Important Factors for Implementing a Resilient System

Christian Ploder [1], Julian Janetschek [2], Thomas Dilger [3], Reinhard Bernsteiner [4]

Abstract: Production systems in the context of Industry 4.0 can react flexibly to changes and failures of components by equipping the system components with some intelligence. Cyber-Physical Systems (CPS) represent a crucial technology of Industry 4.0, characterized by the integration of computation and physical processes. Future production and manufacturing plants should therefore have resilient properties in order to be able to react to faults without human intervention. In this paper, a concept for a resilient production system is discussed using the example of the Fischertechnik Learning Factory 4.0 (FTLF). In the course of this, the incidents occurring in continuous operation are determined in an observation. Based on this observation, the guidelines, strategies, prerequisites, and principles relating to the concept of resilience will be shown and discussed for the resilient architecture. The prerequisites for a resilient architecture include the absence of single points of failure and independence between the sub-components of a system. A resilient production system also requires process disruption management to handle failures with re-configurations based on previously defined possible solutions. A resilient architecture should already be taken into account in the planning and design phase, at which point all incidents that can occur in the system should be known. This fact represents a significant challenge when implementing a resilient architecture in any system.

Keywords: success factors, resilient systems, resilient architecture, systems planning

1 Introduction

The term Industrie 4.0 describes the current trend in production plants to connect the physical, embedded fully, and IT systems [**status_CPPS_WANG2015**]. Such industrial production facilities can react flexibly to changing conditions or failing components in order to remain operational and increase effectiveness [**fault_handling**]. This currently discussed paradigm is considered the fourth industrial revolution [**architecture_reconfigurable_manufacturing_systems**].

The idea of Industry 4.0 is built on vertical and horizontal integration. Vertical integration ensures a seamless flow of information, starting from corporate planning and product development to a manufacturing management system and finally to the sensors and actuators.

[1] MCI Management Center Innsbruck, MCIT, Universitätsstrasse 15, 6020 Innsbruck, AUSTRIA christian.ploder@mci.edu

[2] MCI Management Center Innsbruck, MCIT, Universitätsstrasse 15, 6020 Innsbruck, AUSTRIA julian.janetschek@mci.edu

[3] MCI Management Center Innsbruck, MCIT, Universitätsstrasse 15, 6020 Innsbruck, AUSTRIA thomas.dilger@mci.edu

[4] MCI Management Center Innsbruck, MCIT, Universitätsstrasse 15, 6020 Innsbruck, AUSTRIA reinhard.bernsteiner@mci.edu

Horizontal integration focuses on communication both between different systems and between different companies [**industrie4_0_approaches**].

Cyber-Physical Systems (CPS) are a fundamental component and critical technology of Industry 4.0 [**concept_CPS_industry_4**]. Cyber-Physical Systems first emerged in 2006 and describe the increasingly important interaction between the digital world of computer systems and the physical world. One definition describes CPS as integration of computer computations and physical processes, with embedded systems and networks monitoring the processes and often controlling each other with feedback loops [**status_CPPS_WANG2015**]. Cyber-Physical Production Systems (CPPS) is fundamentally characterized by the three properties: (1) intelligence, (2) connectedness, and (3) responsiveness. These smart components can act autonomously, collect information about their environment, and establish connections to other components and services for cooperation. A CPPS is also characterized by responsiveness to internal and external changes [**CPS_in_manufacturing_MONOSTORI2016**].

2 Theoretical Background

This chapter is dedicated to the general principles and architectural models of production facilities and on the other hand to the definition and concepts of resilience.

2.1 Conventional Automation

The previous standard architecture model of automation, called „automation pyramid“, aimed at reducing complexity by dividing the processes in a company into individual hierarchical levels. The support of the respective levels is provided by various systems such as Enterprise Resource Planning (ERP) or Manufacturing Execution System (MES). The definition of the following levels takes place according to the Purdue reference model [**automation_pyramid**]: (Level0) Production Process, (Level1) sensors and actuators, (Level2) Control Systems, (Level3) Manufacturing Execution Systems (MES), and (Level4) Enterprise Resource Planning (ERP) Systems.

