II. Task Description

Thomas Lindner

Forschungszentrum Informatik, Karlsruhe

Abstract

This chapter presents a case study in the field of control systems. The task consists of developing verified control software for a model representing a production cell installed in a metal-processing plant in Karlsruhe. The paper describes the functionality of the model, explains how the control program relies on the system's sensors, discusses the possibilities for driving the model with the help of various actuators, and finally defines the requirements that are to be fulfilled by the control software.

2.1 Description of the Production Cell

The Forschungszentrum Informatik has created a model of a production cell for mounting frames which was built as part of a study in microcomputer technology in 1989. This is not a model only in theory: it represents an actual industrial installation in a metal-processing plant in Karlsruhe.

The case study presents a realistic industry-oriented problem, where safety requirements play a significant role and can be met by the application of formal methods. The manageable size of the task allows for experimenting with several approaches.

The production cell processes metal blanks which are conveyed to a press by a feed belt. A robot takes each blank from the feed belt and places it into the press. The robot arm withdraws from the press, the press processes the metal blank and

opens again. Finally, the robot takes the forged metal plate out of the press and puts it on a deposit belt (see figure 1).

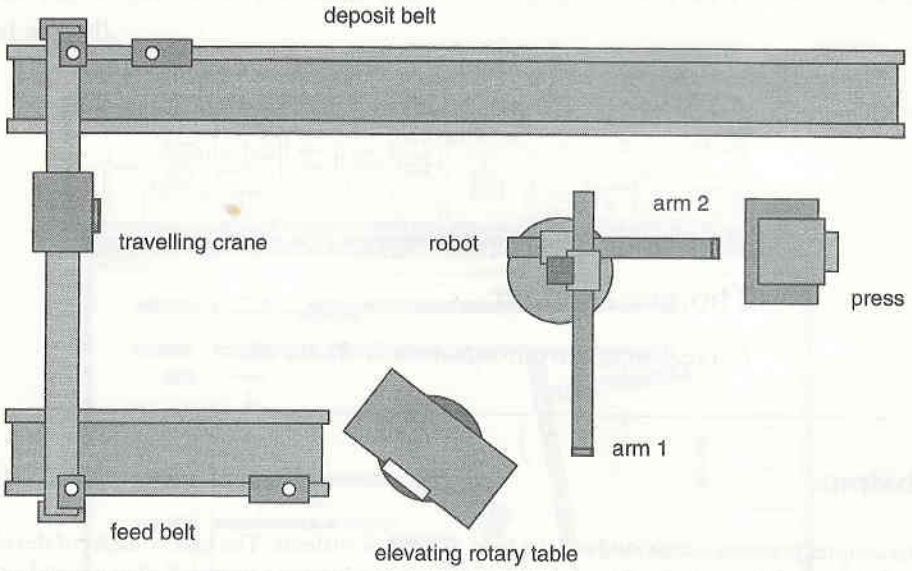

Figure 1 Top view of the model

This basic sequence is complicated by further details:

- To enhance the utilization of the press, the robot is fitted with two arms — thus making it possible for the first arm to pick up a blank while the press is forging another plate.
- The robot arms are placed on different horizontal planes, and they are not vertically mobile. This explains why an elevating rotary table has to be intercalated between the feed belt and the robot.
- Another consequence of the fact that the two robot arms are at different levels, is that the press has not only two, but three states: open for unloading by the lower arm, open for loading by the upper arm, and closed (pressing).
- In order to perform demonstrations with the model, the production sequence should be able to run without an operator. The "forged" metal plates — which the press in the model does not actually modify — are therefore taken from the deposit belt back to the feed belt by a travelling crane, thus making the entire sequence cyclical.

- A photoelectric cell at the end of the deposit belt informs the control program about the arrival of metal plates to be picked up by the travelling crane.

The general sequence (from the perspective of a metal plate) is the following:

1. The feed belt conveys the metal plate to the elevating rotary table.
2. The elevating rotary table is moved to a position adequate for unloading by the first robot arm.
3. The first robot arm picks up the metal plate.
4. The robot rotates counterclockwise so that arm 1 points to the open press, places the metal plate into it and then withdraws from the press.
5. The press forges the metal blank and opens again.
6. The robot retrieves the metal plate with its second arm, rotates further and unloads the plate on the deposit belt.
7. The deposit belt transports the plate to the travelling crane.
8. The travelling crane picks up the metal plate, moves to the feed belt, and unloads the metal plate on it.

This description of the system is of course rather simplified. First, the individual system components are not specified in detail. Secondly, the cell is configured so that several metal plates can be processed and transported simultaneously; this should allow an optimal utilization of the cell capacity.

