CHALMERS

Chalmers Publication Library

Error handling within highly automated automotive industry: current practice and research needs

(article starts on next page)

Error handling within highly automated automotive industry: current practice and research needs

Ashfaq Farooqui, Patrik Bergagård, Petter Falkman, and Martin Fabian

Department of Signals and Systems
Chalmers University of Technology, Göteborg, Sweden 412 96
Email: {ashfaqf, patrik.bergagard, petter.falkman, fabian} @ chalmers.se

Abstract—Fault tolerant systems, commonly found in literature, are implemented in various computer applications. Some of these methods have been studied and developed to aid manufacturing systems; however, they have rarely been integrated into the manufacturing process. Broadly, the problem seems to be integration of error handling procedures towards the end of physically building the manufacturing line, lack of a defined workflow, untested program logic and inadequately equipped personnel to name a few. To this end, a survey was conducted within the Swedish automotive industry to get an understanding of current error handling procedures and its shortcomings, and are presented here. Based on this data, and looking at the trends within the manufacturing industry, this paper also identifies research topics aimed towards defining methods to create next generation fault tolerant manufacturing systems.

I. Introduction

Complexity of automotive manufacturing industry is constantly increasing to keep up with advancement in technology, market trends, legislative requirements, and most of all high quality products. To this end, the systems developed are highly automated with minimal manual handling; they must not only take into account flexibility, efficiency, and development time, but also account for fault tolerant behavior.

Development of automated manufacturing systems is a demanding task. One of the main hurdles is the inability to validate and verify all requirements before physically commissioning the system; this means the physical system needs to continuously be upgraded when problems are encountered in the design. As a consequence, human operators – maintaining these systems – need to be highly skilled, but cannot be given sufficient training until the physical system is commissioned.

Advancement in technology today promises tools and methods that may help overcome these hurdles and will eventually lead to improved designs and more robust solutions. Formal methods and virtual commissioning are good examples of this, that while not previously adapted due to lack of usable tools, are gaining acceptance within the automotive industry. Using these tools will allow industries to first verify and virtually validate a design before physically commissioning the system. Additionally, it will allow operators to be trained within the virtual space; thereby increasing efficiency.

According to Loborg [1], a *fault* is what causes a difference between the specification of a system and that which is observed, also known as an *error*. A *failure* is said to occur when an *error* results in a loss of service. Fault tolerant systems – systems that can handle an error without affecting the service delivered – have been studied in academia within the area of computer science. A number of these methods have been developed for manufacturing systems: Loborg [1] provides a survey of these methods; a case study analysis of eight industries using fault tolerant techniques is presented by Vogel-Heuser et al. [2]; Gao [3], [4] gives an elaborate overview on detection and diagnosis within fault tolerant systems. There is however, a lack of defined workflow that will help design, verify, and validate a manufacturing system before physical commissioning to ensure fault tolerance. *Error handling* on the other hand is the course of action employed, after occurrence of an error, to mitigate its effects and avoid a failure scenario. The present paper will use these definitions for the three terms – *fault*, *error*, and *failure* – while looking at current trends in the industry and providing possible research topics.

A. Contribution

This paper is part of ongoing work aimed towards defining a process to build fault tolerant manufacturing systems. It presents an overview of current error handling procedures employed in the industry today and its shortcomings – based on a survey conducted within the body-in-white segment of the Swedish automotive industry. Based on the problems identified from the survey, this paper will introduce future research areas that aims at supporting operators during error scenarios both for virtual and physical systems. The main idea with such techniques is to define a framework and workflow that will incorporate error handling into the initial preparation phase of the manufacturing system. Also, the paper suggests an additional step to the already existing process to ensure safety of the manufacturing line.

B. Outline

The paper is divided as follows: Section II provides an overview of current industrial setup and processes for error handling. This is followed by a brief outline of the survey results in Section III. Section IV provides some insights into future direction of the manufacturing industry which influence the proposed framework. Finally, Section V suggests possible research topics aimed towards creating fault tolerant systems.

II. Background

Within the body-in-white segment, a manufacturing *line* generally consists of a number of manufacturing *stations* – each responsible for a specific task, such as spot welding, stud welding, gluing etc. These tasks are generally performed by resources including, a certain number of robots needed for the actual process; further assisted by conveyors or Automatic Guided vehicles (AGV) for material handling. Tools, tool changers, and other task specific actuators are also present. The complete station in a broad perspective normally consists of a number of sub-stations: manual or automated feeding sub-stations; process sub-station, where the actual process takes place; a checking sub-station to ensure quality; and an unloading sub-station that feeds the product into the next station.