Level 1 consists of the sensors and actuators that measure and influence the physical process. Level 2 is typically composed of controllers that monitor the actuators based on the measurement data from the sensors. However, level 2 can itself consist of several controller hierarchy levels. Levels 3 and 4 manage various aspects of the production plant. However, this structure dramatically limits the exchange of information between the levels [**industrial_internet_of_things**], as there are few interfaces between the respective levels [**automation_pyramid**].

2.2 CPPS and Industry 4.0

The implementation of cyber-physical production systems means a paradigm shift from the rigid hierarchical structure of the automation pyramid to dynamic and heterarchical structures [**resilience_CP_manufacturing_control**]. In order to ensure high-performance [**CPS_roots_challanges_MONOSTORI20149**] and to guarantee control of the processes in real-time [**VDI_stellungsnahme**], the speed of all participating controllers will remain very close to each other [**CPS_roots_challanges_MONOSTORI20149**]. That results in the partial dissolution of the rigidly structured automation pyramid.

The remaining systems of the different levels arrange themselves in a network structure [**Automatisierungspyramide**]. A CPPS thus consists of various autonomous and cooperative components and subsystems that can interact with each other across all levels depending on the situation [**CPS_roots_challanges_MONOSTORI20149**]. A CPPS is thus a system of complex interactions, whereby the various subsystems are independent, and thus reconfigurable [**CPPS_review_design**]. In the course of the production processes and life cycles of the products, knowledge is generated, which in turn is significant for a continuous automated improvement of the processes [**CPPS_design_challenges**]. According to [**CPPS_design_challenges**], a human component is therefore also essential in a CPPS since a large part of human knowledge cannot be formalized and transferred.

According to [**CPS_in_manufacturing_MONOSTORI2016**], the three main characteristics of CPPS are described as follows. Intelligence refers to the collection of data by the elements about their environment and the autonomous action of the elements. Connectedness is the ability to communicate with other elements and services in order to cooperate and collaborate. Moreover, lastly, responsiveness to internal and external changes [**CPS_in_manufacturing_MONOSTORI2016**].

2.3 Resilience and Dependency

Resilience encompasses both the concept of robustness as the ability to compensate for disturbances and agility as the ability to react to disturbances and reconfigure itself [**resilience_CP_manufacturing_control**]. Robustness describes explicitly the ability of a system to withstand influences from the environment during operation without loss of function [**concept_resilient_machine_2011**]. Resilience is not based on a single property of a system but is determined by the interactions between the individual components [**resilience_CP_manufacturing_control**].

The definition of resilience described in this paper is based on the concept of dependability. Resilience can be described as a consistent avoidance of unacceptable failure in the face of change. In simplified terms, resilience is the persistence of dependability in the face of change [**from_dependability_to_resilience**]. The concept includes both the threats to a system and the attributes of the system and ways to achieve dependability (Figure 1) [**concepts_of_dependability_2001**].

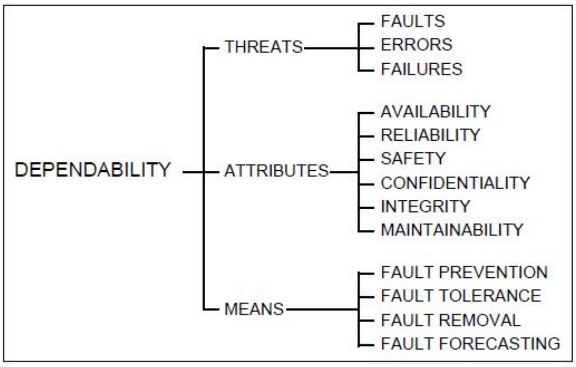

Fig. 1: Depentability Tree [**concepts_of_dependability_2001**]

Requirements for the dependability of a system include the absence of a „single point of failure“, the anticipation of all potential defects, and a system that can respond to all potential defects at an acceptable level [**comparative_analysis_fault_tolerance_etc**].