2.1.1 Feed Belt

The task of the feed belt consists in transporting metal blanks to the elevating rotary table. The belt is powered by an electric motor, which can be started up or stopped by the control program. A photoelectric cell is installed at the end of the belt; it indicates whether a blank has entered or left the final part of the belt.

2.1.2 Elevating Rotary Table

The task of the elevating rotary table is to rotate the blanks by about 45 degrees and to lift them to a level where they can be picked up by the first robot arm. The vertical movement is necessary because the robot arm is located at a different level than the feed belt and because it cannot perform vertical translations. The rotation of the table is also required, because the arm's gripper is not rotary and is therefore unable to place the metal plates into the press in a straight position by itself.

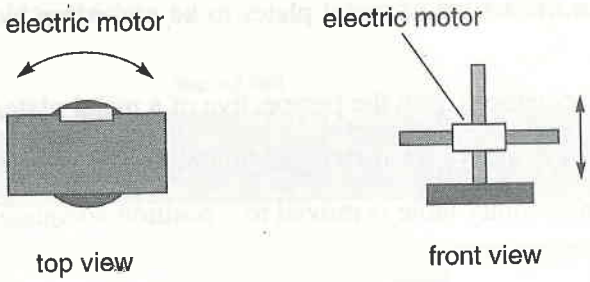

Figure 2 Elevating rotary table

2.1.3 Robot

The robot comprises two orthogonal arms. For technical reasons, the arms are set at two different levels. Each arm can retract or extend horizontally. Both arms rotate jointly. Mobility on the horizontal plane is necessary, since elevating rotary table, press, and deposit belt are all placed at different distances from the robot's turning center.

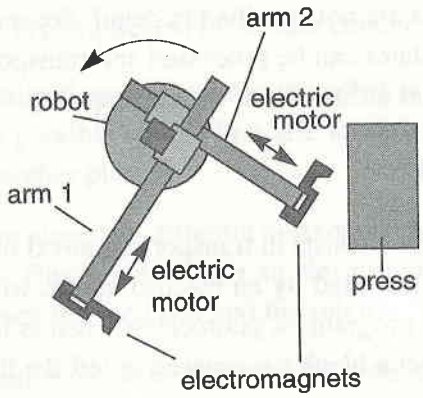

Figure 3 Robot and press (top view)

The end of each robot arm is fitted with an electromagnet that allows the arm to pick up metal plates. The robot's task consists in:

- taking metal blanks from the elevating rotary table to the press;
- transporting forged plates from the press to the deposit belt.

The robot is fitted with two arms so that the press can be used to maximum capacity. Below, we describe the order of the rotation operations the robot arm has to perform, supposed the feed belt to delivers blanks frequently enough. We presuppose that initially the robot is rotated such that arm 1 points towards the elevating rotary table, and assume that all arms are retracted to allow safe rotation.

1. Arm 1 extends and picks up a metal blank from the elevating rotary table.
2. The robot rotates counterclockwise until arm 2 points towards the press. Arm 2 is extended until it reaches the press. Arm 2 picks up a forged work piece and retracts.
3. The robot rotates counterclockwise until arm 2 points towards the deposit belt. Arm 2 extends and places the forged metal plate on the deposit belt.
4. The robot rotates counterclockwise until arm 1 can reach the press. Arm 1 extends, deposits the blank in the press, and retracts again.

Finally, the robot rotates clockwise towards its original position, and the cycle starts again with 1.

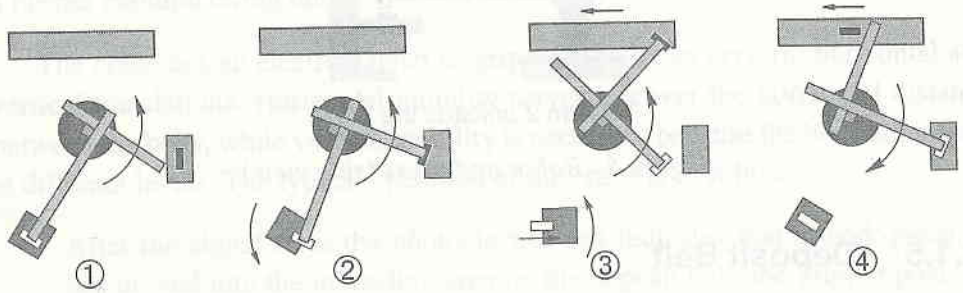

Figure 4 Order of the robot's actions

In order to meet the various safety requirements described in section 2.3, a robot arm must retract whenever a processing step where it is involved is completed.

