Production life cycle stage	Secure, vigilant, resilient categorization	Cyber imperative	Objective
Digital supply network 	Secure, vigilant, resilient	Data sharing	Ensure integrity of systems so private, proprietary data cannot be accessed
	Secure, vigilant, resilient	Vendor processing	Maintain trust when processes cannot be validated
Smart factory 	Vigilant	Health and safety	Ensure safety for both employees and the environment
	Vigilant, resilient	Production and process resilience/efficiency	Ensure continuous production and recovery of critical systems
	Vigilant, resilient	Instrumentation and proactive problem resolution	Protect the brand and reputation of the organization
	Secure, resilient	Systems operability, reliability, and integrity	Support the use of multiple vendors and software versions
	Vigilant, resilient	Efficiency and cost avoidance	Reduce operating costs and increase flexibility with remote site diagnostics and engineering
	Secure	Regulatory and due diligence	Ensure process reliability
Connected object 	Secure	Product design	Employ secure software development life cycle to produce a functional and secure device
	Vigilant	Data protection	Maintain the safety of sensitive data throughout the data life cycle
	Resilient	Remediation of attack effects	Minimize the effects of an incident while quickly restoring operations and security