Maritime Autonomy Framework (MAF) for Autonomous Infrastructure & Fundamental Principles for Safety

A System Engineering Approach

Anita Teo / Bernard Twomey

22nd Nov 2017

Version 1
Contents

• Key Engineering & System Engineering principles for autonomous infrastructure
  • Understanding the “Product” – System of Interest
  • Future products

• How Autonomous is the System?

• Lesson learned - Autonomy Framework from other sectors

• Proposed Maritime Autonomy Framework (MAF)

• The interpretation of level of autonomy

• The attributes of an effective maritime autonomy framework

• Fundamental principles for safety & defence in depth

• Summary & next step
Systems Engineering principles for Autonomous Infrastructure

• Based on Principles derived from the Royal Academy of Engineering:
  • Principle 1: Debate, define, revise and pursue the purpose
  • Principle 2: Think holistically
  • Principle 3: Follow a systematic procedure
  • Principle 4: Be creative
  • Principle 5: Take account of the people
  • Principle 6: Manage the project and the relationships
Understanding the “product”

• The “product” is the system of interest.

• ISO 51288 Section 6.4.2.1 Stakeholders needs and requirements definition process – the stakeholders requirements are defined considering the context of the system of interest with the interoperating system and enabling system.

• System Engineering is about agreeing the scope and context of the “product” from the outset and applying effective system thinking to understand the problems, managing stakeholders communication & collaboration to enable the correct decision making to derive successful systems.

• Effective system engineering framework, techniques & tools can enhance the efficiency of the system engineering process.

• As the complexity of the system increases, the flexibility and the effectiveness of fit-for-purpose system engineering framework, techniques & tools that will enable complexity management & the creation of multiple viewpoints will become increasingly important.
Future Products

- Our System of Interest that define our future products extended beyond the vessel.
- Vessel becomes the sub-system of the “system of interest”.
- The goal of our future products is to transition functionality to higher level of autonomy including but beyond existing onboard operation & ship functions, especially decision support & decision making functionality whether onboard or offboard.
- The majority of classes of functionality of our future products will be assigned to cyber-physical systems and physical systems where the Solutions will be targeted at autonomy Level 3-4 for a broad range of Applications ranging from autonomy Level 1(advisory) to Level 4 (fully autonomous) where human will focus on the sub-tasks level with system taking over the overall responsibility of the main tasks and failsafe tasks.
- System Engineering is required to decompose these highly complex systems (infrastructure level), derive and deliver our future products, identify & manage risks, facilitate collaboration & complex system integration and address the life cycle needs of the products as the scope of the “system of interest” has changed from our current offerings.
## Operational Modes

(Operational Objectives)

### Classification of Functions

<table>
<thead>
<tr>
<th>No Autonomy (L0)</th>
<th>Partial Autonomy (L1)</th>
<th>Conditional Autonomy (L2)</th>
<th>High Autonomy (L3)</th>
<th>Full Autonomy (L4)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitoring</td>
<td>Functions</td>
<td>Functions</td>
<td>Functions</td>
<td>Functions</td>
</tr>
<tr>
<td>Reporting</td>
<td>Functions</td>
<td>Functions</td>
<td>Functions</td>
<td>Functions</td>
</tr>
<tr>
<td>Decision Support</td>
<td>Functions</td>
<td>Functions</td>
<td>Functions</td>
<td>Functions</td>
</tr>
<tr>
<td>Decision Making</td>
<td>Functions</td>
<td>Functions</td>
<td>Functions</td>
<td>Functions</td>
</tr>
<tr>
<td>Decision Execution</td>
<td>Functions</td>
<td>Functions</td>
<td>Functions</td>
<td>Functions</td>
</tr>
</tbody>
</table>

### System of Interests

- **Cyber-Physical Systems (any location)**
- **Physical Systems (any location)**
- **Human (any location)**
How Autonomous is the System?

• Broad product range with a mixture of manual, automated, remote control, semi-autonomous and, autonomous features.

• “How autonomous is the system?”

• This question can be answered with an assessment of how independent the system is in accomplishing its tasks without human interaction and human intervention.

• It is not possible to assess how autonomous the system is without the understanding of automation.

