This article explores how the ports of the future can become smart, safe and secure, through the use of innovative technologies. One of the marvels of the maritime industry is the corporate ability to remain a pioneer during major economic, commercial and geopolitical changes throughout different market cycles. The modern maritime era is most intriguing as dramatic geopolitical and financial shifts force ports to change, but also innovative technologies enable this transition.

The world’s major seaports and ship-owning companies are “jumping on the bandwagon” of technology, in search of synergistic processes that are smarter, faster, and generally more proactive, effective and efficient. Smart technologies serve as the modern glue that unites supply chain partners through Blockchain platforms, the Internet of Things (IoT), Big Data, Artificial Intelligence, Unmanned Vehicles, and much more. And while port authorities invest in smart technologies to grow sustainably through increased efficiency and effectiveness, the same tools can be used to ensure physical and cyber Security.

SMART PORTS AND GLOBAL SUPPLY CHAINS
Ports are significant nodal points of complex global supply chains. As such, port expansion plans should not focus entirely on the port’s growth capabilities, should rather consider the positioning, strength and weaknesses of the entire supply chain (Burns, 2014a). This means three things:

• First, smart ports need to be well-integrated with their supply chain partners and markets, and ensure optimum supply chain and hinterland connectivity. As port authorities make strategic investment decisions aiming to increase capacity, they must also consider if the existing hinterland infrastructure can mitigate the increased traffic. Hence, port growth can only be successful if the supply chain infrastructural needs are met at a regional level.

• Second, for smart ports to be secure and sustainable, their executives must have a clear understanding of the strengths and weaknesses of their global partners. After all, a port is as weak as its weakest link. Ideally, each port, and each supply chain partner should design a risk management platform that includes the entire supply chain, not only its regional partners.

• Third, technology investment decisions should provide solutions for the entire supply chain in terms of integration and real-time visibility.

SMART PORTS & SAFETY AND SECURITY RISKS
While the terms safety and security are often used interchangeably, there is a distinction regarding the motive i.e. the intention of the damage: Maritime safety risks pertain to unintentional threats such as extreme weather, technological failures, infrastructure issues, human error, and so on. Maritime security risks
relate to intentional attacks driven by ideological fanaticism (terrorism), financial or competition motives, among others. (Burns, 2015)

Risk is an interesting term, as it includes both opportunities and challenges, while involving safety, security and environmental hazards, among others (Burns, 2018). Port and maritime industry executives often take pride in serving a high-risk, high-tech and high profit industry. And while it is up to the company to decide how much risk is “acceptable” and how much is “too much”, decision makers must find the perfect balance between fear and greed (Burns, 2014b).

Fear on one hand, leads to risk aversion, which is a corporate strategy for the less ambitious port authorities who decide to take less risks and lower returns. Greed on the other hand, drives more ambitious entities far beyond their comfort zone, while taking reckless risks in the name of growth. In the middle of these extremities lies the truly “Smart” port that invests in advanced technologies in order to manage its risks.

**JUMPING ON THE BANDWAGON**

Smart Ports involve technology-based strategies used by port authorities in order to surpass, or literally “outsail” their competitors. Investing in advanced technologies does not only help ports grow in terms of capacity, efficiency and effectiveness, but also help identify port-related risks, and protect accordingly. Here are some examples:

A blockchain is an unhackable, decentralized, digitalized ledger of financial and commercial transactions, encoded to create fast, cheap and efficient blocks of data. Maritime supply chain partners or nodal points establish blockchain platforms where each transaction represents an independent block, stored in chronological order. What makes this system secure, fast and cheap is its unhackable and decentralized structure: The system receives unencrypted data and transforms them into cyphers, i.e. encrypted mathematical algorithms.

As the system is decentralized, it does not need intermediary entities to process, monitor or control the data. Blockchain has been successfully applied in shipping, through the first virtual documentation such as Bills of Lading, financial transaction in cryptocurrencies, marine insurance, real-time productivity monitoring of ships, cargoes, container boxes, pipelines, cranes and other cargo-handling-technologies. In addition, real-time geographical and weather tracking capabilities enhance security and safety. (Burns 2018 and Burns 2019).

The Internet of Things (IoT) is a massive network connecting “things” including people, computers and technologies. A maritime supply chain is the perfect example of an IoT network, which not only monitors individual performance, but takes action based on performance, such as energy efficiency, processing times. The system monitors the performance of inter-related activities, hence can associate the discharging operations of ship A, the loading operations of ship B, with empty space in container yards or port-owned warehouses. The IoT capabilities encompass the entire supply chain from raw materials, to processed commodities and market distribution. For example, the oil & gas supply chain commences with the oil production in offshore platforms, continues when crude oil moves through ships to the refineries, to the stage where the refined products are distributed in the global markets. Ports and ships play a pivotal role in this secure procedure. In addition, access to real-time information enables stakeholders to be proactive and contingent in case of delays or incidents.

Big Data enables the maritime industry to gather, analyze and draw useful conclusions from large data sets. Imagine ports and the maritime industry as a key nodal point in a vast global supply chain. Big data enables key players and partnering companies to see the big picture encompassing all the supply chain stages, and all the geographical locations.

Artificial Intelligence or AI-enabled platforms utilize Big Data, yet are even more advanced: First, they identify patterns and trends in data which humans may find total unrelated or irrelevant. Second, they can foresee risks and problems, and find proactive solutions. This platform greatly supports maritime and port security measures, as AI identifies systemic vulnerabilities and external threats, and
subsequently proposes a contingency plan before the problem even occurs. The recommendations are always aligned with the technologies available at port and at sea, including sensors, radar systems etc. Piracy threats, terrorist attacks, collision avoidance are some of the many preventable types of threats, due to A.I.

CONCLUSIONS
This is an exciting era for seaports, with technological innovations increasingly redefining the notion of “business as usual”. Ports of the future are investing in technologies not only for commercial growth purposes, but also to minimize and mitigate risks related to security, safety etc. A pioneer is defined as an entity willing to explore new territory and implement new growth techniques. Port authorities and maritime companies are asked to invest in the right technological platforms, that will help them increase their market share and grow, while mitigating security and other threats.

ABOUT THE AUTHOR
Prof. Maria G. Burns serves as the Director for the Logistics and Transportation Policy Program, University of Houston, as SCLT Faculty and Researcher for the U.S. Department of Homeland Security. She is a National Academies scholar, serving as Chair in the Supply Chain Security Subcommittee, in Washington DC. An acclaimed author of transportation security books used as textbooks in Universities worldwide: “Port Management & Operations” (2014); Logistics & Transportation Security (2015); “Managing Energy Security & Critical Infrastructure (2019), and “Maritime Security” (in print, 2020). She is an Honorary Member of the US Coast Guard Auxiliary. In 2016 she received the “Excellence in Emergency Management Award” by the Emergency Management Association of Texas (EMAT). She has developed a series of Training Manuals approved by the US Coast Guard NMC. She is a Certified Auditor for Security (ISPS), Safety (ISM), Quality (ISO9001) and the Environment (ISO14001).

ABOUT THE ORGANIZATION
Established in 1927, the University of Houston empowers students in their pursuit of learning, discovery, leadership and engagement. Located in a sprawling metropolis, our premier campus provides students with cutting edge programs including undergraduate, graduate, doctoral, distance and continuing education. Ranked among the best colleges in America, UH is home to award-winning faculty, innovative research centers, has one of the most diverse student populations in the nation, and alumni who have become international leaders.

ENQUIRIES
Maria G. Burns
Email: mburns2@uh.edu
Tel: (+1) 832-764-3622

REFERENCES