Enhancement of machine productivity and availability in functional safety applications using failover concept with Safety PLCs

Yauheni Veryha

ABB Automation Products GmbH, Eppelheimer Str. 82, 69123, Heidelberg, Germany

Email: yauheni.veryha@de.abb.com

Fan Dai

ABB Corporate Research Center, Wallstadter Str. 59, 68526, Ladenburg, Germany

Email: fan.dai@de.abb.com

Hao Ding

ABB Corporate Research Center, Wallstadter Str. 59, 68526, Ladenburg, Germany

Email: hao.ding@de.abb.com

Abstract:

Safety reaction to hazard events often leads to machine stops with increased downtime of machines. These events are usually triggered by safety devices that detect hazards or when safety devices become defective or unavailable due to failure.

Usage of Safety PLCs with the “failover” concept can enhance the productivity and uptime of machines and manufacturing systems significantly so that machine interrupts can be minimized or even be avoided in many cases. The resulting increase of productivity and availability can be estimated based on anticipated frequency of temporary errors, like communication errors and hazard events, average duration of downtime due to such events, etc. In many customer cases, like those in Assembly Lines, Food and Beverage and Material Handling applications, the effort of implementing additional safety control functionality with failover concept using Safety PLCs pays off.

1 INTRODUCTION

Safety control in discrete manufacturing has the primary goal of protecting humans against hazards, when working at or entering manufacturing sites. Sensors or switches are used to inform a safety control device about the presence of humans in specific zones or their attempt to enter such zones. Based on the actual status of the automated manufacturing process, the manufacturing line or individual devices are put into a state that reduces or limits potential hazards to a specified, acceptable range. Very often, this is achieved by stopping the machines, but sometimes it is also sufficient to reduce the speed of motion or to limit the space of movements of particular mechanisms, e.g. industrial robots, AGVs (Automatic Guided Vehicles) or machine tools. In case of (potential) severe hazards, emergency stop is issued, e.g. via emergency stop button or corresponding sensing devices. It brings the machine into a safe state, which usually needs later an acknowledgement to restart the machine.

In some situations which also often happen in practice, machine safe stops are not necessary. For example, in case faulty communication to a safety sensor or a failure in the sensor device itself is detected, a machine safe stop is usually directly initiated, despite the fact that unavailability of the sensor is often only temporary, for example, due to temporary EMI (Electromagnetic Interference) or communication errors. The failover concept, if implemented as further described using Safety PLCs (Programmable Logic Controller), can be used to bridge this temporary sensor failure, and, thus, avoid triggering unnecessary safe stop in such situation without compromising on safety integrity level expected. This can further enhance the productivity and availability of the machine towards efficient manufacturing resulting in reduced operating costs.

2 SAFETY REACTION WITH FAILOVER

A typical hazard event is that a person enters a work zone where an operating machine may harm the person seriously. Traditionally, if such an event is detected, the machine is stopped instantly. However, the severity of such a hazard can be differently assessed so that sometimes the machine can run at a safely limited speed instead of a complete stopping and, as a result, the overall productivity of the machine is enhanced significantly. A good example is an AGV (Automated Guided Vehicle) which can run within a safely limited speed, if obstacles or human worker is within certain area and it stops, when the distance becomes critical, as it is shown in the example in Figure 1. This reaction can be done by applying the “failover” concept that means switching to a redundant device or function, when a dedicated device or function fails.

