

Zero Defects Manufacturing Platforms

Raul Poler^a and Ricardo Jardim-Gonçalves^b

^a CIGIP, Universitat Politècnica de Valencia, Calle Alarcón 1, Alcoy, 03801, Spain

^b UNINOVA, Universidade Nova de Lisboa, Monte de Caparica, Caparica, 2829-516, Portugal

In the last five years, many industrial production entities in Europe have started strategic work towards a digital transformation into the fourth industrial revolution termed Industry 4.0. The concept of zero-defects in the management of quality is one of the main benefits deriving from the implementation of Industry 4.0, both in the digitalization of production processes and digitalization of the product quality.

To remain competitive and keep its leading manufacturing position, European industry is required to produce high quality products at a low cost, in the most efficient way. Today, manufacturing industry is undergoing a substantial transformation due to the proliferation of new digital and ICT solutions, which are applied along the production process chain and are helping to make production more efficient, as in the case of smart factories.

As an answer to these needs a H2020 European project entitled “Zero Defect Manufacturing Platform” (ZDMP) funded under the call H2020-DT-2018-2020 “Digitising and transforming European industry and services: digital innovation hubs and platforms” and topic DT-ICT-07-2018-2019 “Digital Manufacturing Platforms for Connected Smart Factories” started in January 2019, 4 year of duration. The aim of this workshop is to show the research performed in the project during its first year and to contrast with the research performed in other H2020 projects, academia and industry. Seven papers have been presented at the vf-OS workshop:

- “A European Manufacturing Platform for Zero-Defects”: This paper presents the European Manufacturing Platform for Zero-Defects build in the frame of the H2020 project Zero Defect Manufacturing Platform (ZDMP). It discuss about the challenge faced, the concept developed and the business opportunities that the platform can provide.
- “ZDMP Technical Challenge”: This paper discusses the technical approach followed in the ZDMP project. It includes the overall architecture and specifications which are the foundation for the project’s development activities from both a functional and technical point of view.
- “ZDMP Core Services and Middleware”: This paper addresses the software components that are being developed within the Core Services and Middleware work package, which are aligned with corresponding layer: Developer Tier, Platform Tier, Enterprise Tier and Edge Tier.
- “Evolution of Industry 4.0 Platforms within H2020 Projects and Current Issues”: This paper depicts the most important concepts of H2020 platform projects in the manufacturing domain of Industry 4.0 in the last 10 years to demonstrate which issues hindered dissemination of these platforms in the past and how the following projects are evolving to get a foothold in the market.
- “A Technical Approach to Achieve Zero Defects Manufacturing Process in the ZDMP Project”: This paper proposes a holistic process quality assurance solution, which combines the partial optimization results and takes into consideration their interactions to ensure process quality by optimising three different aspects of the manufacturing process, namely the preparation stage, the production stage, and the material consumption during production.
- “Modelling, predicting, inspecting and supervising product quality for Zero Defects Manufacturing in ZDMP Project”: This paper describes the technical approach to develop solutions to control manufacturing product quality based on the different supporting services provided by the Zero Defect Manufacturing Platform, which are based on both preventing and inspecting functionalities, relying upon sensor data and other product and process information.



- “Security Implications of Interoperability”: This paper investigates the relationship between interoperability and system security. This is mainly an optimisation problem, since making a system interoperable means that some APIs need to be exposed, which can potentially open the system to malicious attacks.