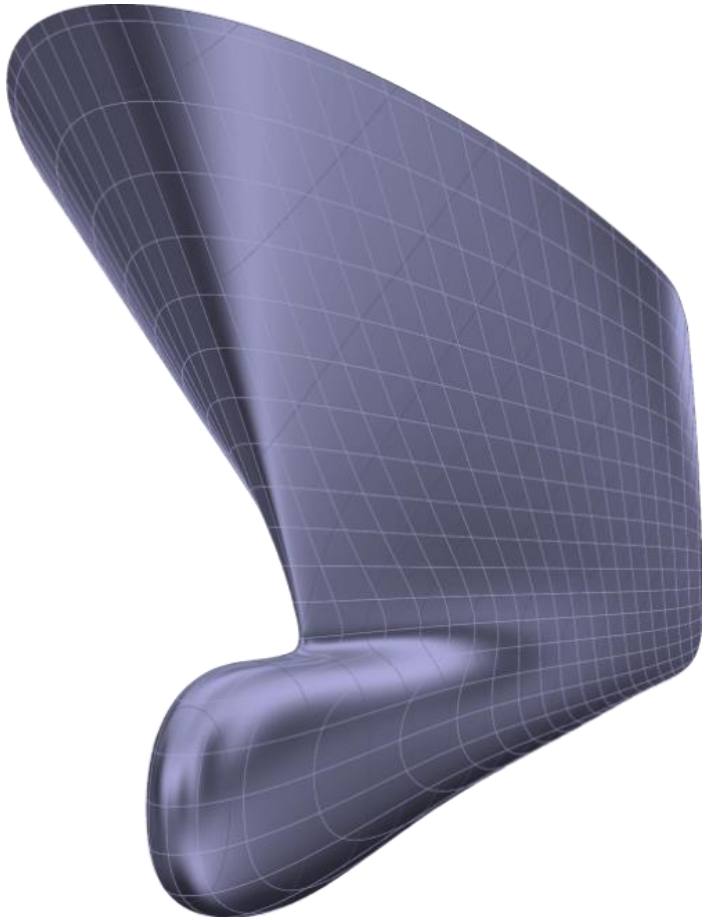
SOFTWARE FOR CYBER SECURITY AND BUSINESS RULES COMPLIANCE IN THE MARINE DOMAIN

Dimitri Lyras,
Director of Lyras Shipping,
Founder of Ulysses Systems

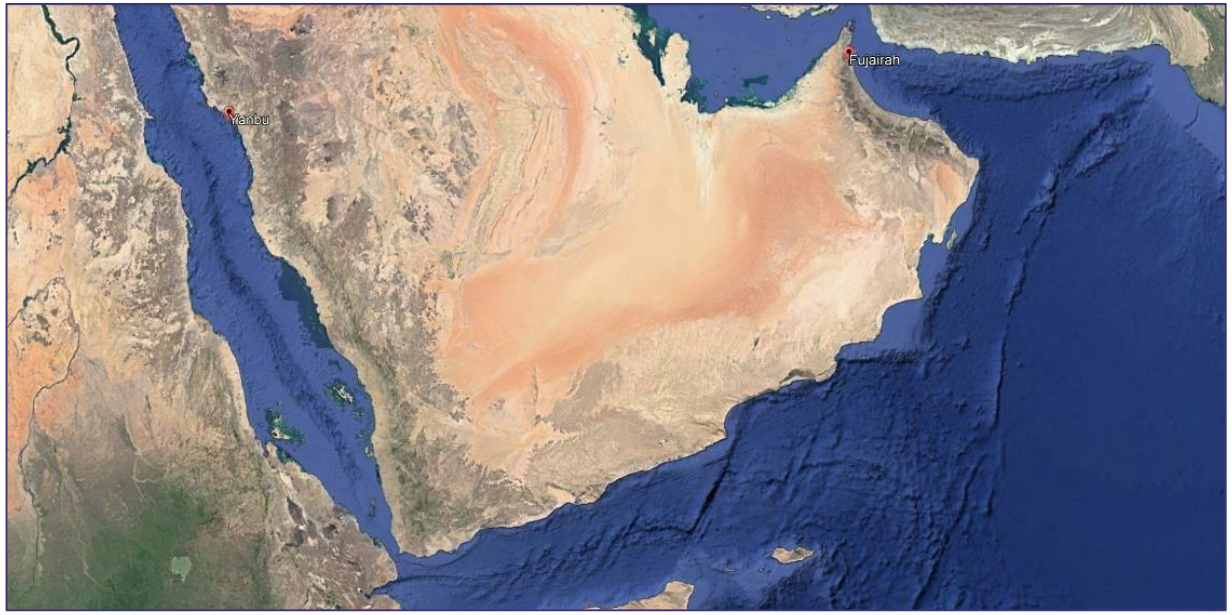
Discussion Points

1. Use case scenario for crew sign on
2. Cyber Security Verification Approach using contemporaneous information
3. Abstracted layers for run time monitoring of the cyber security legislation and business compliance rules
4. Executable modeling framework For denoting system requirements



Use case scenario for crew sign on

Risk of unauthorized onboarding of personnel and the knock on effect on third parties relying on accurate onboarding information



