPA as part of system development process to strengthen the safety of their systems.

Questions and Answer (Q&A)

L3Harris MAPPS Inc.
L3Harris.com
t +1 514 787 5000
f +1 514 788 1530

The content of this presentation is intended solely for the 2024 MIT STAMP Workshop and is for informational purpose only.

For any questions, clarifications, or further discussion regarding the content of this presentation, please feel free to contact Xin Qi at Xin.Qi@can.l3harris.com. I am always open to discussions and to learn more about STPA and relating topic. ☺