A service failure of a system designates a deviation from the executed service and the correct service that implements the function wholly and correctly.

The designation of the deviation from the correct internal or external state of a system as a fault or error is based on a deficiency in the system. An active defect results in a fault; otherwise, the defect is dormant. A fault that does not affect the external state of a system thus does not trigger a service failure [**basic_concepts_of_dependability_2004**].

2.3.1 Means for Dependability

Defect tolerance aims at avoiding service failure in the presence of defects [**basic_concepts_of_dependability_2004**]. It is considered one of the most important means to improve the dependability of a system [**comparative_analysis_network**]. It is generally implemented with the mechanisms of error detection and subsequent system recovery [**basic_concepts_of_dependability_2004**].

2.3.2 Error detection and diagnosis

Fault detection and diagnosis aim to detect and localize a failure as quickly as possible and determine the fault's type and characteristics. Simple methods of supervision are based on the evaluation of directly observable measured variables. They include checking the limit values and trends, as well as a plausibility check of the input signals [**fault_tolerance_drive_systems**].

In the approach of analytical redundancy, correlations and dependencies between variables, which are redundancy of information according to the viewpoint of information theory, are the basis for fault detection and diagnosis. The representation of the relationships between the variables is either explicit through a mathematical model or implicitly hidden in large amounts of data. Generally, however, methods based on either physical or analytical redundancy are used for this purpose [**survey_fault_detection_isolation**]. These are used to check the consistency and correspondence of the data against a model or expertise, or directly between the data itself [**data_driven_fault_detection_diagnosis**].

2.3.3 Resilient Production Systems

The authors of [**disruption_management_CPPS**] also set out general basic requirements and principles for a resilient production system. Such a system must be resistant to external influences and adaptable to disruptions. Furthermore, autonomous regulation of processes and system recovery after a disturbance is necessary. Rapid decision-making and implementation of suitable solution strategies are essential to minimize the duration of disruptions. A resilient system requires intelligent components that have a data model about their operations and processes. Furthermore, these components can exchange information and make decisions autonomously. Potential solution strategies and disruption scenarios should be stored in a database [**disruption_management_CPPS**].

In [**concept_resilient_machine_2011**], a modular architecture is recommended to allow for different configurations. However, this should be independent of each other or easily separable [**resilient_architecture**].

The presence of redundancy generally increases the resilience of a system. [**resilient_system_zhang_und_luttervelt**; **concept_resilient_machine_2011**; **fault_tolerance_MUENCHHOF2009**; **disruption_management_CPPS**; **resilient_architecture**]. The distinction is generally made between physical, functional [**concept_resilient_machine_2011**] and analytical redundancy [**fault_tolerance_MUENCHHOF2009**].

A resilient CPPS should be able to detect and analyze a defect automatically and then respond to it using one of the following four strategies: (1) Reconfiguration, (2) Controller Reconfiguration, (3) Stop of Operations and (4) Repair. [**resilient_architecture**; **fault_tolerance_MUENCHHOF2009**]

3 Empirical Study Design

This paper is dedicated to the research question: How can a concept for resilient production systems and the implementation of resilient properties look like using the example of the FTLF?

The FTLF maps a holistic production process, starting with the order and continuing through the production process to product delivery. The plant consists of the following modules, which are interconnected via a network [**fischertechnik**].

- SSC: Sensor Station with swiveling camera
- HBW: High-bay Warehouse
- VGR: Vacuum Gripping Robot
- DPS: Delivery Station with Near Field Communication Reader
- MPO: Multi Processing Station with furnace
- SLD: Sorting Line with color Recognition

The determination of potential incidents that may occur during the continuous operation of the FTLF takes place in a second step and the course of observation. The continuous operation of the plant takes place in two steps. First, the complete filling of the high-bay warehouse with the workpieces takes place by positioning the workpieces one after the other in the material storage area. The orders for the workpieces that are then placed empty the warehouse again. That followed by the material storage step again and the filling of the warehouse. After a malfunction has occurred, the system is returned to its initial state.