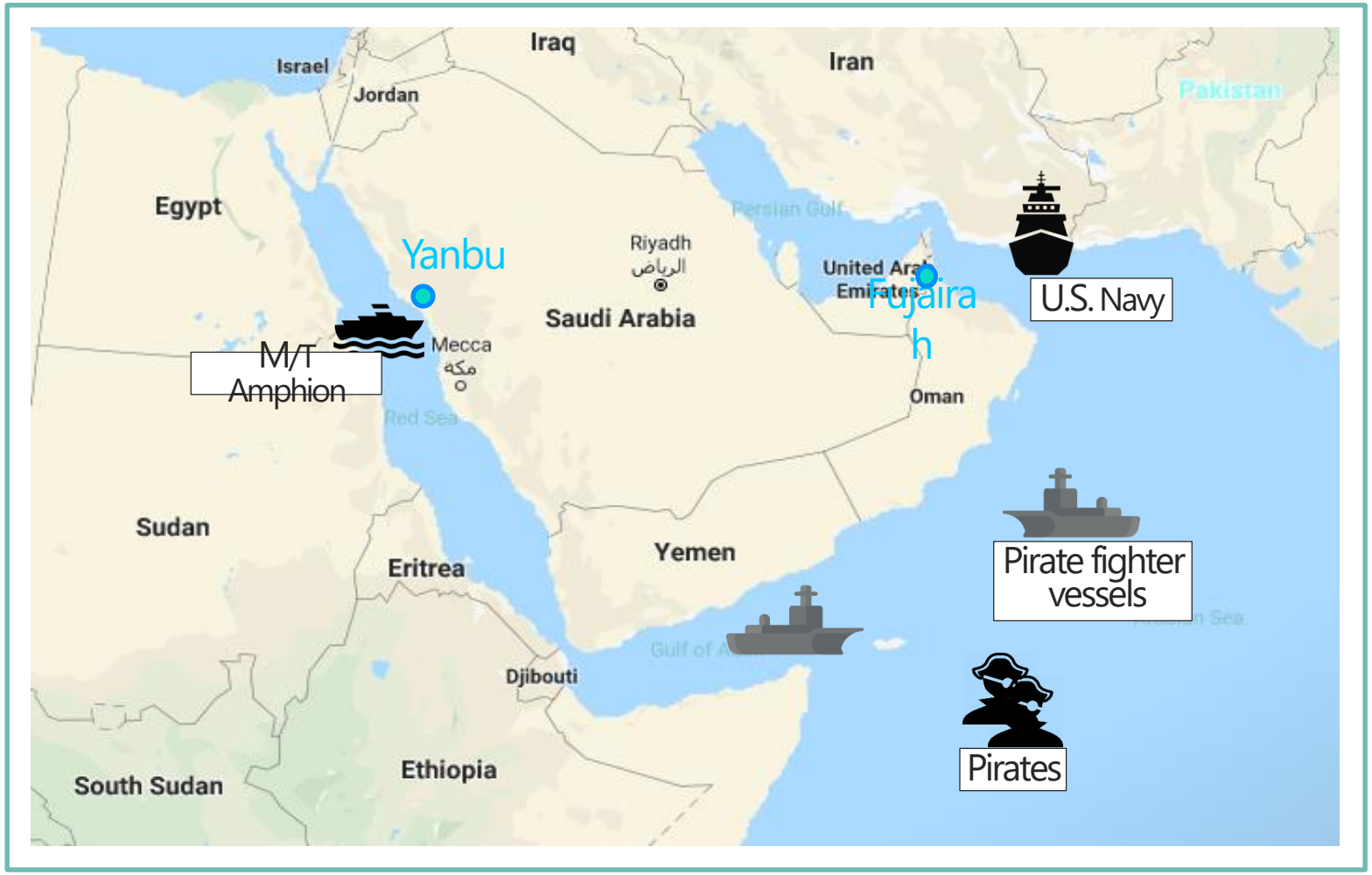
Example

The specific example chosen points to a model superimposed over a personnel on-boarding sign-on application in the maritime domain, incorporating new compliance requirements with respect to minimizing access to employee personal data (e.g. medical data) while maintaining compliance for record privacy when a mariner has to be cleared to operate critical equipment, or when the on-boarding process requires other domain specific business and certification requirements

Ship trade route from Yandu to Fujairah

Signing-on act

HR Officer, K.Louvari, is about to sign-on (onboarding) Captain N. Mangouras as a temporary replacement in the Master's rank on the M/T Amphion, trading in the Red Sea, mainly between Yanbu and Fujairah.
We will be discussing the consequences if a hacker were to perform an illegal sign-on (onboarding)



Piracy Risk

Provide correct crew information to authorities

- Indian ocean anti pirate force
- U.S. Navy patrolling Hormuz Straits
- Port Authorities
- Immigration

M/T Amphion trade route is in proximity of three piracy zones: Gulf of Aden, Horn of Africa and the Hormuz Straits. Consequently the onboarding process has elements of risk with respect to information provided to anti-piracy task forces and military forces as well as conventional port liaison processes, including immigration.

Authorized sign-on Vs Hacked sign-on

1. On a set date before Capt. Mangouras onboards the M/TAmphion, the HR system automatically sends manifests to authorities without which the ship cannot enter Port

1. On a set date the System sends incorrect crew manifests to authorities. This would mean background checks by various regulatory and corporate forces would be run on the wrong Master.

Cyber Threat assessment includes hacking but not internal infiltration

The company employing Katerina Louvari excludes the eventuality of insider illicit information handling

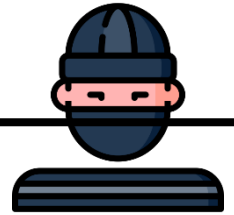
In this example there is no concern that Katerina Louvari would sign on Captain Manguras ahead of time, or in any other untrue way because the company does not deem there to be sufficient incentive for her to do so.

Katerina has in-house information a hacker would not have. Not even a targeted attack expert hacker

A hacker who may have replicated K.L's authorization credentials would not know background information without which crew cannot enter onboard