2.1.4 Press

The task of the press is to forge metal blanks. The press consists of two horizontal plates, with the lower plate being movable along a vertical axis. The press operates by pressing the lower plate against the upper plate. Because the robot arms are placed on different horizontal planes, the press has three positions. In the lower position, the press is unloaded by arm 2, while in the middle position it is loaded by arm 1. The operation of the press is coordinated with the robot arms as follows:

1. Open the press in its lower position and wait until arm 2 has retrieved the metal plate and left the press.
2. Move the lower plate to the middle position and wait until arm 1 has loaded and left the press.
3. Close the press, i.e. forge the metal plate.

This processing sequence is carried out cyclically.

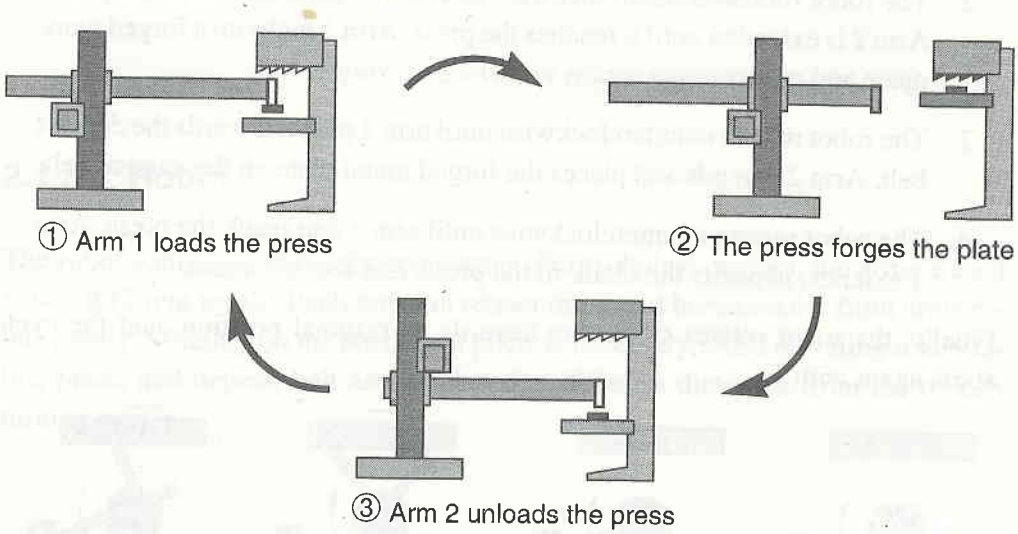

Figure 5 Robot and press (side view)

2.1.5 Deposit Belt

The task of the deposit belt is to transport the work pieces unloaded by the second robot arm to the travelling crane. A photoelectric cell is installed at the end of the belt; it reports when a work piece reaches the end section of the belt. The control program then has to stop the belt. The belt can restart as soon as the travelling crane has picked up the work piece.

The system designer is free to decide if the belts are to run continuously and should be stopped only when necessary, or if they should stand still and move only when necessary.

2.1.6 Travelling Crane

The task of the travelling crane consists in picking up metal plates from the deposit belt, moving them to the feed belt and unloading them there. It acts as a link be-

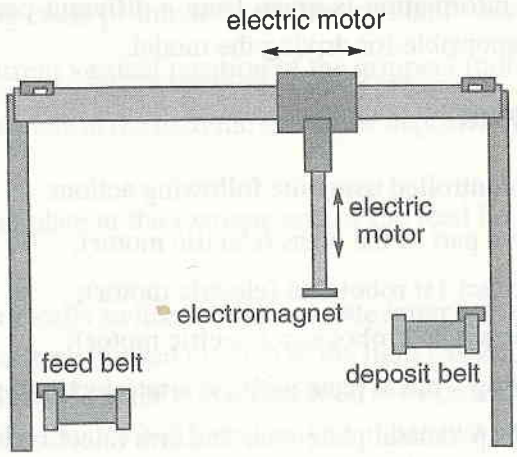

Figure 6 Travelling crane

tween the two belts that makes it possible to let the model function continuously, without the need for an external operator. In a more realistic setting, the travelling crane could unload the metal plates into a container, or link the production cell to a further manufacturing unit.

The crane has an electromagnet as gripper which can perform horizontal and vertical translations. Horizontal mobility serves to cover the horizontal distance between the belts, while vertical mobility is necessary because the belts are placed at different levels. The typical operation of the crane is as follows:

1. After the signal from the photoelectric cell indicates that a work-piece has moved into the unloading area on the deposit belt, the gripper positions itself through horizontal and vertical translations over the deposit belt and picks up the metal plate.
2. The gripper transports the metal plate to the feed belt and unloads it there.

