Sofia University “St. Kliment Ohridski”
Faculty of Mathematics and Informatics

DISTRIBUTED CONTROL OF CONVEYER SYSTEMS

Synopsis
of the PhD Thesis
Conducted for the purpose of receiving the academic title
“Doctor of Philosophy”
(PhD) in the field of 4.6. Informatics and Computer Science

Submitted by: mag. eng. Ivailo Todorov Andonov
Advisor: assoc. prof. Simeon Emilov Tsvetanov, PhD

Sofia, 2021

Acknowledgments

I would like to express my biggest thanks to all those who supported me and contributed for the successful creation and completion of this thesis.

To my supervisor assoc. prof. Simeon Tsvetanov with high contribution to the shaping the thesis in scientific view and his initiative for the publications.

The company Industrial Software Co. and its president Dimitar Petrov for the opportunity and all supplied technology for doing experiments like conveyors, control modules, measurement tools etc.

Prof. Ivan Petrov for his notes and directions with scientific point of view and for the materials he supplied about the motorized rollers.

The academic staff of the Faculty of Mathematics and Informatics of Sofia University "St. Kliment Ohridski" who regularly reminded me about the important deadlines in a friendly manner and used constructive criticism to keep me going.

In addition, not on last place my brother and my family who were my support in hard moments and motivated me to finish this thesis.

Table of content

List of figures

Abstract

The main goal of the thesis is developing a solution for achieving a better efficiency in the conveyor systems by applying a new method for distributed control.

Provided solution considers the zones of the conveyor as software agents, which with their own behavior aim to achieve better product density over the line and high average transfer speed

New solution is provided that achieves the goals by using the information about the rotor position of the driving motors, the computational power of the zone's control modules, cameras with affordable price and the high speed of the communication network.

The aim is to gather all possible useful information from the controller and to use it as best as possible to get better efficiency of the conveyor.

The contributions of the dissertation are useful for companies engaged in engineering activities for the construction of systems including conveyors for automated warehouses, sorting centers, airports, shops, various manufacturing plants, etc., allowing them to reduce their total cost and make them more intelligent.

The thesis is prepared in four chapters.

The first chapter analyzes the subject area and ends with defining the goals and objectives of the dissertation.

The second one suggests a solution for distributed control while considering each zone as software agent, which with its own behavior is trying to make the global system parameters better. Some solutions for improvements of the power supply system, distance measurement and communication are provided.

The third chapter deals with the implementation of the suggested solutions and their system integration.

The last chapter is about testing and evaluation of the results of the system by doing experiments. It is divided on two parts where in the first the results of the separate units testing is shown and in the second one, the whole system integrating all the solutions is evaluated and verified.

I CHAPTER - INTRODUCTION

Nowadays conveyor systems play more and more important role in material handling automation found in many areas as manufacturing, goods sortation, automated stores, airports etc. The number of tasks that a conveyor is expected to do and their complexity are getting higher. Parallel to that the price of the conveyor components gets lower and the market gets bigger.

I.1 Types of conveyor systems

Depending on the driving source, one can group the conveyors into conveyors with a centralized drive unit Fig. 1 and into conveyors with a distributed drive Fig. 2 – usually motorized drive rollers (MDRs)

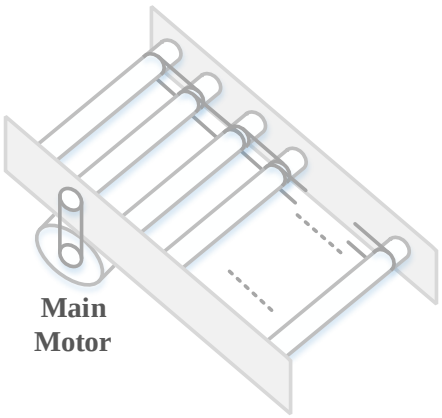

Fig. 1 Centralized drive

There are two main reasons for the zone-controlled conveyors to have a higher share in the conveyors market with a human access. First is safety. When a centralized drive unit is used, its power should be enough to drive all the conveyor line. This is usually many times the power of each drive unit in distributed zone controlled system. Injuries like smashing hands between moved products, hair or cloth winding around rotating part of the conveyor are much higher in a system with centralized drive.