The observation method belongs to qualitative research and is a data collection method based on intentional, purposeful, and selective perception. The form of observation determines the degree of purposefulness and selectivity. The differentiation of the various forms of observation from each other is made based on various dimensions. The observation system, which describes the scope of guidance in the course of implementation, characterizes either structured or unstructured observation. The observation system includes, among other things, how the observation data are recorded. The extent to which the object of observation is restricted in advance in terms of documentation, the behaviors to be recorded, and the object of observation thus determines the structuredness of the method.

In the context of this paper, the classification of the observation procedure is as follows. The observation scheme involves logging the collected data in natural language, and the processes in the factory in the course of continuous operation are observed without restriction. The observer also influences the factory by returning the plant to its initial state in a malfunction. Thus, the method can be classified as unstructured or unsystematic. The distinction between overt and covert observation is not relevant in this context, as the object of observation is a thing. The observer perceives the events in the course of an unmediated observation and subsequently describes the events in natural language [**qualitative_sozialforschung**; **Kochinka2010**; **sarantakos2012social**].

4 Results & Discussion

The implementation was divided into six sessions of 4-5 hours each and done from May to July 2021. The incidents that occurred and were perceived in operation are assigned to a module and a component. The errors are shown in table 1.

Tab. 1: List of the observed incidents

Module	**Component**	**Error**	**Description**
Vacuum Gripping Robot (VGR)	Vacuum Gripper Suction Cup	#1	The vacuum gripper arm does not pick up the workpiece and it therefore remains in the material delivery station, in the storage container or in the storage locations
		#2	The vacuum gripper arm loses the workpiece after it has been successfully picked up in the course of onward transport
Multi Processing Station (MPO)	Vacuum Gripper Suction Cup	#3	The vacuum suction cup does not pick up the workpiece
	Rotary Table	#4	The workpiece is thrown from the surface in the course of the rotary movement
		#5	The workpiece is clamped in the course of the rotary movement between a spacer and the table
High-bay Warehouse (HBW)	High-bay Warehouse	#6	A workpiece delivery to a fully occupied warehouse
Sorting Line (SLD)	Conveyer Belt	#7	The workpiece gets stuck on the transition between conveyor belts

The FTLF does not implement a complete architecture about the automation pyramid presented in 2.1. The sensors, actuators, and TXT controllers in the modules of the learning factory implement levels 1 and 2 of the automation pyramid. In a CPPS, however, these levels are not fundamentally different from the traditional approach of the automation pyramid [**CPS_roots_challanges_MONOSTORI20149**].

The sensors and actuators of the modules are directly connected to the associated controllers utilizing cables and are thus not wholly independent of the associated module. That means that only limited reconfiguration [**resilient_architecture**] is possible at the module level, but not at the component level [**CPS_methodsAndApplications**].

The wireless communication of the modules takes place via a single node, whose failure then brings the entire communication of the system to a standstill. Similarly, the MQTT protocol standard defines the broker as the central node to which each client must connect in order to exchange data with other clients [**data_exchange_MQTT**].

These circumstances represent a „single point of failure“ and according to [**comparative_analysis_fault_tolerance_etc**]; however, avoiding such scenarios means an essential requirement for the resilience of a system.

According to [**resilient_architecture**; **disruption_management_CPPS**], the FTLF does not have any resilient properties in its factory state. In addition, the basic properties of a CPPS are not fulfilled by the learning factory. [**CPS_in_manufacturing_MONOSTORI2016**]

One way to remove the „single points of failure“ is to provide physical redundancy by duplicating the hardware and merging multiple MQTT brokers into a cluster. The majority of solutions currently available, however, are proprietary. These include, for example, HiveMQ^{TM}, which defines the MQTT broker clusters as a single logical MQTT broker regardless of the actual active number [**federation_of_MQTT_Brokers**].