A manufacturing station can broadly be divided into: *physical system* consisting of resources and the product parts; and *control system* that defines the behavior of the station. This control system consists of a number of operations that must be executed in a defined manner by the physical system. For the control system to effectively control the physical system it is important that their states are always synchronized, here the *state* refers to a set of variables that capture the properties of a system or subsystem in a unique way.

A. Error handling process

Inspired by [1], [5] divides the process of error handling into the following phases:

- *Detection*: Where the actual state of a system is monitored and compared with its specifications in order to determine any discrepancies during execution.
- *Diagnosis*: Once an error has been detected, using available information to determine the fault that caused the specific error.
- *Correction*: Here the fault which caused an error is corrected, either by replacing or fixing the faulty part, usually by intervention of an operator.
- *Restart*: In order to continue execution safely and efficiently after the correction phase, the control system and physical system are resynchronized i.e making state of the controller and physical machinery to correspond, resulting in process restart.

During the restart phase, the state of the physical system is changed to a legal one by the operator. The challenge is then, to modify the controller state to correspond to the new physical state [6] so as to allow safe and efficient restart.

Though there have been a plethora of approaches towards fault tolerant systems within academia, there is no clarity on how many have been tested and implemented within the industry. The reason being lack of tools, processes and more often than not a disconnect between industry and academia.

III. Survey summary

A survey was conducted involving Volvo Cars, Volvo Group Trucks, Scania, National Electric Vehicle Sweden, and GKN Aerospace. The main intention was to identify and understand common errors faced in these industries, how they are dealt with, and measures taken to ensure fault tolerance.

A. Error scenarios

A set of commonly occurring errors that were identified are discussed below:

- Tool breakage is generally one of the most common fault that result in an error leading to loss of service; in extreme cases it might result in scrapping of the part. Detection and diagnosis in this case is rather quick, correction is fault dependent in most scenarios. The restart phase is handled in various ways depending on the task performed by the station. In some cases where cycle time is a few seconds (0-5s), re-running the complete cycle has no effect; in other cases when the process takes more than few minutes (15-45 min) re-running the complete process is redundant and might induce lags in the manufacturing line.
- Missing parts or buffer shortage are rarely an issue in the surveyed manufacturing stations as they are manually fed. In any case, if there is a missing part, production is paused and will be resumed when there is availability of the said part. Though there is no need for error handling procedure, it often results in a delay for the manufacturing line. Such delays tend to cause unsynchronized behavior in the subsequent stations possibly resulting in an unintended sequence of operations.
- Resource malfunction, i.e when any one of the resources in the station breaks down; this can result in a complete halt of the station or a temporary break. If the resource is replaceable it is replaced and production continues. On the other hand, if the resource cannot be replaced, for example a robot, then production is delayed until it has been repaired. The restart procedure in this case remains similar to that of tool breakage; the specifics are left to the operators discretion.
- Software bugs are not so uncommon in a manufacturing station and take up considerable amount of time to diagnose and implement permanent solutions. Since changes need to be made directly to the system, each bug fix may, as a side effect, inject new bugs. Apart from this, detection and diagnosis of software bugs requires highly trained and experienced personnel.
- Power outage is not a very common problem in industry today, there are backup systems to keep the production going. However, there are instances of power outage, e.g due to lightning. The problem lies not in the loss of power but rather its effect, as the *manufacturing stations* in the *line* could be unsynchronized with its respective control system; this can complicate the recovery process. In restarting the line, there lies a major risk of damage to the various stations or a product part. The operator is then responsible to ensure the different systems are in the correct and safe state in-order to restart. This process is cumbersome, manually exhaustive and results in loss of production time.

- Preemptive emergency stops, as the name suggests, halts the manufacturing station in order to prevent the occurrence of an error. This is usually done on recognition of a fault by the operator as a safety measure. The effects are similar to that of power outage, and the operator is faced with the same challenges to ensure the safety of the complete line. Apart from this, there is no data from the manufacturing line to help further diagnose and study the fault.
- Unintended sequence of operations was not reported as a commonly occurring problem in the survey, mainly because most manufacturing stations have a fixed sequence of operations predefined in the control system. Hence, the manufacturing station can perform a single process. By allowing the control system to dynamically create the sequence of operations the station will then allow processing a range of product parts. In the future, with highly automated systems in which dynamic sequences are the norm, the control system must be verified to avoid occurrence of unintended sequences.

All the above errors implicitly require the operators to be highly skilled to handle any error scenario. This further opens up possibilities for human error due to miscommunication, lack of training and documentation, or misjudgment of the situation.

B. Measures to avoid error handing scenarios

Given the process of handling errors, having skilled operators is key to high productivity and low downtime. Apart from the training every operator is provided, line builders provide instruction manual or remote/on-site assistance to help support operators. In cases where there are multiple operators working within a single station, an internal operator manual and a logbook are maintained to support knowledge transfer and allow for better judgment.