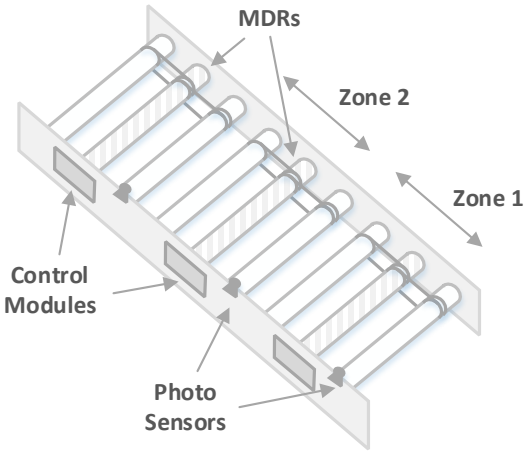

Fig. 2 Distributed drive

The second reason is efficiency. Moving only the rollers that need to transfer a product and keeping all others off gains higher power efficiency.

Usually the purpose of a conveyor is not only to transfer the load to its destination but also to make a buffer that allows storing some number of products before the accepting side is ready to accept them. This requires the zones to have some kind of autonomy and to receive information about the status of their upstream and downstream zones and to be capable of sensing the presence of a product above them using photo or magnetic sensor and sometimes using the value of their motor torque during the movement.

Compromise between the throughput and storage density gets harder when the loads length are very different from the zones length. Example where loads have high difference in their length are postal or courier services conveyors. Although there is an optimal zone's length, there will be loads with length occupying from few zones to a very small part of the zone Fig. 3.

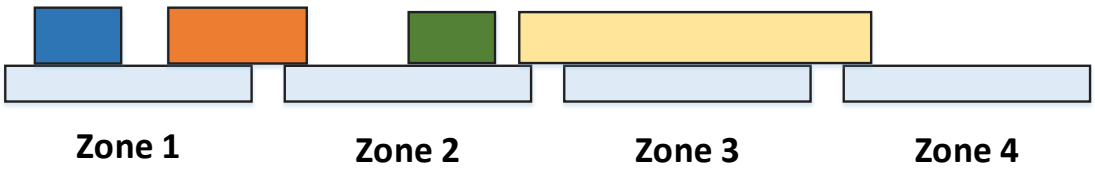

Fig. 3 Loads with length occupying from few zones to a very small part of the zone

I.2 Powering of the conveyer systems

Optimization of the cost of the conveyor components leads to the utilization of a much weaker power supply block on a conveyor than the sum of the nominal

power of all zones connected. The reason for that is the assumption that it is very rare to have all the zones accelerating a load and thus consuming their nominal power at exactly the same time Fig. 4. As a side effect in a scenario with a fully loaded conveyor with heavy loads a module under voltage or supply current trip lockouts may occur preventing the conveyor to work properly.