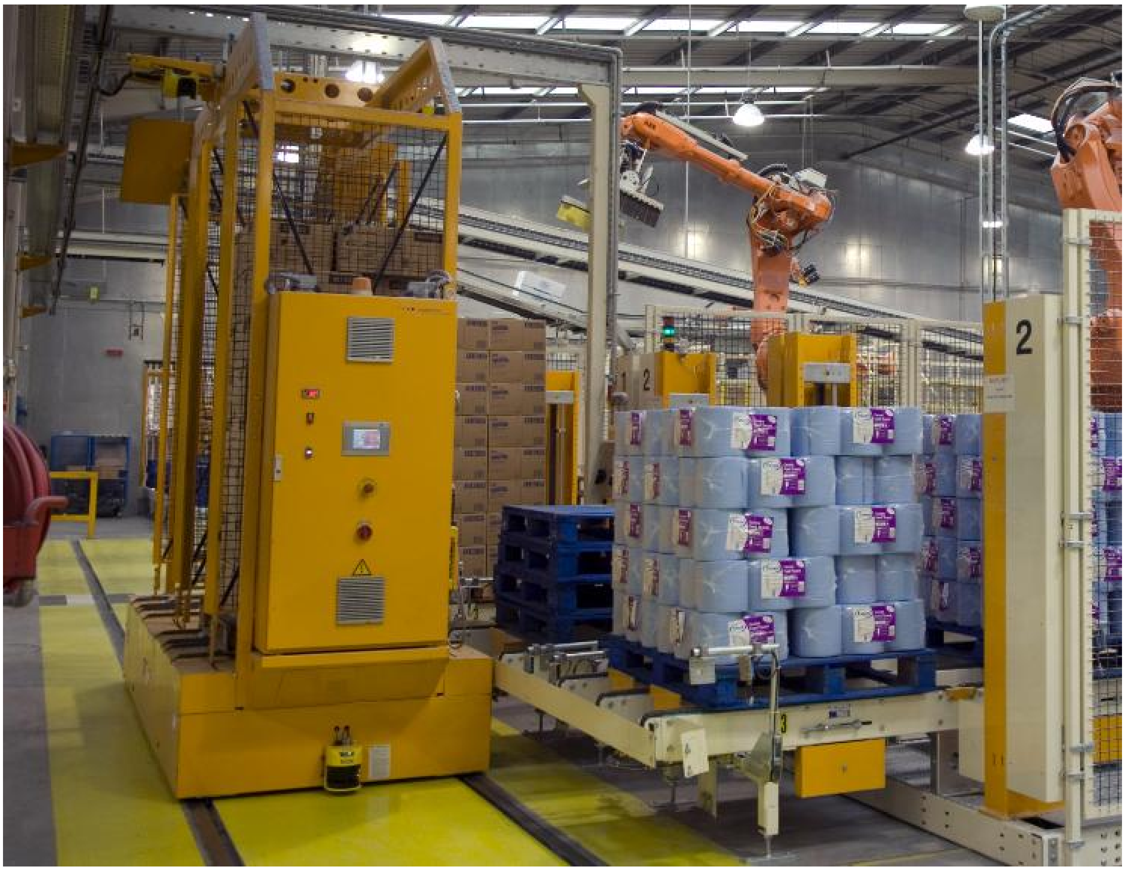

Figure 1: Example with AGV and safety work zones

To explain the failover concept, we assume the following scenario for AGV:

- AGV has a safety laser scanner sensing the front area ahead for detecting a localized hazard event and triggering a safety function (e.g. safe stop) through the Safety PLC. AGV can move only forward.
- There is a remote safety camera installed in the production facility and safely observing the working area of AGV for detecting a less-localized hazard event and triggering a safety function (e.g. safely limited speed) through the Safety PLC.

In most of current safety applications, the events of triggering safety reaction from the safety laser scanner and/or remote safety camera and failure of laser scanner and/or remote safety camera are equivalent and lead to the pre-defined safety reaction predominantly a safe stop. There is still one open question left: What if the failure of the safety laser scanner and/or remote safety camera is only temporary or momentary? Typical reasons for temporary communication errors in safety applications are electromagnetic interference, short power supply drops (< 20 ms), network traffic load, wireless drop-outs or cyber attacks, which can cause PROFIsafe (safety profile for PROFINET and PROFIBUS, refer to http://www.profibus.com/technology/profisafe/ for more details) to trigger a safety function without an actual demand. In most safety applications, there is no differentiation between temporary and permanent failures and, thus, the pre-defined safety reaction is usually a safe stop.

