L3HARRIS™

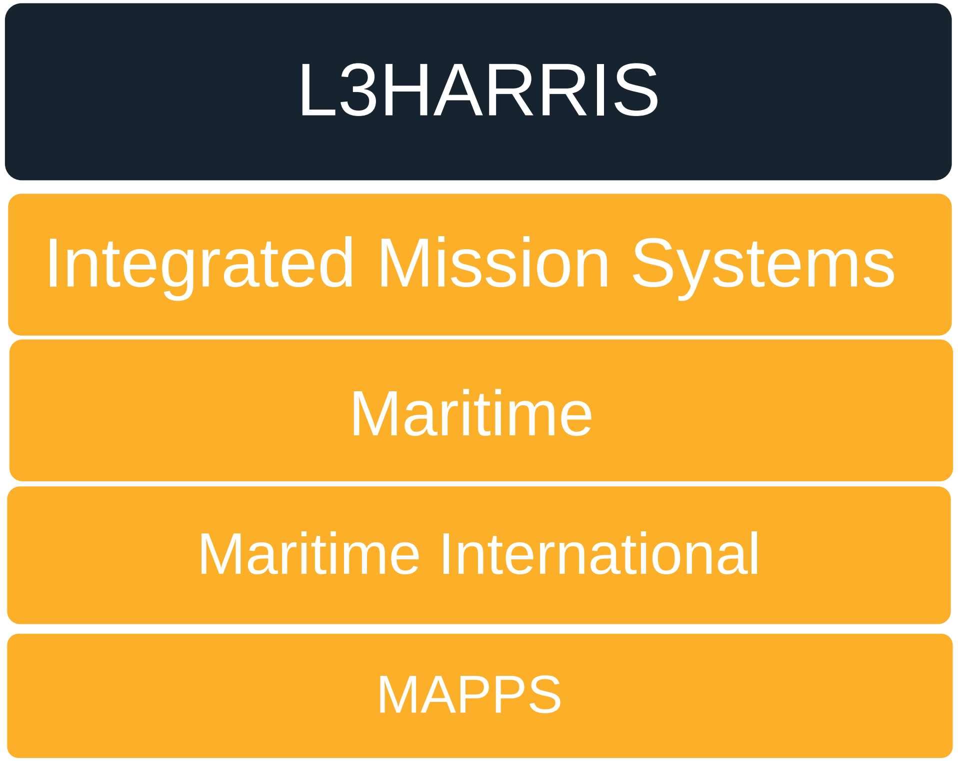
ASSURING MARITIME AUTONOMY THROUGH STPA AND STAMP

20th July 2020

Dr. Giles Howard | Senior Safety Engineer

Background

- I work for L3HARRIS as a Senior Safety Engineer within MAPPS UK.
- My background is in software assurance, both from a safety and security perspective.
- I hold a PhD from the University of Southampton, where my thesis involved developing a unified approach to safety & security analysis (based on STPA) paired with the Event-B formal method.
- I am Project Safety Lead for one of our major IPMS projects at this time.