Efficiency considerations may lead a system designer to move the travelling crane back to the deposit belt at the end of this sequence so that incoming plates can be transported immediately.

2.2 Actuators and Sensors

In the previous section, the system and its operation have been described from an "object-oriented" perspective — in the broadest possible sense of the term. In this

section, additional information is given from a different perspective, that of the control program responsible for driving the model.

2.2.1 Actuators

The system can be controlled using the following actions:

1. move the lower part of the press (electric motor);
2. extend and retract 1st robot arm (electric motor);
3. extend and retract 2nd robot arm (electric motor);
4. pick up and drop a metal plate with 1st arm (electromagnet);
5. pick up and drop a metal plate with 2nd arm (electromagnet);
6. rotate robot (electric motor);
7. rotate elevating rotary table (electric motor);
8. move elevating rotary table vertically (electric motor);
9. move gripper of travelling crane horizontally (electric motor);
10. move gripper of travelling crane vertically (electric motor);
11. pick up and drop a metal plate with gripper of travelling crane (electromagnet);
12. activate and deactivate feed belt (electric motor);
13. activate and deactivate deposit belt (electric motor).

2.2.2 Sensors

The control program receives information from the sensors as follows:

1. Is the press in its lower position? (switch)
2. Is the press in its middle position? (switch)
3. Is the press in its upper position? (switch)
4. How far has 1st arm been extended? (potentiometer)
5. How far has 2nd arm been extended? (potentiometer)
6. How far has the robot rotated? (potentiometer)
7. Is the elevating rotary table in its lower position? (switch)
8. Is the elevating rotary table in its upper position? (switch)
9. How far has the table rotated? (potentiometer)
10. Is the travelling crane positioned over the deposit belt? (switch)

11. Is the travelling crane positioned over the feed belt? (switch)
12. What is the current vertical position of the gripper? (potentiometer)
13. Is there a metal plate at the extreme end of the deposit belt? (photoelectric cell)
14. Is there a metal plate at the extreme end of the feed belt? (photoelectric cell)

Both photoelectric cells switch on when a plate intercepts the light ray. Just after the plate has completely passed through it, the light barrier switches off. At this precise moment, the plate is in the correct position to be picked up by the travelling crane (sensor 13 of the deposit belt), respectively it has just left the belt to land on the elevating rotary table — provided of course that the latter machine is correctly positioned — (sensor 14 of the feed belt).

While light barriers and switches provide a go/no-go kind of information, the potentiometer returns a value — which, in the case of rotation for instance, is proportional to the angle.

2.3 Requirements

In a reactive system, one typically distinguishes between safety and liveness requirements. Obviously, the safety requirements are most important in this setting: if a safety requirement is violated, this might result in damage of machines, or, even worse, injury of people. The safety requirements are described in section 2.3.1, liveness properties are discussed in section 2.3.2, and the last section discusses other properties interesting in this context.

The requirements listed below should be viewed as a pool of ideas. This case study allows for evaluating methods and approaches according to a wide spectrum of requirements, but not all properties can be formally proved to hold. We encourage contributors to prove representants of the single classes of properties, or discuss whether or how certain kinds of properties can be expressed or verified using the method under consideration.

2.3.1 Safety requirements

The control program must make sure that various safety requirements are met. Each safety requirement is a consequence of one of the following principles:

- the limitations of machine mobility: the robot, for instance, would destroy itself if rotated too far; the press would damage itself if opened too far;
- the avoidance of machine collisions: the robot, for instance, would collide with the press arm 1 would extend too far while pointing towards the press;
- the demand to keep metal blanks from being dropped outside safe regions: the robot, for instance, may deposit blanks only at some, few places, the feed belt has to make sure that the table is in the right position before transporting the blank too far;
- the necessity to keep the metal blanks sufficiently seperate: light barriers, for instance, can distinguish two consecutive blanks only, if they have a sufficient distance.

✔ Restrict machine mobility!