Failover concept can provide an alternative to a direct safe stop provided that there are means in the Safety PLC to differentiate those two events (triggering safety reaction from the safety laser scanner and/or remote safety camera and failure of safety laser scanner and/or remote safety camera) and safe measurement of time (e.g. using timers in the Safety PLC) to identify and measure the duration of temporary failures. There are Safety PLCs with an option to differentiate in the safety application logic part different events such as:

1. Real triggering of safety function from the safety laser scanner and/or remote safety camera
    - *Safety application logic mean*: Safety process variable state
2. Malfunction or unavailability of the safety laser scanner and/or remote safety camera due to an undervoltage, temporary communication error (CRC (Cyclic Redundancy Check) or Watchdog), etc.
    - *Safety application logic mean*: Use of safety diagnostic bits in addition to safety process variable state in a safety application program;
    - *Safety application logic mean*: Use of PROFIsafe safety variables (detected CRC or Watchdog errors) for PROFIsafe devices, as defined in PROFIsafe specification in addition to safety process variable state in the safety application program
    - *Safety application logic mean*: Use of timers in the Safety PLC to measure the duration of failures.

Safety network protocol like PROFIsafe (see Figure 2) supports the recognition of communication errors and device faults, which enables us to distinguish between the temporary communication error and the device faults. Due to the availability of above-mentioned functionality with differentiation of events (triggering safety reaction from safety laser scanner and/or remote safety camera and failure of safety laser scanner and/or remote safety camera) in some Safety PLCs, one can easily implement the so-called failover concept in machine safety applications. It is largely based on the concept that the temporary failure of a safety device does not always lead to a safe stop, but can be temporarily safely bridged by the re-configuration (pre-defined safety reaction as part of the failover concept) of safety program logic execution and reaction on safety events.

