SEMI EU Machinery Directive Working Group Comments on the European Commission's Report on safety and liability implications of AI, IoT and robotics

June 2020

Introduction

SEMI EU Machinery Directive Working Group welcomes the opportunity to participate in the public consultation and provide its comments on the Report on safety and liability implications of AI, IoT and robotics.

Safety and liability implications of AI, IoT and robotics is a very broad topic. In this paper, we focus on AI and health and safety implications related to semiconductor manufacturing equipment. We use AI as advanced algorithms that are designed by humans to process structured or unstructured data collected in manufacturing fabs to determine optimum steps to perform a pre-defined task by the manufacturer.

Using AI in semiconductor manufacturing is not new. It was first used in semiconductor manufacturing fabs in the 1990 to help automate some productions steps which included manual work. Many semiconductor manufacturers are already using AI applications to improve the performance of semiconductor manufacturing equipment. Today's semiconductor fabs embed artificial intelligence to manage massive amounts of fault detection data, increase manufacturing efficiency and improve yields. For instance, AI enables the real-time collection and monitoring of big data, then alerts fab's system administrators of any hardware failures or other operating abnormalities. AI also makes it possible to automate adjustments and corrections to manufacturing processes by providing feedback that can drive higher processing efficiency. Integrating AI-driven solutions in semiconductor manufacturing provides value by focusing on three core areas:

- **Optimization of manufacturing processes:** The manufacturing complexity of building cutting-edge logic and memory chips needed in today's data economy is pushing the technological limits of the semiconductor industry. Through the collection, evaluation and use of big data, manufacturers have the possibility to access detailed production and processing information, advancing operations improvement, design specifications, identify variables that influence logic and memory chip quality, reliability and performance.
- **Increased industrial competitiveness and modernization:** AI innovation advances the development of novel methods, processes and technologies enabling the creation of innovative business models and cutting-edge semiconductor technologies. This, in turn, enhances the diversity and competitiveness of the semiconductor manufacturing industry, making it more reactive and adaptable to shifts and developments within global markets through a larger portfolio of technological solutions.
- **Societal and economic prosperity:** As key component of various consumer and industrial technologies, AI-enabled semiconductor innovations advance societal wellbeing and economic growth, and must be placed at the center of national, regional and global innovation strategies.

The following lists the key benefits of AI in semiconductor manufacturing:

- **Advanced Process Control:** By utilizing AI and big data, manufacturers can apply advanced control strategies and/or employ analysis and computation processes to suggest optimized machine setting and operational efficiency.

- **Predictive Maintenance:** Semiconductor manufacturers face often-unpredicted downtime throughout the production-process lifecycle. AI and big data enabled innovation can utilize the equipment and process state information; predict when a specific component, part or tool might be in need of maintenance. Big data-enabled solutions have the capacity to address the entire maintenance cycle, from predicting maintenance down-time through addressing recovery and return to production.

- **Virtual Metrology:** As a technology of post-production process variables, metrology utilizes process- and wafer-state information that could include sensor data gathered at various stages of production. Machine learning and data-enabled virtual sensing and digital twin technologies are at the forefront of industrial research and development efforts.

- **Yield Prediction:** By monitoring information across the fab, yield prediction is utilized to foresee process or end-of-line yield. Using data and machine learning can help manufacturers to find hidden patterns in processes, enabling the pursuit of continuous improvement with greater clarity.

- **Resources Efficiency:** Big data and machine learning provide semiconductor manufacturers with essential insight into production anomalies, aligning energy and other resources needed, reducing manufacturing cost and production waste.

Machinery Directive and AI

Given the specific scope described above, it is important to understand the difference between AI applications in B2C/consumer markets and B2B/industrial settings. In B2B, AI is about technical process to improve manufacturing processes.

Incorporation of AI in semiconductor manufacturing equipment has been done in a way that is compatible with the existing framework of the Machinery Directive (2006/42/EC). This Directive is well-adapted to emerging technologies and is the appropriate compliance mechanism for the semiconductor manufacturing industry.

The Machinery Directive provides a comprehensive set of essential health and safety requirements while remaining technology neutral. Its Annex I, the Essential Health and Safety Requirements (EHSRs) are foundational requirements and the provisions are deemed applicable for the risks associated with incorporation of AI in the machine. The Machinery Directive also incorporates appropriate flexibility and by promoting the use of safety standards, it can address particular requirements for machine types and their unique uses and hazards. It entrusts organizations competent in standards development taking the current stage of technology into account to achieve compliance by defining technical specifications. This framework was and is instrumental in the Machinery Directive maintaining its relevance as a cornerstone of semiconductor manufacturing equipment design.

The Machinery Directive requires that machinery placed on the market is safe to operate based on its intended use. To assure safety compliance, Annex I requires the machinery manufacturer or an authorized representative to conduct a risk assessment to determine the particular health and safety requirements applying to the machinery, then design and construct the machinery to meet those mandates. Also required by Annex I, machinery control systems must be designed to prevent any hazards in the event of system hardware or software errors such as failures in the control system logic. Only when the output from machine learning constitutes a part of functional safety (e.g. the output from machine learning is used to adjust a parameter of safety-related control system (SCS) that executes functional safety), transparency of algorithm and datasets may become critical to satisfy the safety requirement, but in such case applicable harmonized standard for functional safety will address this issue.