During the preparation phase, before physical commissioning of the manufacturing station, simulations are run to make sure no geometric reachability issues arise. Apart from that, no other simulations are run to verify any other aspects of the system. Physical subsystems are generally validated along with function blocks at the line-builders site; the next stage of testing, today, is only when the station is setup. After which the logic and station are iteratively modified and validated. In this procedure, error scenarios are considered at a late stage of commissioning, generally after the physical station is commissioned. This leaves very little room for modifications and to incorporate error handling.

IV. Future trends within manufacturing

Proposing effective ideas as solutions to the scenarios discussed in Section III must also take into account technological heading of the industry. This section introduces research questions, pursued by both academia and industry, that either require additional consideration to make them fault tolerant or will provide a framework to help realize the solutions.

Industry 4.0 [7], also called as the fourth industrial revolution, can be seen as a collection of various technologies – Internet of Everything(IoE), Cyber-physical Systems (CPS), and smart factories – to create the next generation of industrial systems [8]. Enabled by interaction between products, machines, and people, future industrial systems will be able to make smart decisions. From the design principles of Industry 4.0 provided by Hermann et al [8], distributed modular systems are key to build these next generation factories. Various projects directed towards the future of industrial systems have been initiated in many countries; *Factories of the Future* [9] is one such long term project running within the EU.

Automated robot systems are finding space within ship construction [10] and within aircraft construction [11]; the unique feature here is that the product stays in one place, while the robots move around depending on task and requirement to perform their respective operations. These types of systems increase complexity to keep the physical and control system synchronized, hence a robust control strategy and decision making algorithms are needed. Furthermore, verification of restart methods for multi-robot distributed systems needs to be well defined.

Apart from distributed systems, flexible or reconfigurable system design is another key factor in the Industry 4.0 vision. These systems will allow for dynamically changing configuration based on product requirement. One such project is *Factory in a day* [12] where a new manufacturing line can be setup in a short time. Or, it can be used to temporarily extend an existing manufacturing line to cater to market needs. While the project is aimed at Small and Medium scale Enterprises (SMEs), it has created interest within a larger community. In the light of fault tolerance, the reconfigured systems must be compatible with the existing error handling work-flows, and must also be verified for fault tolerance before changing the physical system.

Manufacturing lines produce large amounts of raw low-level data during each operation cycle. This data is then refined to provide meaningful information regarding the manufacturing line, which can further facilitate real-time decision making. To this end, Theorin et al. [13] provide a *Line Information System Architecture (LISA)* – an event-based service-oriented architecture which is both flexible and scalable. Manufacturing lines capable of utilizing this can provide much needed help in building future fault tolerant systems and improved error handling procedures.

Integrated Virtual Preparation and Commissioning (IVPC), introduced in [14], provides a framework to iteratively design and develop a manufacturing system within a virtual environment. In this method, the control system is implemented employing formal tools and validated, both against visual inspection and computations by formal methods, using a virtual model before actual commissioning of the station. Apart from providing an agile process to construct the control system, such a framework also allows for hardware-in-the-loop testing and virtual training for operator personnel.

V. Research needs

In Section III various error scenarios that effect the manufacturing station were presented. After an error-causing fault has been corrected, the physical and control system are unsynchronized; synchronizing the two is part of the restart phase referred to as resynchronization. Unlike Loborg [6] who suggests changing the internal controller state to correspond to that of the physical system, Bergagård et al. [5] suggest that the control system is changed to a state from where it is correct to restart the system, and that the state of the physical system is changed accordingly. This method has been validated in a windscreen mounting station [15] with positive results. This solution holds for error scenarios like tool breakage, machine malfunction etc, but does not address safety of the complete manufacturing line on restart after a power outage or an emergency stop. Hence, an additional phase after the restart phase is suggested for further study, henceforth called *assurance phase*.

The *assurance phase* is made possible by using raw low-level data collected during the operation cycle, similar to the LISA project discussed earlier in Section IV. Using the current and last known sensor values to determine the state of the system and comparing this with the intended state, safety measures can be computed. Then, the control system will guide an operator to re-start the manufacturing line safely.

Another issue touched upon in Section III is the use of a logbook by operator personnel. In many cases this book is not well updated or could be misinterpreted leading to misjudgment and unwanted decisions. Maintaining logs of raw sensor data, a *digital logbook* in this case can come of use, instead of using manually maintained logbooks. The functionality of such a *digital logbook* can be extended to: help diagnose errors; facilitate training of operator personnel using the virtual environment to recreate various scenarios; and use in restart situations for safety assurance as already discussed.