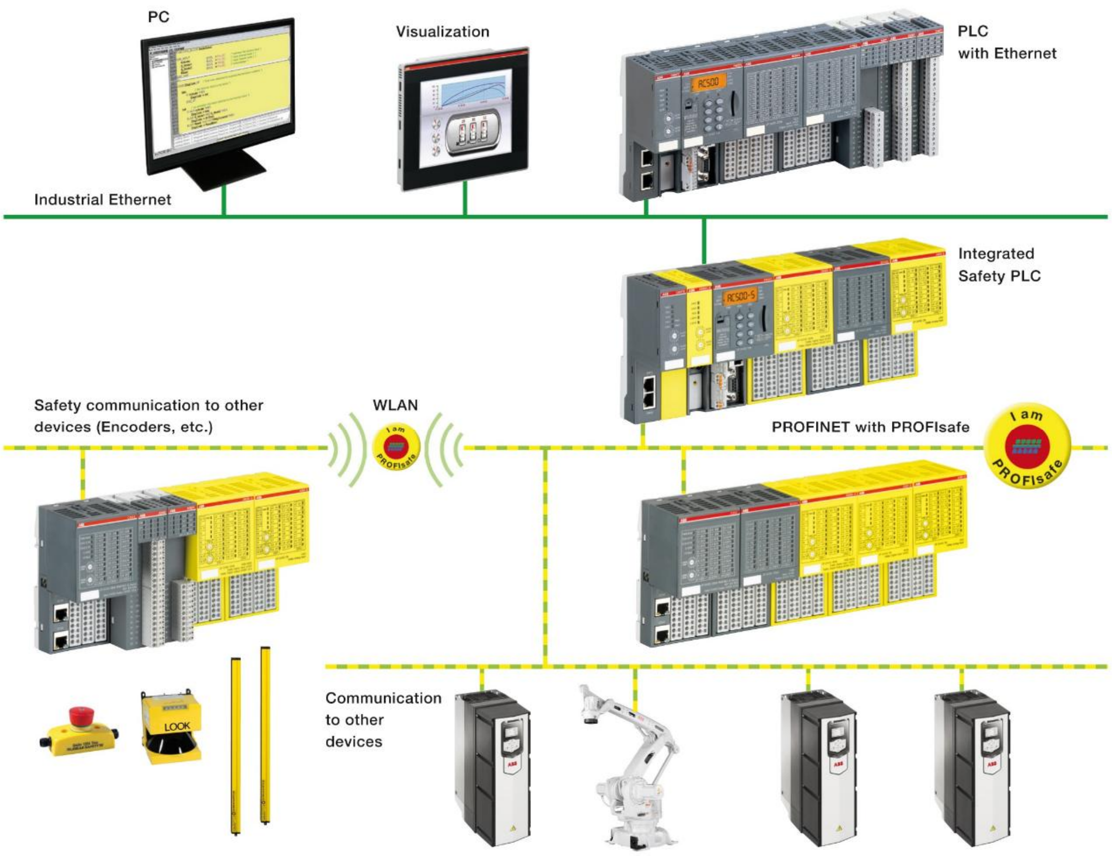

Figure 2: Exemplary PROFINET/PROFIsafe network with advanced failure detection means in safety application program on Safety PLC

The failover concept with pre-defined reactions on safety events has to be, of course, taken into account in the overall machine safety design, verification and validation including Safety Function Response Time and SIL (Safety Integrity Level) calculations.

3 FAILOVER CONCEPT IMPLEMENTATION

When designing a machine with safety control, risk analysis must be done in accordance to relevant international functional safety standards, e.g., those listed in the European Union Machinery Directive 2006/42/EC. In addition to risk reduction, uphold production steps, like implementation of the failover concept, is much recommended.

As described in the example with AGV, if hazards cannot be detected due to malfunction (e.g. communication error) of the safety laser scanner or the remote safety camera, it would cause the activation of the emergency stop. After the emergency stop, the system must undergo error diagnostics, recovery and then shall be restarted. The average time period for the process to be restarted after the emergency stop can vary from 5 minutes to 1 hour and more, in practice. However, in case of temporary unavailability of the device and if the device’s function recovers after an acceptable time period (not compromising Safety Function Response Time) without the need to manually repair and to restart the system, one can bridge this time period by using redundant devices and/or functions using proper implementation in the Safety PLC program.

A redundant safety device or function usually also means initial costs (at least additional programming efforts, verification and validation), which at times is not well appreciated in the industry, if the benefits are not significant enough. However, with failover control as mentioned above in the AGVs case, even existing redundancies in system design can be used. For example, the protection area of the safety laser scanner can be also partially covered by the remote safety camera. It means if the safety laser scanner fails temporary due to a communication error, the function of the safety laser scanner can be covered by the remote safety camera. As a result, during the unavailability of the safety laser scanner, any valid hazard detection in the zone observed by the remote safety camera will cause a safe stop instead of the safety limited speed, because the safety laser scanner detection is temporary not available at this point of time.

This behavior shall be pre-programmed in the safety application using, for example, ST (Structured Text) for safety programming (FBD and LAD can be used as well). ST provides better readable safety applications and application specific safety PLC libraries which save safety programming costs (faster safety program development) and improves safety program readability resulting in less programming mistakes. To realize such scenario, the remote safety camera has to fulfill at least the same SIL level as the safety laser scanner. As a result of such implementation, the machine could run at 100% efficiency, if no safety zone violation is detected. Thus, if the remote safety camera is not working, the safety control remains intact with the reconfiguration of reaction in the remote safety camera zone from the safely limited speed to the safe stop. The productivity is lower than with the safety laser scanner working, because each time the remote safety camera is triggered in such case, the machine safely stops instead of initiating safely limited speed function, but the overall productivity is still higher compared to always stopping the machine, if the safety laser scanner is not working.