Therefore, machine learning only enables the semiconductor manufacturing equipment to conduct the functions that are already pre-set by the manufacturer. Machine learning algorithms never change the function or the intended use of semiconductor manufacturing equipment or the response of the interface between the equipment and the human operator and therefore do not create any unforeseen health and safety risks. The control system of any machine under the scope of the Machinery Directive is already designed and constructed in a way that it prevents the use of machine beyond its intentional use conditions.

Machinery Directive and use of robotics in semiconductor manufacturing

Robotic systems are already being incorporated into semiconductor manufacturing fabrication environments. These robotic systems are automated and may have incorporated AI but are not with autonomous operation features as in the AI systems considered within the scope of the consultation. The Machinery Directive has been the primary legislative tool for the safe and reliable incorporation of these (as above, 'these' relates to the non-autonomous robots currently used) robotic systems. Annex I of the Machinery Directive requires machinery to be designed and constructed so that it is fitted for its function, and can be operated, adjusted and maintained without putting persons at risk when these operations are carried out under the conditions foreseen. It is also required that machinery must be designed and constructed in such a way as to prevent abnormal use if such use would engender a risk. This requirement is adapted for environments where robots and humans share the same operating space. In some semiconductor manufacturing fabs, a class of robots called automated guided vehicles (AGVs) or rail guided vehicles (RGVs) transport wafer carriers and load/unload carriers to/from semiconductor manufacturing equipment. In such fabs, taking the Machinery Directive into account, robots (AGVs or RGVs) are designed and constructed considering any shared-space risks. SEMI confirms that the Machinery Directive and existing industry standards (e.g. SEMI-S17) already provide detailed and well-functioning guidance to mitigate health and safety risks related to such robots (AGVs or RGVs). Concerning any autonomous behavior, Machinery Directive EHSR shows the flexibility in its clause (1.2.1), 'Safety and reliability of control systems. Combined with improved MD guidance and additional supporting standards, it may accommodate autonomous machine behavior within its framework.

Machinery Directive, cyberthreats and software updates

A cyberthreat includes any unauthorized manipulation of a device, manipulation of remote controller devices suppressing the state of a control device, or modification of its configuration (see ENISA - Good practices for Security of Internet of Things in the context of Smart Manufacturing). These and other intentional cyberattacks are criminal acts outside the scope of the Machinery Directive and not addressed by machinery safety standards. Risk assessment standards harmonized to the Machinery Directive (e.g. ISO 12100) do not explicitly address IT security attacks, which are categorized as an intentional abuse and criminal act. The determination of the limits of the machinery as part of the strategy for risk assessment and risk reduction in ISO 12100 only considers the intended use and any reasonably foreseeable misuse (see ISO 12100:2010, Clause 4). External IT security attacks and their safety implications (via vulnerabilities of the machine control system or other electronic parts) are not considered as reasonably foreseeable misuse. However, vulnerabilities to IT security attacks are considered by manufacturers of machinery when machinery is designed to be connected to the Internet or other IT systems that can be a conduit for cyberattacks. In this case, the manufacturer refers to the guidance available in ISO/TR 22100-4. Moreover, not all machinery covered by the Machinery Directive is network-connected or even designed to be remotely monitored, controlled and to have adjustable machine parameters from outside a factory.

In addition, the recently communicated EU Cybersecurity Act introduces, for the first time, EU-wide rules for the cybersecurity certification of products. The main objective of the Cybersecurity Act is to achieve a high level of cyber-resilience and cybersecurity in Information and Communication Technology (ICT) products. The Act defines ICT products as an element or a group of network and information systems to ensure that future cybersecurity schemes specify product categories, cybersecurity requirements, standards references, evaluation protocols (e.g. self-assessment or third-party evaluation), and security assurance levels. In this light, revising the Machinery Directive to address cyberthreats, while the EU Cybersecurity Act already does so, could introduce uncertainty for manufacturers of network-connected machinery. Furthermore, machine learning software does not override safety functions performed by machine control systems to fulfil the essential health and safety requirements. Therefore, machine learning software updates should not be addressed by the Machinery Directive. Even in very limited cases, where machine learning software constitutes a part of machine's safety-related control systems (SCS), software updates are addressed by applicable harmonized standards for functional safety. SEMI underlines that the Machinery Directive should remain focused on the machine itself.

About SEMI Europe

SEMI Europe is the European arm of SEMI, the industry association connecting more than 2,400 semiconductor and electronics manufacturing companies worldwide, including nearly 300 European headquartered businesses. SEMI members are responsible for the innovations in materials, design, equipment, software, devices and services that enable smarter, faster, more powerful and more affordable electronic products. Since 1970, SEMI has built connections that have helped its members prosper, create new markets and address common industry challenges together.

Contact

Marek Kysela, EU Policy and Project Coordinator, SEMI Europe | mkysela@semi.org