For implementing a resilient architecture with the help of reconfiguration methods, the recommendation of implementing a mesh network also applies. That requires the components or subsystems to be independent of each other [**resilient_architecture**]. Implementing a software-based reconfiguration at the level of the sensors and actuators in the FTLF requires the connection of the controllers with the sensors and actuators via cables to form a mesh network. The sensors and actuators in the factory state do not have the option of wireless communication.

In the factory state of the learning factory, fault detection and handling are only implemented for a workpiece that has broken down in the material delivery station concerning fault #1. If an attempt is made to read the NFC tag of the workpiece using the NFC reader, but the tag cannot be read, an error is detected, and the gripper arm is activated again. In the other situations, no clear differentiation and identification of the faults #1 and #2 are possible in the factory state. Only a subsequent installation of sensors can make this possible.

Fault detection with the already existing sensors is only possible concerning the faults #3, #6, and #7. For faults #4, a subsequent installation of sensors is necessary. The detection of failure mode #5 can be implemented with a subsequent software implementation.

Possible fault treatments can include, among others, a cancellation of the order, return of the components to the initial state, and reactivation, as well as an alternating rotation of the running direction of the motors. These are all based on a reconfiguration of the controllers, as there are no physical or functional redundancies in the FTLF to respond to these faults.

5 Conclusion

The basic requirements of dependability include the absence of a „single point of failure“, the **anticipation of all possible defects** and the management of these predicted defects at an acceptable level. However, predicting all possible defects in a system is a major challenge [**comparative_analysis_fault_tolerance_etc**]. All the deficiencies are ideally analyzed in the design phase and listed with their causes [**resilient_architecture**]. General principles and prerequisites for a resilient production system are also intelligent components and a digital data model of these components [**disruption_management_CPPS**], **modular and independent components** [**resilient_architecture**] and **physical as well as functional redundancies** in the system [**resilient_system_zhang_und_luttervelt**; **concept_resilient_machine_2011**; **fault_tolerance_MUENCHHOF2009**; **disruption_management_CPPS**; **resilient_architecture**].

A process failure management system needs detailed information about the failures for a correct response [**fault_tolerance_MUENCHHOF2009**]. The storage of possible solution strategies for process disturbances is done in advance in a database [**disruption_management_CPPS**]. Some of the knowledge about production processes and components is only built up during the execution of the processes. Likewise, the formalization of human knowledge can be a challenge [**CPPS_design_challenges**]. To overcome this challenge, the data combination of a system-wide ticketing system and a quality management-based deviation management system, as required by most of the quality norms, could help get deeper insights into the failure from the past and continually improve the resilience of the new system. Every defect is mentioned in these systems, and the corrective action and preventive action are documented there (ISO 9001:2015).

With the requirements as mentioned above of dependability, the points of the absence of a „single point of failure“, presence of physical and functional redundancies in the system, and intelligent components are not entirely fulfilled. The modules of the learning factory can be arranged and exchanged as desired [**fischertechnik**]. That fulfills the requirement of modules being independent of each other. However, the individual elements such as sensors and actuators in the respective modules are not independent.

The **maintainability of the program code**, in order to be able to carry out possible subsequent implementations of functions or removal of the defects, should generally be given high priority. Maintainability is also an essential component of dependability [**concepts_of_dependability_2001**].

A system developed with the concept of CPPS with autonomous and cooperative components and sub-systems [**CPS_roots_challanges_MONOSTORI20149**] facilitates the **subsequent installation and replacement of physical components and modules** because of their independence from each other.

6 Limitations and Future Research

The changes discussed and proposed in this paper for a resilient architecture are limited due to the factory condition. Retrofitting hardware such as sensors or subsequent modification of the software was not carried out for the data collection in the observation. Future work will implement the presented improvements for a resilient architecture. That will be followed by a re-evaluation of the resilient properties of the learning factory and further improvements. For more practical-oriented application scenarios, it would be interesting to connect the idea of process documentation (5 in machine-readable formats that can then be used as a database for machine learning and connected system improvement.