In case the remote safety camera is not available, the situation is slightly different because its zone is only partially covered by the detection means of the safety laser scanner and, thus, the safety laser scanner cannot be used as the failover device for the remote safety camera. However, we can use safely limited speed as the failover function for the unavailability (malfunction) of the remote safety camera in combination with continuously working safety laser scanner. It means that each time the remote safety camera temporary malfunctions, safely limited speed can be activated instead of direct safe stop. Using Safety PLCs with its trigonometric function and safety sensors for safe position and speed detection, one can also safely calculate the position of the AGV to differentiate between various scenarios in failover concept implementation.

Timers in the safety application program shall be started to supervise the temporary unavailability of the safety laser scanner and the remote safety camera or any other safety devices used in accordance with the pre-defined Safety Function Response Time for the given application.

In case of PROFIsafe technology, F-Host (Master) instance on Safety CPU (Central Processing Unit) is available for each PROFIsafe device. As a result, for each PROFIsafe device one can read in the safety application program the following additional PROFIsafe device status:

- *FV_activated_S*: With PROFIsafe input devices this variable indicates if TRUE that the PROFIsafe driver is delivering fail-safe values "0" to the PROFIsafe F-Host (Master) program for every input value.
- *WD_timeout*: It is set to TRUE if the PROFIsafe device is recognizing a communication failure, i.e. if the watchdog time in the PROFIsafe device is exceeded.
- *CE_CRC*: It is set to TRUE if the PROFIsafe device is recognizing a communication failure, i.e. if the consecutive number is wrong or the data integrity is violated (CRC error).
- *Device_Fault*: This parameter is set to TRUE if there is a malfunction in the PROFIsafe device (e.g., under- or overvoltage).
- *Host_CE_CRC*: This parameter is set to TRUE if the communication fault (CRC error on F-Host side) occurs.
- *HostTimeout*: This parameter is set to TRUE if the communication fault (Timeout on PROFIsafe F-Host side) occurs.

These PROFIsafe device statuses can be used in the safety application for safe evaluation of PROFIsafe device state and, thus, make decisions for various pre-defined failover approaches with safe time supervision using timers in the safety application.

In two sample scenarios, we will have a closer look at temporary watchdog and CRC communication errors and their potential handling in failover concept. We assume that the safety laser scanner (see previous example with AGV) is connected remotely via PROFINET/PROFIsafe to the Safety PLC and, thus, temporary communication errors like CRC or Watchdog errors could lead to an emergency stop of the system, if there is no implementation of failover concept.

Let’s take a closer look at the CRC errors, which are typical examples for temporary failures of the communication to the safety device. CRC errors can be detected by the Safety PLC using safety telegram checksum calculation. At present, an occasional single CRC error on the safety layer would cause an emergency stop in a number of safety protocols (e.g., PROFIsafe), if no additional measure is implemented to deal with this situation at the application level. But in many cases, CRC errors disappear after a short time period, and a stable communication with the device is re-established again. In such situation, if failover concept is implemented, the system need not to be stopped with a single CRC error (since there is a redundant safety device) and can recover itself automatically by switching back to the normal safety functions, when the next telegram becomes valid. Multiple CRC errors within a defined time interval can be interpreted as a serious failure, wherein the machine must be stopped. The commonly applied time interval for multiple CRC error detection is currently 100 hours for PROFIsafe V2.4.

The result of CRC check is available in the safety application of the Safety CPU for the given PROFIsafe device using related PROFIsafe F-Host (Master) program instance with Host_CE_CRC and CE_CRC outputs. Therefore, the safety application on the Safety CPU can detect the communication failure and interpret it as a malfunction of the particular safety device or communication channel. One can use timers in the safety program to measure the duration of safety device failure. Of course, in case of permanent failure of safety device, the automatic recovery is not possible. The safety devices shall be replaced or the problem causing safety device malfunction is eliminated. Afterwards, the safety application can be restarted.

Another typical example for temporary communication errors are watchdog errors. These errors can happen every minute or even more often in practice, depending on the parameters used. The watchdog time defines the compromise between SFRT (Safety Function Response Time) and availability. The smaller the watchdog time is higher is the probability that one may have to stop the machine due to “Black channel” sudden performance deficiency.