Corroborating information, Changeover risk assessment form

- The authorized person Katerina Louvari has to fill a form, a changeover risk assessment, instructing the onboarding participants of the risks of change in command, by hand with the latest instructions and information from various systems which the hacker would not have access to while also not having the knowledge to select the right information.



This corroborating information has different access authorization that is not in the HR system and is a change of command risk assessment form

The form also contains instructions to Captain Mangouras related to the ships current situation which the hacker has no way of knowing.

Corroborating information

The system and the recipients of the changeover risk form would notice an unauthorized person filling the changeover risk assessment from discrepancies in the data recorded in various systems and the data entries on the changeover risk management form, such as:

- recent procurement events
- current ship operation events
- commercial risks that the system could corroborate between the risk assessment form written by hand by the authorized person (Katerina Louvari), and other data sources thereby exposing any lack of contemporaneous knowledge by the hacker
- The changeover risk assessment form will contain recent high level commercial and operational entries, which the two masters would notice
- Errors or omissions show that the person filling the form is, or is not, aware of the current running situation on-board of which both ships Masters are aware

If not, the onboarding is not the work of an authorized person

Generalizing this example

The effectiveness of contemporaneous information in making the necessary abstractions in order to deduce legitimate from illegitimate acts in our example, is similar to the abstractions banks use to validate the proper use of a credit card.
They ask for information the hacker does not have.
Sometimes it's personal information, sometimes it's about the last transaction, as in the case of a card related enquiry after a card has been blocked

Corroborating info in payment transfers

More contemporaneous information will be needed in marine applications managing processes such as crew payments, for example,
where the need is to guard against illicit diversions of funds and
overcome impersonation of authorized stakeholders