The electric motors associated with the actuators 1-3 and 6-10 (cf. section 2.2.1) may not be used to move the corresponding devices further than necessary. In detail:

- the robot must not be rotated clockwise, if arm 1 points towards the elevating rotary table, and it must not be rotated counterclockwise, if arm 1 points towards the press,
- both arms of the robot must not be retracted less than necessary for passing the press, and they must not be extended more than necessary for picking up blanks from the press,
- the press must not be moved downward, if sensor 1 is true, and it must not be moved upward, if sensor 3 is true,
- the elevating rotary table must not be moved downward, if sensor 7 is true, and it must not be moved upward, if sensor 8 is true,
- the elevating rotary table must not be rotated clockwise, if it is in the position required for transfering blanks to the robot, and it must not be rotated counterclockwise, if it is in the position to receive blanks from the feed belt,
- if the crane is positioned above the feed belt, it may only move towards the deposit belt, and if it is positioned above the deposit belt, it may only move towards the feed belt,

- the gripper of the crane must not be moved downward, if it is in the position required for picking up a work piece from the deposit belt, and it must not be moved upward beyond a certain limit.

To fulfil these restrictions, the certain constants must be known. We refer to Appendix A.

✓ Avoid machine collisions!

A couple of possible collisions are already avoided by simply obeying the above-mentioned restrictions on machine mobility. We do not mention these collisions in the following. Additionally, collision is possible and has to be avoided between the press and the robot, and between the crane and the feed belt:

- the press may only close when no robot arm is positioned inside it,
- a robot arm may only rotate in the proximity of the press if the arm is retracted or if the press is in its upper or lower position,
- the travelling crane is not allowed to knock against a belt laterally (this would happen if the travelling crane moved from the deposit belt to the feed belt without a simultaneous vertical translation),
- the travelling crane must not knock against a belt from above.

Again, we refer to Appendix A for the corresponding constants.

✓ Do not drop metal blanks outside safe areas!

Metal blanks can be dropped for two reasons:

- the electromagnets of the robot arms or the crane are deactivated,
- a belt transports work pieces too far.

To avoid this, it suffices to obey the following rules:

- the magnet of arm 1 may only be deactivated, if the arm points towards the press and the arm is extended such that it reaches the press,
- the magnet of arm 2 may only be deactivated, if its magnet is above the deposit belt,
- the magnet of the crane may only be dactivated, if its magnet is above the feed belt and sufficiently close to it,
- the feed belt may only convey a blank through its light barrier, if the table is in loading position,
- the deposit belt must be stopped after a blank has passed the light barrier at its end and may only be started after the crane has picked up the blank.

Keep blanks sufficiently distant!

Errors occur if blanks are piled on each other, overlap, or even if they are too close for being distinguished by the light barriers. To avoid these errors, it suffices to obey the following rules:

- a new blank may only be put on the feed belt, if sensor 14 confirms that the last one has arrived at the end of the feed belt,
- a new blank may only be put on the deposit belt, if sensor 13 confirms that the last one has arrived at the end of the deposit belt,
- do not put blanks on the table, if it is already loaded,
- do not put blanks into the press, if it is already loaded
- do not move the loaded robot arm 1 above the loaded table, if the latter is in unloading position (otherwise the two blanks collide).

2.3.2 Liveness properties

A very strong liveness property for this system is satisfied, if the following requirement is fulfilled:

Every blank introduced into the system via the feed belt will eventually be dropped by the crane on the feed belt again and will have been forged.

There are many weaker forms of this liveness requirement.

2.3.3 Other requirements

Efficiency. It might be required that no blank is longer than a certain amount of time in the production cell. The best result would be to prove that the implemented controller achieves minimum possible time. To prove these properties it is necessary to remove the crane from the part of the system where time is measured.

Additionally, it can be required that the controller takes care that there are never less than a certain number of work pieces in the system, provided that there are enough blanks available.

Flexibility. The control software has to be as flexible as possible. The effort for changing the control software and proving its correctness must be as small as possible, when the requirements or the configuration of the cell change.

Questions

Several contributors found it helpful to consider the following question during their work or while writing the documentation:

- Which properties have been proved?
- Have assumptions about the architecture or the behavior of the production cell been made explicit and are they documented?
- How long, how complicated is the description? Is it understandable without deep knowledge of the method? Can it be discussed with a potential customer?
- How much effort was spent? Is the cost-benefit ratio balanced?
- Is it easy to change the controller? Can proofs be reused, or does a change in one part of the cell invalidate all proofs?
- How efficient is the controller? Does it achieve maximum possible throughput?
- Is it possible to draw conclusions on how the hardware design of the production cell could be improved? Would it be easier to prove certain properties, if additional sensors would be added? Would it be easier to control the cell, if any other additional hardware would be provided?

Acknowledgements

The author thanks Eduardo Casais for various suggestions and for providing the production cell clip-art from which all figures are adapted. Several contributors detected various errors and inconsistencies in earlier versions of this case study. Finally, thanks are due to Jochen Burghardt, who found the classification of safety requirements presented in section 2.3.1.