Presently, there is no limitation on the occurrence frequency of the watchdog error, but the machine would stop each time if we do not implement the failover concept. In case of communication error with actuators, the failover concept cannot be applied, because the safety logic would not be able to ensure appropriate safety functions on the corresponding actuator.

AGVs are very often connected through WLAN (Wireless Local Area Network) and controlled from a central location. Imagine that WLAN is suddenly too slow (disturbance or blocking wall due to bad environment for data transfer, etc.). AGV control system loses communication to central station and gets watchdog error because communication via WLAN is too slow. One could instead of stopping the AGV in case of watchdog error, start a timer. If within, e.g. 3 second the communication is not back and running, the AGV is stopped. Otherwise, it goes to safely limited speed mode and uses local safety sensors (e.g. the safety laser scanner, as it is in an example with AGV) as failover devices.

4 PRODUCTIVITY ENHANCEMENTS

To calculate the productivity enhancement from failover concept, we used the following practical example of CRC errors. CRC error may occur in a safety communication network 1 per year with a single-shift operation for 300 days (2400 hours) and safety communication cycle of 30 ms. Assume that the average downtime due to an emergency stop including restart operation is 15 minutes. This means that we may have 15 minutes of downtime per year due to temporary CRC errors. As a result, the implementation of the failover concept can prevent 15 minutes of downtime per year. According to some surveys, one minute of machine downtime costs an average of 20000 $. This means that the implementation of the failover concept can save 300000 $ per year. If we take into account also the required design efforts for the failover concept in the production facility as ~100000 $, the customer would still benefit with cost savings of 200000 $ in the first year and 300000 $ per year in the following years.

In a safety network with wireless communication (and therefore relatively high variations in response time) we can assume the frequency of the watchdog errors to be 10 per year and the average downtime due to an emergency stop including restart operation is 5 minutes. There is a single-shift operation for 300 days (2400 hours). This means that we may have 50 minutes of downtime per year due to the temporary watchdog errors. The potential savings in such application are 1 M$ per year. In this case, additional design efforts estimated to be ~100000 $ for the failover concept implementation are significantly smaller than potential savings which would be 900000 $ already in the first year and 1 M$ per year in the following years.

5 CUSTOMER CASE

A good customer case for failover concept implementation is a production of MCB (Miniature Circuit Breakers) at ABB STOTZ-KONTAKT in Heidelberg, Germany. This highly automated production line for a certain number of MCB variants is running 24 hours / 6 days a week. The production frequency is higher than one MCB per second.

The total production line is divided into five parts:

- Assembly of MCBs
- Test area
- Intermediate stock
- Finalizing
- Packaging.

An uninterrupted production flow of all production line parts is crucial for the production efficiency.

Two robotized cells in ABB STOTZ-KONTAKT production line are suitable examples for the failover concept implementation:

- Robot cell for thermal short-time measurement of MCBs (Miniature Circuit Breaker) (see Figure 3)
- Robot cell with handling of MCB poles in the storage (see Figure 4)

In the current implementation, the robots in both cells are stopped if safety sensors (laser scanner or safety door, respectively) are triggered.