The corroborating information for bank transfers, in this situation, provides evidence that a crewmember has participated in employment activities and
therefore is entitled to certain financial transfers,
information that needs to be validated alongside member's rank,
years of experience and other considerations

An HR System, therefore, needs to be one system that manages onboarding, crew information, financial calculations and transactions, i.e. a system with high availability requirements

Access to medical records compliance but no access to medical records themselves

It is company policy, following one of the statutory rules of Information Privacy Law,
to conceal medical records from all users and have only the system able to make compliance comparisons

During sign-on the new crew member's medical record is checked by the system.
The system could block a crew member like Captain Mangouras from boarding due to identifying a medical non- compliance

HR Manager
CAPT. B. BINIKOS

Overriding medical criteria

Only HR manager Captain Binicos is authorized to check the compliance criteria of the system to ascertain whether the enlistment and voyages of the ship in this case, could allow for his medical condition.
In this example the company does not consider the rules to be of interest to hackers nor the overriding of medical compliance rules.

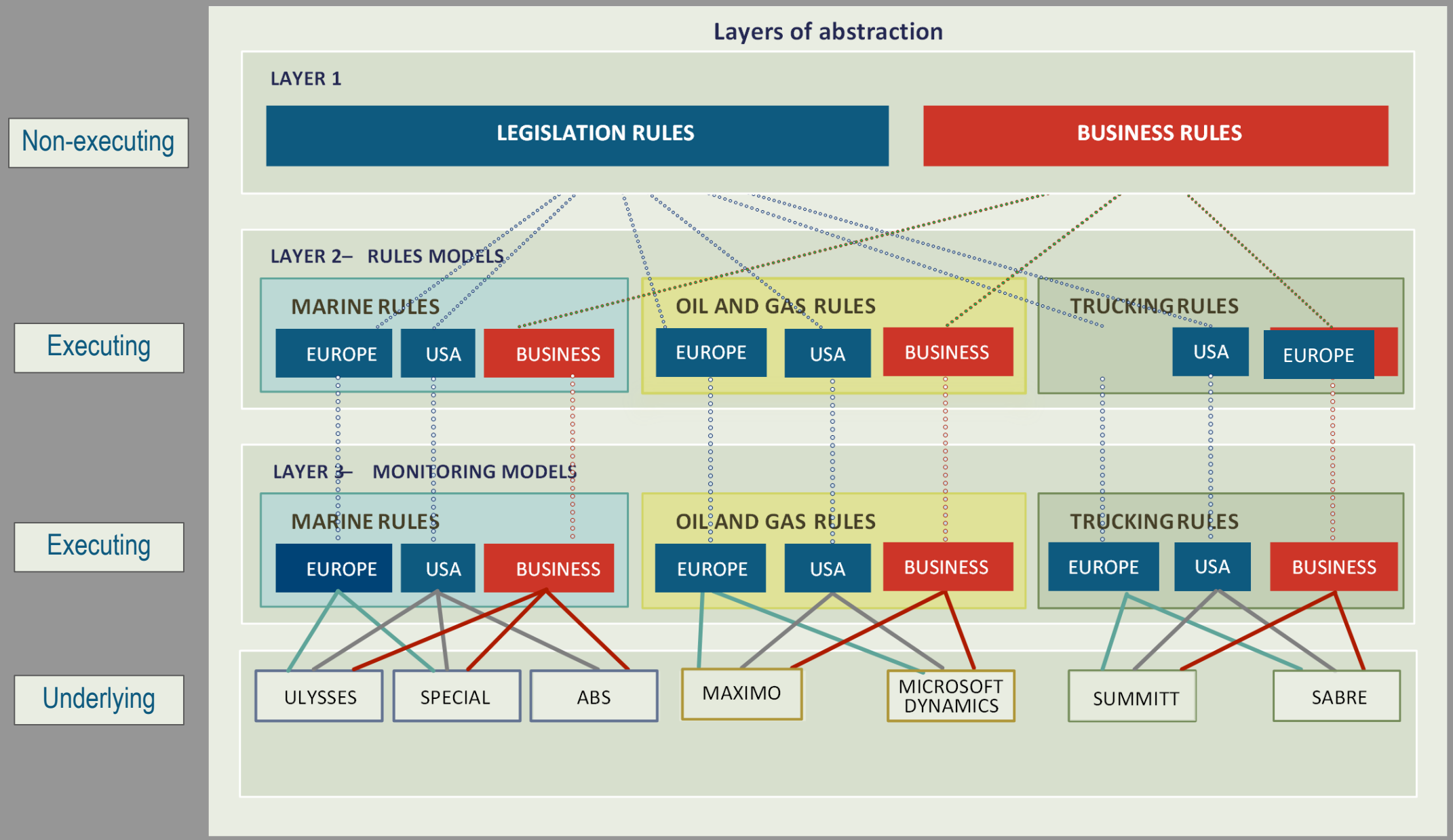
Complementary security measures

Security for high availability requirements can be assisted by various means. Conventional virus and disruptive agent detection, separation of systems according to availability criteria, protection of high availability functionality through the use of tokenized code for operating the protected functionality, unconventional programming and unconventional storage and more.