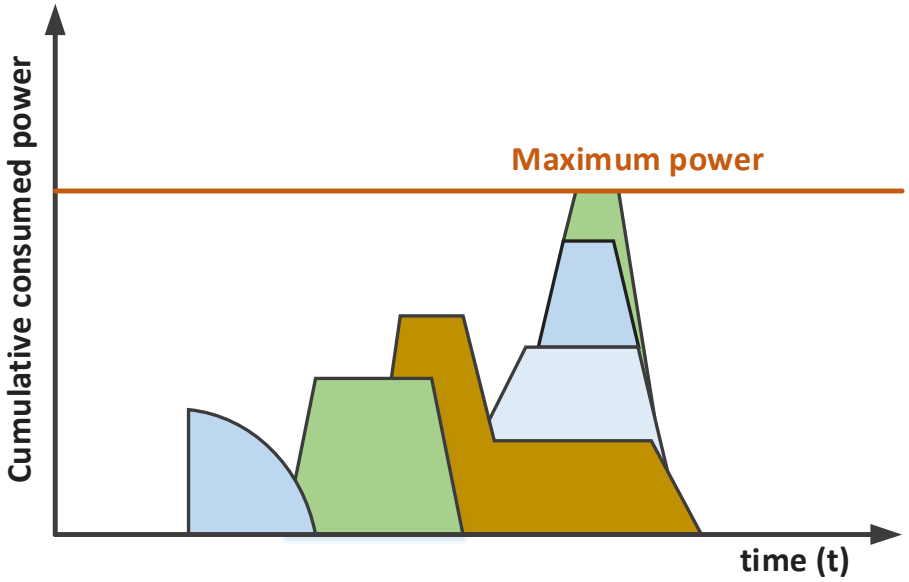

Fig. 4 Consumed energy during the time

Another issue in the conveyor systems is the returned energy during motor deceleration especially with heavy loads. The overvoltage protection of the power supply will trip if its voltage goes above some limit. Moreover, components can damage if that voltage goes above their limits. Since that behavior is not acceptable, control modules usually convert that excess energy to a heat inside, with the help of some compensation circuit (a circuit that dissipates heat over some components when it is necessary). Modules connected to the same power supply can avoid that inefficiency if they know how to exchange that energy between themselves.

I.3 Data reliability in noisy environment

In order to do a commutation of brushless DC motor an information from sensors that detect the rotor position is used.

Transmission of the data to the controller is sent either using some separate wires either with serial encoding over one wire. Nowadays the second method gains popularity because the cable diameter gets smaller. In both cases, though electromagnetic disturbances from the current commutation of the coils can lead to an error of the received information because they are strongly capacitively coupled.

I.4 Method for intellectual property protection of the controllers

Nowadays almost every part of our life is somehow dependent on computer systems. Security is a critical for computer systems usage and its importance increases with the continuously increasing number of connected devices.

The Internet of Things (IoT) ecosystem offers multiple levels of attack [1] and each of them has its own importance.

The risk of cloning the device is relatively small piece of the IoT security puzzle and it is often neglected, but is critical, because any vulnerable component can compromise the whole system.

A company that invests in developing of an IoT device usually tries to return the investment by selling that device.

Since the costs of manufacturing without the research and development (R&D) costs are much lower, often a competitor company tries to copy the product. Because of the R&D costs reduction, the copied product can be provided at much lower price.

The competitors use reverse engineering methods in order to read the firmware and start manufacturing a copy of that device. In this case, there is no investment in R&D, but in the reverse engineering. So if the original developer makes the design in such a way that the investment for reverse engineering is equal or even more that investing in a new design, coping the device become unreasonable and that risk is significantly reduced.

Patenting the device in order to protect its design and other security regulations are outside the scope of this paper.

In general any product or system can be hacked, but such goal becomes unreasonable if requires too much effort and investment.

I.5 Artificial intelligence

Computer programs are getting more and more intelligent and they are capable of taking own decisions which is related to the term software agents.

Software agents have their own goals, achieve them autonomously by interaction with the environment

Generally speaking software agents are autonomous and do things autonomously. The have a broad application in collecting an information to be used for taking some decisions.

There are many types of network agents with doing many functions for example searching for security violations, fault finding etc.

The term artificial intelligence is related to the intelligent behavior. In contrast to the human intellect, though this one deals with an artificial matter like computer programs.

In the case of conveyor systems where the average quantity of objects passing for a period of time , the total number of objects on a particular part of the line, the ratio between the quantity entering and the quantity leaving the conveyor for a period of time are values usually with some periodicity in time. Appropriate for modeling of such a values are neural networks of type Long Short-Term Memory.

I.6 Computer simulations

Appropriate for computer simulations are software products working in a discrete time based on events from the simulated process like FlexSim and SimCAD etc. The first is better because it offers user-friendly interface and because it is very easy to create a model Fig. 5.