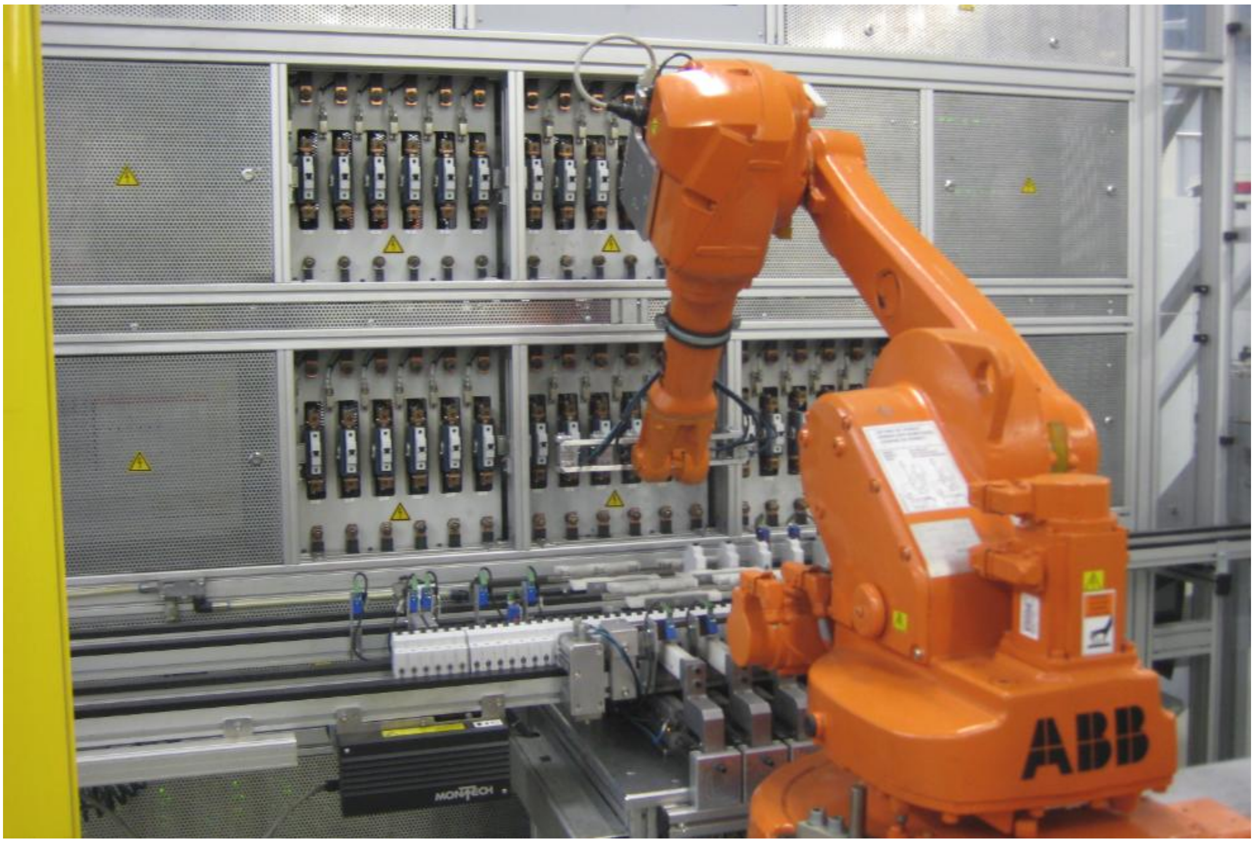

Figure 3: Robot cell for thermal short-time measurement of MCBs at ABB STOTZ-KONTAKT production facility in Heidelberg, Germany