Cyber Security Certification

By applying layers of descending abstraction
it is possible to create a system that encompasses
executing models of general rules dictated by business or regulators
more specific executing layers that implement of these rules at the enterprise level
enriching existing and underlying domain application

The example that follows is that of implementing
Information Privacy Law in marine enterprises.

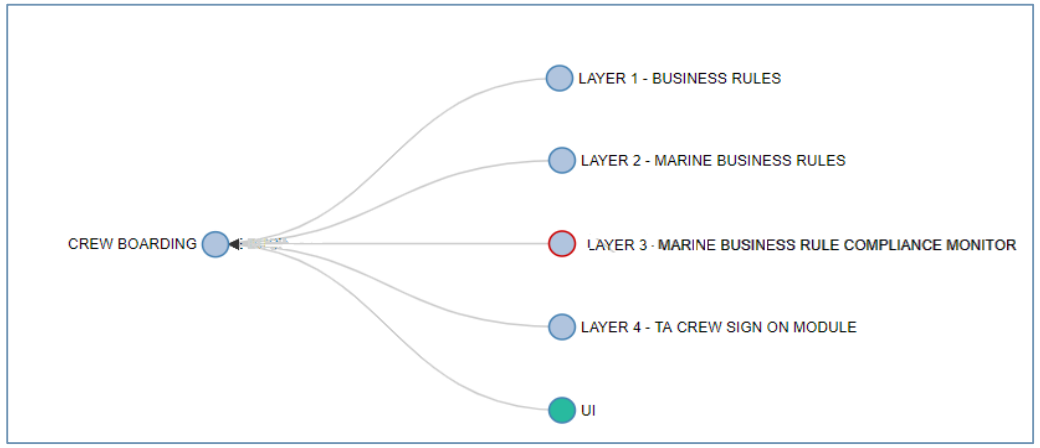

Layers of abstraction
Non-executing
Executing
Executing
Underlying
LAYER 1
LEGISLATION RULES
BUSINESS RULES
LAYER 2– RULES MODELS
MARINE RULES
EUROPE
USA
BUSINESS
OIL AND GAS RULES
EUROPE
USA
BUSINESS
TRUCKING RULES
USA
EUROPE
LAYER 3– MONITORING MODELS
MARINE RULES
EUROPE
USA
BUSINESS
OIL AND GAS RULES
EUROPE
USA
BUSINESS
TRUCKING RULES
EUROPE
USA
BUSINESS
ULYSSES
SPECIAL
ABS
MAXIMO
MICROSOFT DYNAMICS
SUMMITT
SABRE

Modelling the statutory and business rules

LAYER 1
Rules set by legislators or business rule designers written in text

Thematic cross industry rule templates
for example,

- Legislative Themes:
  - Confidentiality of medical records
    No access to medical records, or copying of medical records; only medical experts look at medical records and only under ***medical circumstances*** the medical expert to connect the person with his medical records
  - Personnel assignment to Jobs with security sensitivity



Jobs with security sensitivity to be performed by authorized people and
security measures to be in place to block illicit interference

- Business Theme
  - Procurement item identification
    must follow functional
    as well as manufacturer identifications and
    each to be clearly differentiated

