EXECUTIVE SUMMARY

The priority for the member companies forming the Industrial Internet Consortium is to build together a safe, reliable and secure Industrial Internet.

Networks originally designed to be isolated are now exposed to continuous attacks of ever-increasing sophistication. The continuing explosion of connected devices provides opportunities for unprecedented growth and performance gains in industrial systems, as well as unprecedented increases in risks to plant personnel, to society and the environment at large, as well as to the businesses which operate industrial processes.

There is also the risk of being 'attacked' from unexpected sources from inside and outside the firewall, whether intended or unintentional. With the proliferation of connected devices, there is a need to protect against error, mischance and malicious intent.

The Industrial Internet Consortium is taking seriously the security risk of this new industrial revolution and has created a Security Working Group with the intention of developing a common security framework and a rigorous methodology to assess security in Industrial Internet Systems (IIS).

The common security framework attempts to describe the consequences in security terms of merging different security fields (industrial, information, controls, analytics, cloud), which in the past were guided by different protection axioms. While doing so, it also provides guidance on how to select improved security objectives appropriate to different classes of industrial activity, how to achieve those objectives, and how to leverage novel technologies to overcome different classes of adversaries, each of which continues to innovate cyber-sabotage and cyber-espionage attack technologies focused on these nascent architectures. The review process and suggested practices outlined in this document will help to improve the protection of a wide range of industry verticals implementing industrial internet systems, from smart cities to critical infrastructures.

This document will also be a live reference for the different industrial evaluation testbeds hosted by the Industrial Internet Consortium, which at the time of writing already spans verticals such as smart grid, transportation, industrial maintenance and others. The security evaluation of these testbeds will provide continuous feedback which will then be used to update the information contained in the security framework. The engagement with testbeds will drive technical references to support these frameworks.

The security framework evolves naturally from, and builds upon, the already published Industrial Internet Reference Architecture (IIRA). This will ensure that security is not just bolted on to the architecture, but rather is a fundamental part of it. This document will elaborate on the contributions already made to the IIRA and take that work into more security-specific territory.

To implement a successful security design for an IIS, several system characteristics must be taken into account. These end-to-end characteristics include scalability, usability, maintainability, portability and composability. The criticality of some of them, such as safety, reliability, and resilience is well understood in respect to industrial systems, such as the electric grid, but the emergence of new threats has driven security to a new level of prominence in the Industrial Internet, and the spotlight is shining on privacy as well. The security framework includes information on how to combine them to achieve the desired level of security based on drivers such as regulatory compliance, business process, and industry norms. The five key characteristics are: safety, reliability, and resilience, privacy and security.

Security technologies and their application to IIS is also an important part of the security framework. The evolution of technology, with improved endpoint protection, communication security and data protection, can be daunting. Many of these concepts have been around for a long time, but people are still learning how to implement and apply these concepts to industrial systems.

The Industrial Internet Consortium has actual testbeds to prove out these concepts. Members are creating several testbeds that implement functionality in different verticals. The Security Working Group is tasked with providing security & privacy guidance to the individual testbed teams for the implementation of more mature security solutions. The Security Working Group utilizes the latest approaches for holistically evaluating the maturity of the testbed security posture as it evolves.

In the coming months, the Security framework will be released to the general public.