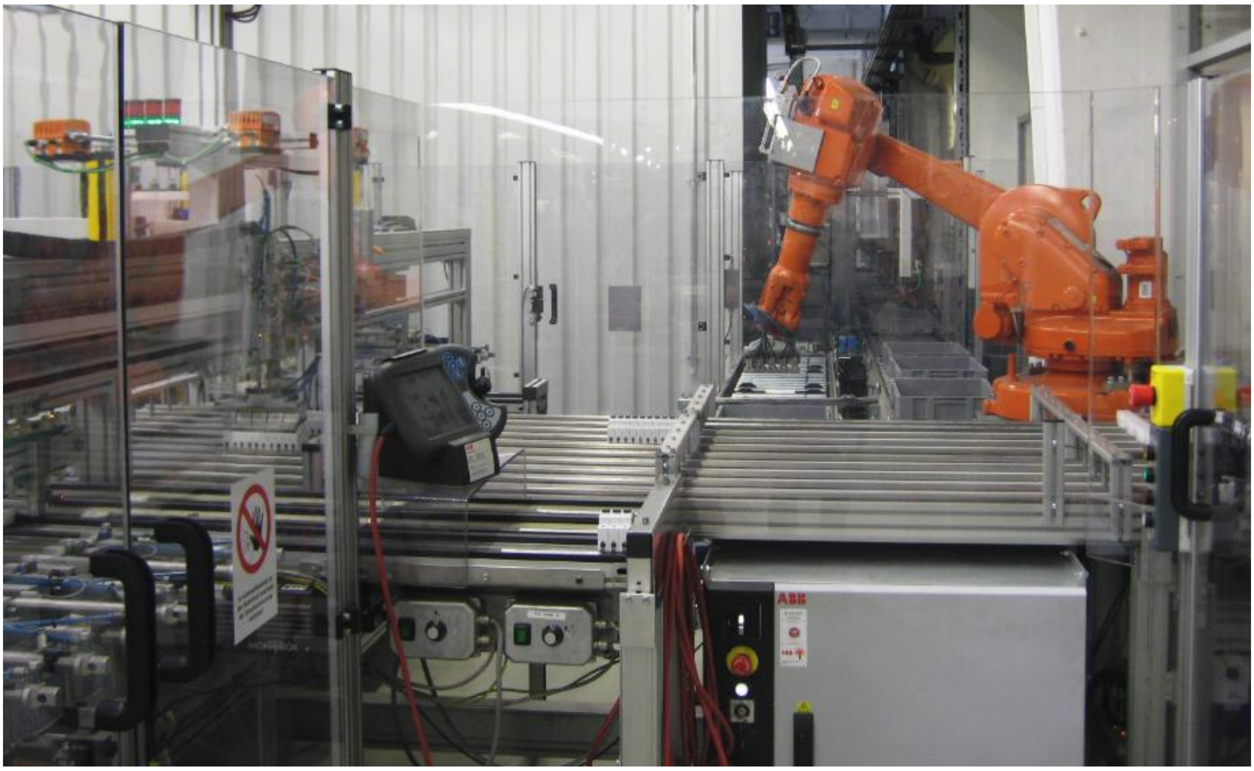

Figure 4: Robot cell with handling of MCB poles in the storage at ABB STOTZ-KONTAKT production facility in Heidelberg, Germany

After failover concept implementation in the re-design phase, less downtime due to temporary unavailability of safety sensors will be detected, because the differentiation between real triggering of safety functions and malfunction/unavailability of the safety device due temporary communication errors, undervoltage, etc. at the safety application level is available.

6 CONCLUSIONS

Safety reaction to hazard events often lead to machine stops with remarkable downtime of machines. These are usually triggered by safety devices that detect hazard events, or when safety devices become unavailable. The implementation of the failover concept can enhance the productivity of machines and manufacturing systems significantly so that the number of machine stops can be minimized, or even the stops can be avoided in many cases for temporary errors like communication errors (CRC or watchdog). If the analysis of hazards takes this fact into consideration, the safety functions and the overall safety control of the machine or manufacturing system can be designed in such a way that it maximizes the productivity.

The increase of productivity can be estimated based on anticipated frequency of hazard events and temporary errors, average duration of downtime due to such events, etc. It is then possible to judge whether the cost and effort of implementing the failover concept pays off. In the examples cited before, we have shown that significant cost savings are achieved (in the order of 100000 $ or more per year) due to less machine interruption resulting in increased productivity.

Nevertheless, the steps for designing functional safety defined in the international standards are to be followed, and the safety function design including the selection of safety devices must take all relevant combinations of subsystems into consideration. We recommend taking availability and productivity into considerations while doing risk assessment and designing functional safety.

The implementation of failover safety concept is made easy and efficient using Safety PLCs with the feature that could distinguish the real safety trigger from safety device malfunctions caused by temporary communication errors, undervoltage, etc.

Power and productivity
for a better world™