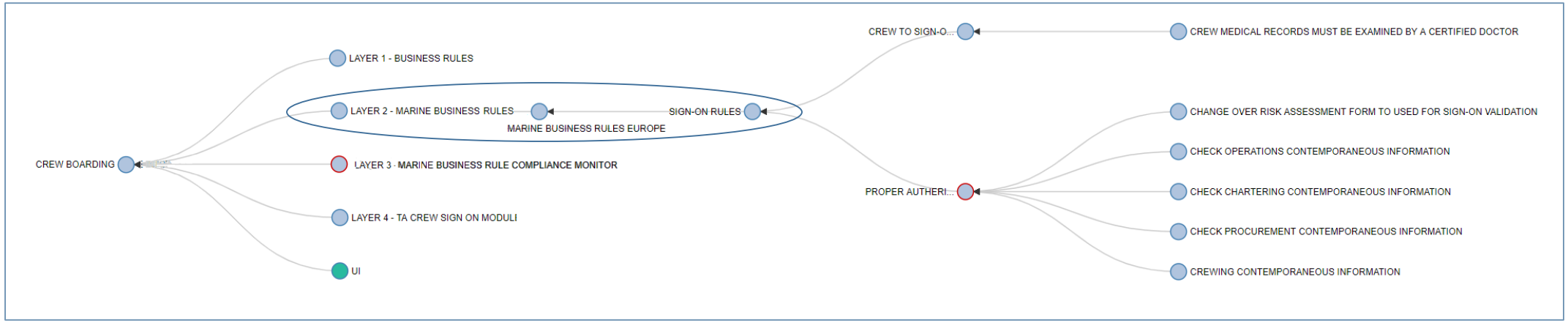
Executing cross-industry layer

LAYER 2
Cross industry abstraction preparing for same industry abstraction

Cross industry thematic abstractions are modelled and enriched with predictive patterns and generalized context able to propagate and if necessary return converted values to underlying applications

This is appropriate because:

Groups of industries share thematic abstractions *for example*:
Shipping and Offshore will have similar medical and similar on boarding rule abstractions. They will also both share very wide abstraction of payment security that involves other industries



Executing industry layer

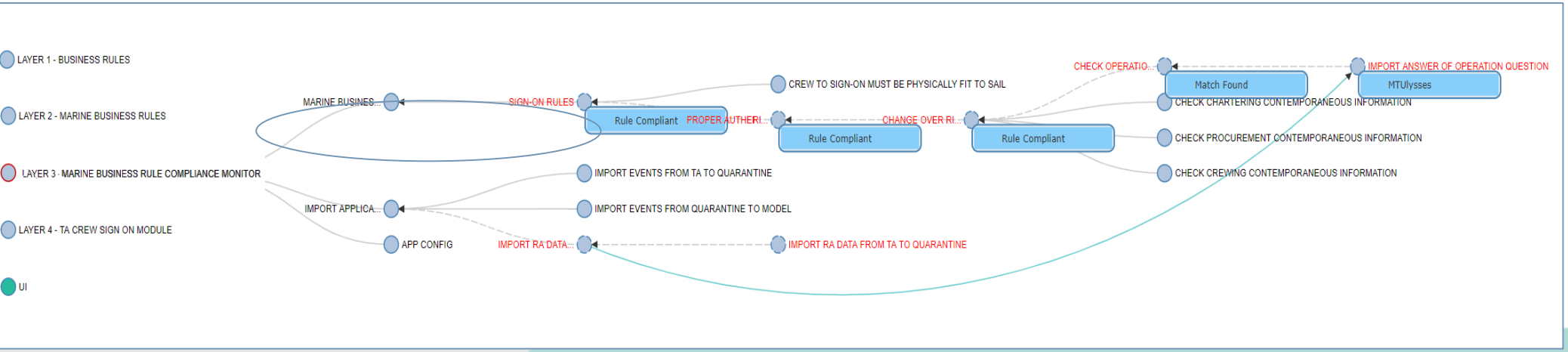
LAYER 3

- Off the shelf Industry Abstractions ready for use across same industry domain

  These constitute a model combining thematic abstractions modelled and suitable to the industry

LAYER 3

- Industry abstractions adapted to client enterprises for monitoring domain applications
  for example:
  Procurement, Crewing, Critical Maintenance Work



Summary

The layered design approach partly presented today shows
an executable modeling framework applied over existing domain applications and business rules,
a framework for denoting system requirements
and applied to personnel enlistment in the marine domain

THANK YOU!