L3HARRIS

Integrated Mission Systems

Maritime

Maritime International

MAPPS

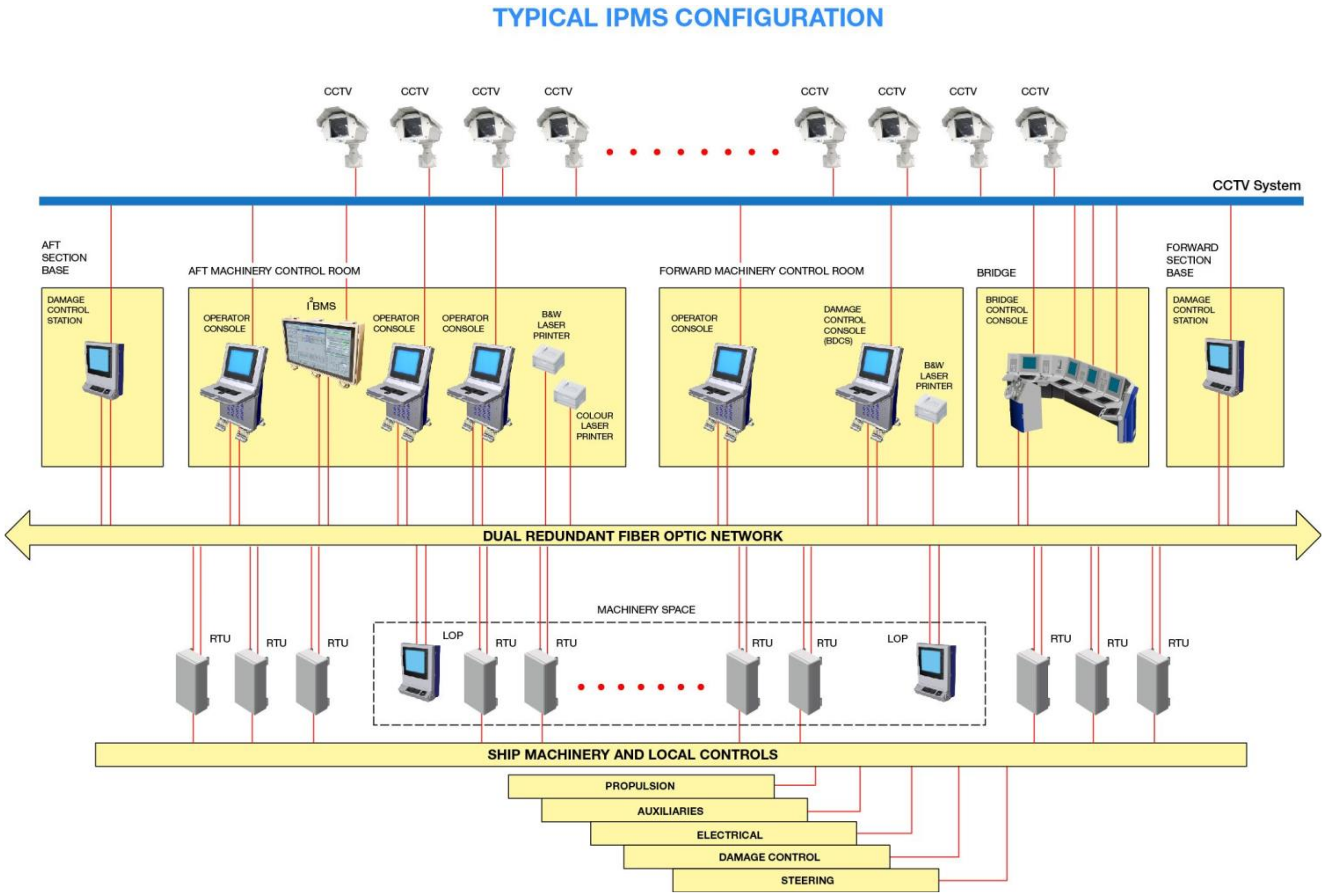
Technical offering and customer base

Our main areas of business are:

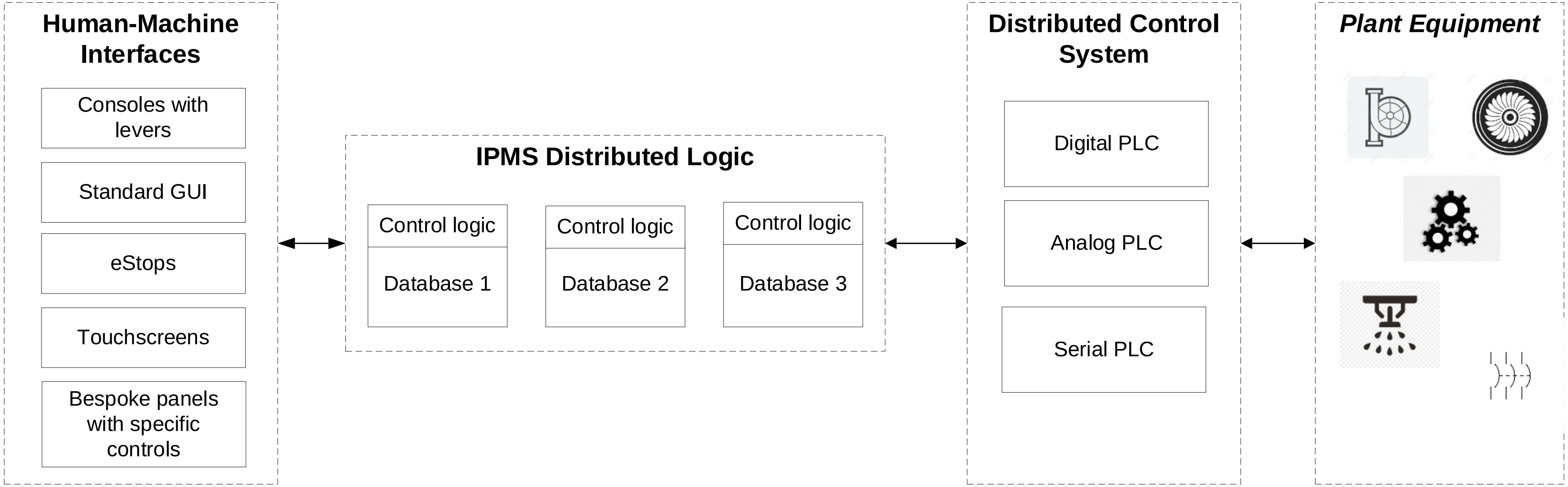
1. Supply of **Integrated Platform Management Systems (IPMS)** to UK naval shipbuilding primes.
2. Supply of **Control and Instrumentation (C&I) solutions** to UK naval shipbuilding primes.
3. **Training and Simulation solutions**, both on-vessel and shore-based, to both UK naval primes and the Ministry of Defence (MoD).