The software offers a 3D visualization of the simulated process and it is easy to change the time scale for the simulation. For example, a process that takes hours can be simulated and overlooked for seconds.

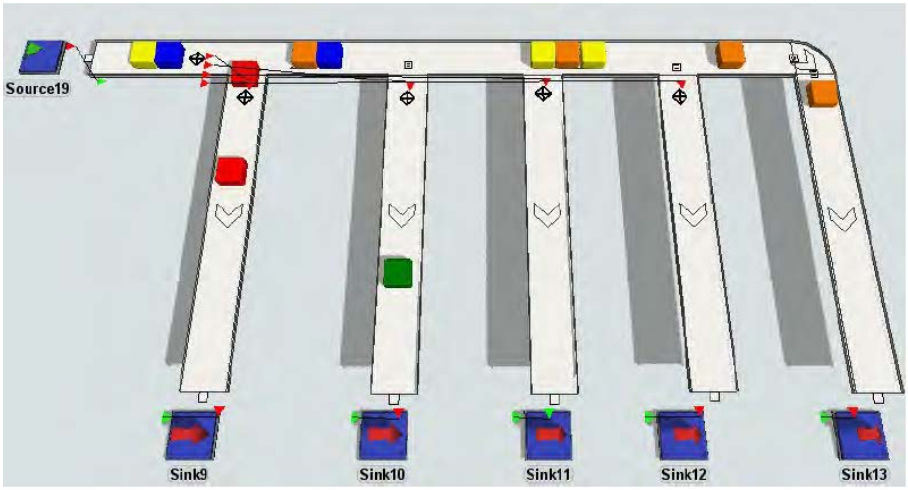

Fig. 5 Simulation of a distribution center

II CHAPTER - ADDING INTELLIGENCE TO THE CONVEYER SYSTEMS

In this chapter, some solutions for obtaining a better performance of the conveyor systems are suggested by adding an intelligence where each zone is considered as standalone agent solving a piece of the common task in order to achieve the goal.

II.1 Enhancing the efficiency by using distributed control of the conveyer

An intelligent way of a zone control can be developed to account for longer and shorter loads. Distributed algorithm can try to accumulate as much loads as possible over the conveyor while keeping the throughput high. In order to do that a communication between the zones and information about the distance that the motor moved (load traveled) is required.

Upon receiving a load from upstream the zone can capture its movement distance value as c_1.When its sensor signal appears it captures again the counter as c_2. There is some distance between the photo sensor of the upstream zone and its end x_a and some distance between the current zone photo sensor and its end x_b. So (1) one can deduce that the current zone length z_b is:

$$z_b = c_2 - c_1 + x_b - x_a \tag{1}$$

Fig. 6 shows this graphically. Usually all the zones of the linear part of the conveyor are the same so one can assume that the distances between the zone sensor and their ends x are equal (2) and (3):

$$x_a = x_b = x \tag{2}$$

$$z_b = c_2 - c_1 \tag{3}$$

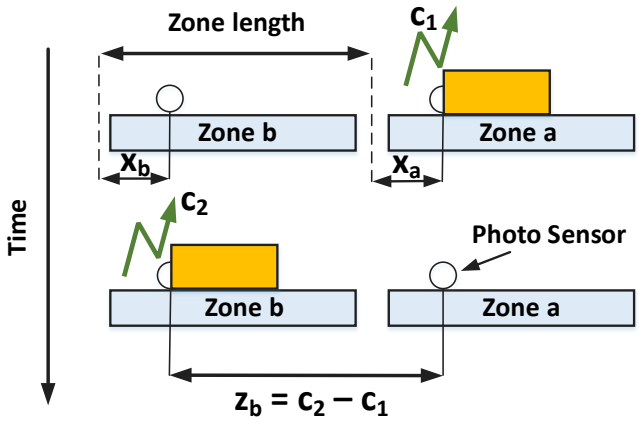

Fig. 6 Each zone maintains three lists with the loads

A zone can measure the load length from the distance it moved between the events when the load appeared on its sensor c_2 and when it disappeared c_3 (4).