To be able to achieve both, *assurance phase* and *digital logbook*, functionalities a common format for the logged data needs to be defined. Algorithms to efficiently, process, analyze, visualize, and store such large amounts of data need to be created. Additionally, the defined format must support interoperability between the physical system and its virtual counterpart.

Another area of study within error handling is distributed systems. With distributed systems decision making is decentralized, for example in ship and aircraft construction robots discussed in Section IV. As there is no centralized controller keeping track of individual subsystems, there is a need for formal tools and processes that will enable modeling and verification of such decentralized systems, specifically to ensure fault tolerance. Once a technique to model and verify decentralized systems is in place, the actual restart of such manufacturing system is of interest. A study of well defined workflow and efficient algorithms that can guide the operator to safely restart one or more resources will provide much needed foundation.

VI. Conclusion

In conclusion, a survey conducted within Swedish automotive industry exhibited the need for a framework and work-flow to handle the following problems:

- Restart after power outage and emergency stops.
- Software bugs after commissioning.
- Training and support to personnel.
- Knowledge transfer and maintenance.

Based on future trends within the industry, this paper presented a need for further study on:

- An additional *assurance phase* after resynchronization.
- Use of logged data– *digital logbook* – from the manufacturing line to perform *assurance*; maintain knowledge; and, train personnel using the virtual world.
- Data format and algorithms to realize an *assurance phase* and a *digital logbook* leading to a fault tolerant system.
- Modeling and verification of restart within distributed and decentralized systems using formal methods.
- Validating restart of one or more distributed and decentralized system resource during active process.

References

[1] P. Loborg, "Error recovery in automation an overview," in *AAAI-94 Spring Symposium on Detecting and Resolving Errors in Manufacturing Systems, Stanford, Ca, USA*, 1994.

[2] B. Vogel-Heuser, S. Rösch, J. Fischer, T. Simon, S. Ulewicz, and J. Folmer, "Fault handling in plc-based industry 4.0 automated production systems as a basis for restart and self-configuration and its evaluation," *Journal of Software Engineering and Applications*, vol. 9, no. 1, p. 1, 2016.

[3] Z. Gao, S. X. Ding, and C. Cecati, "A survey of fault diagnosis and fault-tolerant techniques;part ii: Fault diagnosis with knowledge-based and hybrid/active approaches," *IEEE Transactions on Industrial Electronics*, vol. 62, no. 6, pp. 3768–3774, June 2015.

[4] Z. Gao, C. Cecati, and S. X. Ding, "A survey of fault diagnosis and fault-tolerant techniques ;part i: Fault diagnosis with model-based and signal-based approaches," *IEEE Transactions on Industrial Electronics*, vol. 62, no. 6, pp. 3757–3767, June 2015.

[5] P. Bergagård and M. Fabian, "Calculating restart states for systems modeled by operations using supervisory control theory," *Machines*, vol. 1, no. 3, pp. 116–141, 2013.

[6] P. Loborg and A. Törne, "Manufacturing control system principles supporting error recovery," in *Proceedings of the AAAI Spring Symposium on Detecting and Resolving Errors in Manufacturing Systems, Palo Alto, CA, USA*, vol. 2123, 1994.

[7] H. Lasi, P. Fettke, H.-G. Kemper, T. Feld, and M. Hoffmann, "Industry 4.0," *Business & Information Systems Engineering*, vol. 6, no. 4, pp. 239–242, 2014. [Online]. Available: http://dx.doi.org/10.1007/s12599-014-0334-4

[8] M. Hermann, T. Pentek, and B. Otto, "Design principles for industrie 4.0 scenarios," in *2016 49th Hawaii International Conference on System Sciences (HICSS)*, Jan 2016, pp. 3928–3937.

[9] "Factories of the future." [Online]. Available: http://www.effra.eu/

[10] "Carlos." [Online]. Available: www.carlosproject.eu

[11] "Cablebot." [Online]. Available: www.cablebot.eu

[12] "Factory-in-a-day." [Online]. Available: www.factory-in-a-day.eu/

[13] A. Theorin, K. Bengtsson, J. Provost, M. Lieder, C. Johnsson, T. Lundholm, and B. Lennartson, "An event-driven manufacturing information system architecture," in *IFAC/IEEE Symposium on Information Control Problems in Manufacturing, INCOM*, 2015, pp. 547–554.

[14] M. Dahl, K. Bengtsson, P. Bergagrd, M. Fabian, and P. Falkman, "Integrated virtual preparation and commissioning: supporting formal methods during automation systems development," 2016.

[15] P. Bergagård, P. Falkman, and M. Fabian, "Modeling and automatic calculation of restart states for an industrial windscreen mounting station," *IFAC-PapersOnLine*, vol. 48, no. 3, pp. 1030–1036, 2015.