Our IPMS offering is built around a product developed by our parent company (L3 MAPPS Inc, based in Montreal).

L3 MAPPS Ltd do “applications logic” development in-house on top of this product and is bespoke per ship class.



What is an IPMS?



IPMS usually consists of three major functionalities:

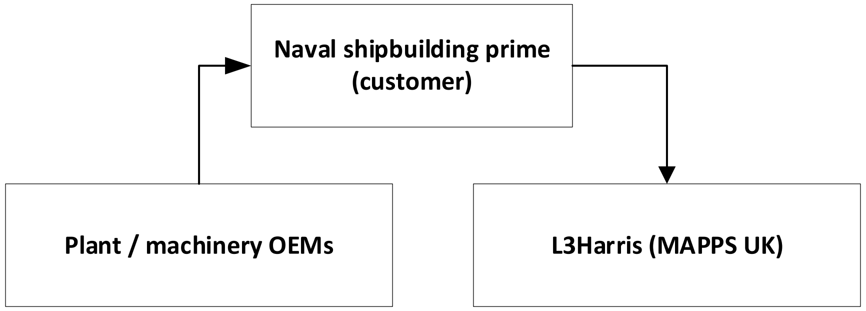
1. A Distributed Control System (DCS) layer, interfacing to a variety of ship machinery / plant equipment via Remote Terminal Units (RTUs).
2. A logic layer, based around a distributed, failure-tolerant database which synchronises and can undertake automatic functionality in response to changes in data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

IPMS and Safety - Challenges

- IPMS is increasingly required to provide safety-related control and monitoring of ship machinery and plant equipment due to control over key ship systems such as propulsion and electrical distribution:
  - This normally comes in terms of a Safety Integrity Level for specified functions (i.e. safety functions) as part of the contract from UK shipbuilder / defence primes.
- We’ve managed this quite effectively to date with the usual combination of qualitative (HAZOP, FMEA, FFA, LOPA) and quantitative (FTA) techniques to ensure our achievement of these safety functions in a safe and justifiable way.
- We’re exploring and trialling the use of STPA for ensuring that we have considered all possible failures associated with safety functions as well as being able to demonstrate that these failures are well controlled through derived safety requirements.
- We also are looking to use STPA to assist us with flowing derived safety requirements to our customer (naval defence prime) as far as operating procedures, training and operational limits.

IPMS and Safety – Organisation interfaces

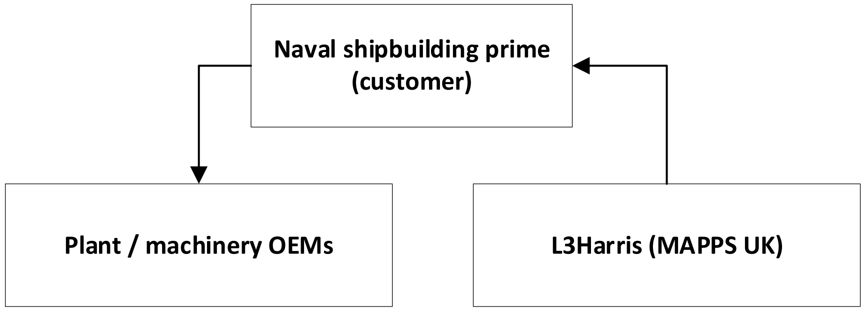


Naval shipbuilding prime (customer)