• The key questions to be addressed include:
  • “What tasks (types) do we want to automate?”
  • “What are the level of automation intended for the targeted tasks?”
  • “What is the role of the human in the loop?”
  • “Who/what is in control for the sustained operational tasks?”
  • “Who/what takes over control in fail safe situation?”
  • “What is the autonomous capabilities of the platform?”
Lesson Learned from other Sectors

- What tasks (types) do we want to automate?
- What are the level of automation intended for the targeted tasks?
- What is the role of the human in the loop?
- Who/what is in control for the sustained operational tasks?
- Who/what takes over control in fail safe situation?
- What is the autonomous capabilities of the platform?
<table>
<thead>
<tr>
<th>Level</th>
<th>Name</th>
<th>Definition (Proposed Maritime Autonomy Framework)</th>
<th>Who is in Control?</th>
<th>Who takes over control?</th>
<th>System Capability</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>No Autonomy</td>
<td>All aspects of operational tasks perform by human operator even when enhanced with warning or intervention system. Human operator safely operates the system at all time. (e.g. Select pumps)</td>
<td>Manual</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>1</td>
<td>Partial Autonomy</td>
<td>The targeted operational tasks perform by human operator but can transfer control of specific sub-tasks to the system. The human operator has overall control of the system and safely operates the system at all time. (e.g. start engine sequence)</td>
<td>Automation</td>
<td>Some Operational Tasks</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Conditional Autonomy</td>
<td>The targeted operational tasks perform by automated system without human interaction and human operator perform remaining tasks. Human operator is responsible for its safe operation.</td>
<td>Semi-Autonomous</td>
<td>Majority of Operational Tasks</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>High Autonomy</td>
<td>The targeted operational tasks perform by automated system without human interaction and human operator perform remaining tasks. System is responsible for its safe operation. (e.g. PMS, DP)</td>
<td>Semi-Autonomous</td>
<td>Majority of Operational Tasks</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Full Autonomy</td>
<td>All operational tasks perform by an automated system under all defined conditions.</td>
<td>Full Autonomous</td>
<td>All Operational Tasks</td>
<td></td>
</tr>
</tbody>
</table>
Vessel goals

Operational Modes
(Operational Objectives)

Classification of Functions | No Autonomy (L0) | Partial Autonomy (L1) | Conditional Autonomy (L2) | High Autonomy (L3) | Full Autonomy (L4)
--- | --- | --- | --- | --- | ---
Monitoring | Functions |  |  |  |  
Reporting |  | Functions |  |  |  
Decision Support | Functions | Functions | Functions |  |  
Decision Making | Functions |  |  |  |  
Decision Execution |  |  |  | Functions |  

Systems In ROC

© 2017 Rolls-Royce plc
The Interpretation of the Level of Autonomy

• A System engineering approach to use case generation for risk assessment:
  • The context include the infrastructure – vessels, ports and remote operational centres
  • Identify the vessel / fleet objectives or goals
  • Identify the vessel operational modes
  • Determine functions for all targeted vessel operational modes
  • Classify functions type
  • Assign level of autonomy to functions
  • Assign functions to be performed to actors (an actor can be human or system)
  • Determine location of the actors (location can be remote or onboard)

• There is a need to segregate the interpretation of level of autonomy according to:
  • Specific function(s) (e.g. different functions may have different level of autonomy, functions may change their level of autonomy over time)
  • Specific solution(s) in question (e.g. how functions with different level of autonomy integrated to form a solution (e.g. sub-system) with a defined level of autonomy)
  • The specific vehicle platform in addressing its overall strategic objective(s) or goal(s) (e.g. how different solutions with varying level of autonomy integrated to deliver the vessel autonomous capability to accomplish its overall mission).

• Having an appropriate taxonomy to define the level of autonomy for maritime operation enable safety critical function and safety critical system to be identified.
The Attributes of An Effective Maritime Autonomy Framework

An effective MAF should be:

• **Simple** enough to be understood and remembered.
• **Practical** enough to be used in the design process & implementation.
• **Flexible** enough to cover a wide range of operational scenario and solutions at all levels (function, sub-system, system, platform level) with mixtures of autonomous features. The framework can be further extended to show technology readiness.
• **Robust** enough to provide consistency, traceability, evidence and argument to support strategic, operational, safety objectives.
• **Transparent** enough to be understood by the regulators how the safety argument has been achieved. Support customers map the value creation to the level of autonomy.
Domain-Neutral Terminology

- **Strategic Objective**
- **Operational Objective**
- **Task**
- **Cyber-Physical System**
- **Name**
- **Operational Mode**
- **Flow**
- **Data**
- **Material**
- **Input**
- **Output**
- **System View**
- **Operational View**
- **Strategic View**

**System View**
- **Human Role**
- **Business-Level Objective - Services that can be sold**
- **Platform-Level Objectives - things the vessel can support**
- **Manual Operations**

**System-Level Functions**
- (a) Manual (aka 'Task')
- (b) Remote Controlled
- (c) Autonomous

A part of a cyber-physical system to support remote control or autonomous
Domain-Specific Terminology

Example Task: Leaving...