Plant / machinery OEMs

L3Harris (MAPPS UK)

Information about the plant equipment we control flows from the OEMs via the shipbuilder to ourselves



Naval shipbuilding prime (customer)

Plant / machinery OEMs

L3Harris (MAPPS UK)

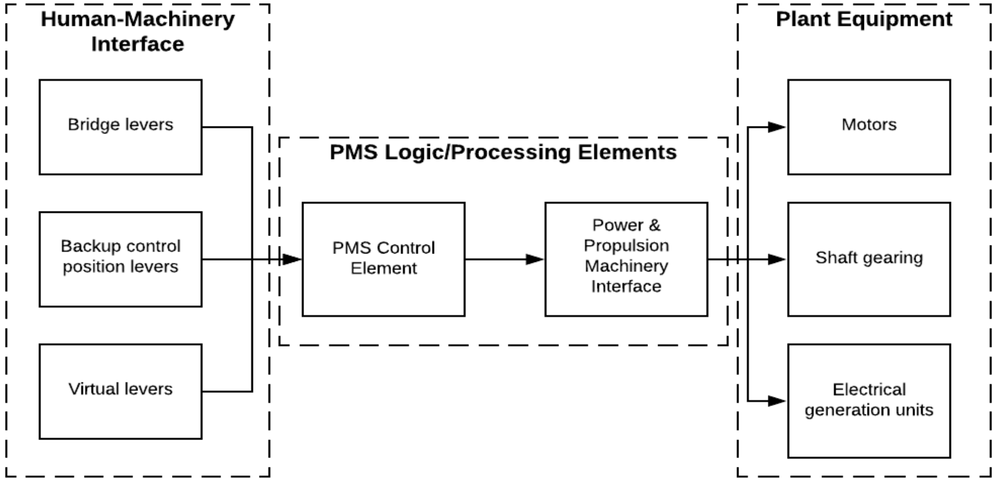
We then derive and feedback derived safety requirements which are either actioned by the shipbuilder or the OEMs.

The benefit of STPA is that it enables us to consider a wide range of operational conditions of a vessel, and explore how IPMS control of those ship systems can become hazardous.

One major example is that IPMS is often involved in controlling & monitoring propulsion, and we can leverage derived requirements to ensure that alternative communication methods exist in the event of a failure or disruption to IPMS.

IPMS and Safety – Experience with STPA to date

- STPA used on a realistic-scale case study (a *Power Control System*) as an internal demonstration of the approach and as a pipe-cleaning exercise for future use of STPA as part of day-to-day operations.
  - This derived a number of useful requirements, including a few that we weren't necessarily expecting, and set the stage for future work.
  - As PMS is highly software-defined, deriving requirements can occur quite effectively and rapidly at any lifecycle stage, as our ability to implement derived safety requirements isn't limited to particular project phases.
  - Use of the technique allows us to demonstrate we've considered operation in a number of degraded / environmentally-challenging circumstances, which is important for stakeholder confidence and our safety argument.
- Opportunities are being sought to deploy it on current projects, however, there are some challenges associated.


Human-Machinery Interface
Bridge levers
Backup control position levers
Virtual levers
PMS Logic/Processing Elements
PMS Control Element
Power & Propulsion Machinery Interface
Plant Equipment
Motors
Shaft gearing
Electrical generation units

Barriers to adoption

- Well-established safety programmes are often built around the existing techniques, which can make it challenging to sell STPA into existing projects.
  - We’re finding that education internally is helping to drive exploration of where we can use STPA most effectively with our safety team within the bounds of our existing programmes, and management are also interested in the technique.
- Using it as a ‘core’ technique requires buy-in from all of our stakeholders, which creates a chicken-and-egg situation as we have multiple safety stakeholders (both MoD and customer).
  - To some extent we’re hoping to use smaller chunks of analysis to demonstrate the concept and its value, and then scale up to bigger, more fundamental analyses.
- The lack of a certification / accreditation regime makes it difficult to assess and demonstrate that personnel are suitably qualified & experienced (SQEP) in the techniques, which can raise flags during audits and formal document reviews.
  - This is an improving situation; several of our team have attended the training offered by Leveson and colleagues, or have worked in an academic context with the technique previously.

L3HARRIS™

Questions and Answer (Q&A) session

Dr Giles Howard
giles.howard@l3harris.com