• Berth
• Dock
• Anchor
• Mooring

• Each task description is different
• Post-condition of task is similar (if not the same)

Agreement on domain-specific terminology is essential for integration and interoperability
# Fundamental Principles for Safety

<table>
<thead>
<tr>
<th>Fundamental Principles</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FP1 Responsibility for Safety</td>
<td>The prime responsibility for safety must rest with the person or organisation responsible for the activities that give rise to the risk.</td>
</tr>
<tr>
<td>FP2 Leadership and Management for Safety</td>
<td>Effective leadership and management for safety must be established and sustained throughout the systems life cycle.</td>
</tr>
<tr>
<td>FP3 Safety Assessment</td>
<td>The ‘dutyholder’ must demonstrate effective understanding of the potential hazards and their control for the autonomous infrastructure through a comprehensive and systematic process of safety assurance.</td>
</tr>
<tr>
<td>FP4 Prevention of Accidents</td>
<td>All reasonable practicable steps must be taken to prevent and mitigate accidents.</td>
</tr>
<tr>
<td>FP5 Emergency Preparedness and Response</td>
<td>Arrangements must be made for emergency preparedness and response in the event of a total failure of the ships or its infrastructure.</td>
</tr>
</tbody>
</table>

The concept of defence in depth should be applied so that:

a) deviations from normal operation and failures of the ship, systems and autonomous infrastructure are prevented;

b) any deviations from normal operation are allowed for by design that enable timely detection and action that prevents escalation;

c) inherent safety features, fail safe design and safety measures are provided to protect against fault conditions progressing into accidents; and

d) additional measures are provided to mitigate the consequences of accidents, especially severe accidents.
Objective of each level of protection;

*Objective Level 1:* Prevention of abnormal operation and failures by design

*Defence/Barrier:*

Conservative design, high quality in construction, maintenance and operation in accordance with appropriate safety criteria, engineering practices and defined quality levels

*The underpinning safety aim for any autonomous infrastructure should be an inherently safe design consistent with the key operational purposes of the infrastructure.*

*An inherently safe design is one that avoids key hazards rather than controlling them, when an inherently safe design is not achievable then the design should be fault tolerant.*
Objective of each level of protection

• **Objective** Level 2: Prevention and control of abnormal operation and detection of failures.

• **Defence/Barrier:**
  Control, limiting and protection systems, other surveillance features and operating procedures to prevent or minimise damage from failures
Objective of each level of protection;

• **Objective** Level 3 Control of faults within the design basis to protect against escalation to an accident

• **Defence/Barrier:**
  Engineered safety features, multiple barriers and accident or fault control procedures
Objective of each level of protection;

- **Objective** Level 4 Control of severe ship or infrastructure conditions, in which the design basis may be exceeded, including protecting against further fault escalation and mitigation of the consequences of severe accidents.

- **Defence/Barrier** Additional measures and procedures to protect against or mitigate fault progression and for accident management.

- Examples; Fire, flooding or grounding of the vessel. Loss of control of the Remote Operating Centre – Fire within the ROC or complete loss of power.
Objective of each level of protection:

- **Objective** Level 5 Mitigation of accident consequences through emergency responses.

- **Defence/Barrier** Emergency control and on- and off-site emergency response (e.g. Salvage, fire-fighting tugs, transfer of control from the ROC, Security procedures in place, etc).

- Examples: Vessel out of operation (not under command) and drifting towards a main shipping lane. Terrorist attack, earthquake, flooding event
Summary & Next Step

We have identified:

- framework for categorising autonomy
- framework for applying system engineering principles to autonomy
- fundamental principles for safety & defence-in-depth

Next step:

- Apply the framework and principles in forthcoming projects
- Provide more clarification how to achieve fundamental principles
- Provide guidance on the body of evidence to be submitted to the regulators
- Identify all relevant stakeholders who would have an interest in the autonomous infrastructure such as port state control, interaction between land-based and maritime legal framework, marine / land-based insurers, flag states and classification societies, other government organisations (e.g. DFT, CPNI, NCSC, ONR, etc)