$$l_b = c_3 - c_2 \quad (4)$$

The opposite measure between the disappearing c_3 and appearing c_4 events is a measure for the gap between the load just passed and the one that is coming (5).

$$g_b = c_4 - c_3 \quad (5)$$

On Fig. 7 a basic idea is shown where each zone maintains three lists with the loads that are currently accepted (list length is zero or 1), currently moving over the zone (list length from 0 to some limit 10 for example), and loads currently passed to the next zone (list length 0 or 1).

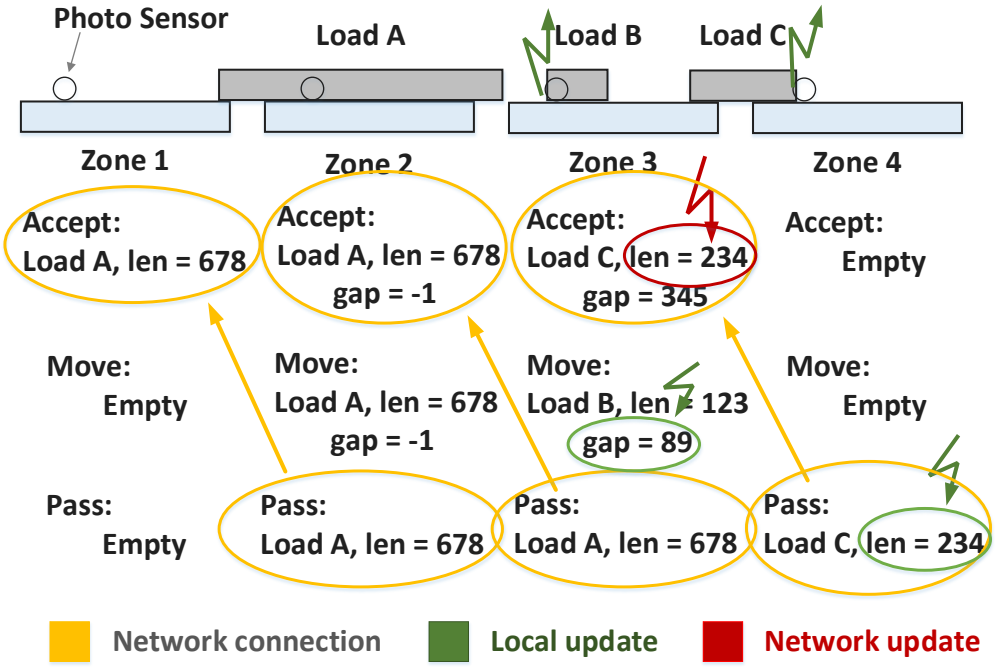

Fig. 7 Each zone maintains three lists with the loads.

The events from the photo sensors trigger an updates in the measured values of the gap and the load length in zones 3 and 4. Zone 4 load length's change in turn triggers a network update for zone 3.

If the zone has the knowledge about the loads lengths, its length and the load's gap length it can dynamically lengthen or shorten the gaps between the loads favoring better throughput or better density.

The zone can easily determine whether it is the end or the beginning of the linear part of the conveyor if the information exchanged between them contains information about its functionality.

For each load an information is gathered about how many loads are waiting to be discharged between it and at the end of the linear part of the conveyor and

how many loads are currently accepted between it and the beginning of the linear part. Based on those numbers the desired trailing gap is calculated so that the higher the number of the downstream waiting loads the lower the gap gets. This computation is distributive performed from each zone and can give linear or other dependence of the gap size in relation to distance along the conveyor. There is a preconfigured minimal gap size for the computation in order for the photo sensors to distinguish between the different loads. A preconfigured maximum number of loads above which the gap is always the minimum one gives an opportunity for increasing the storage density.

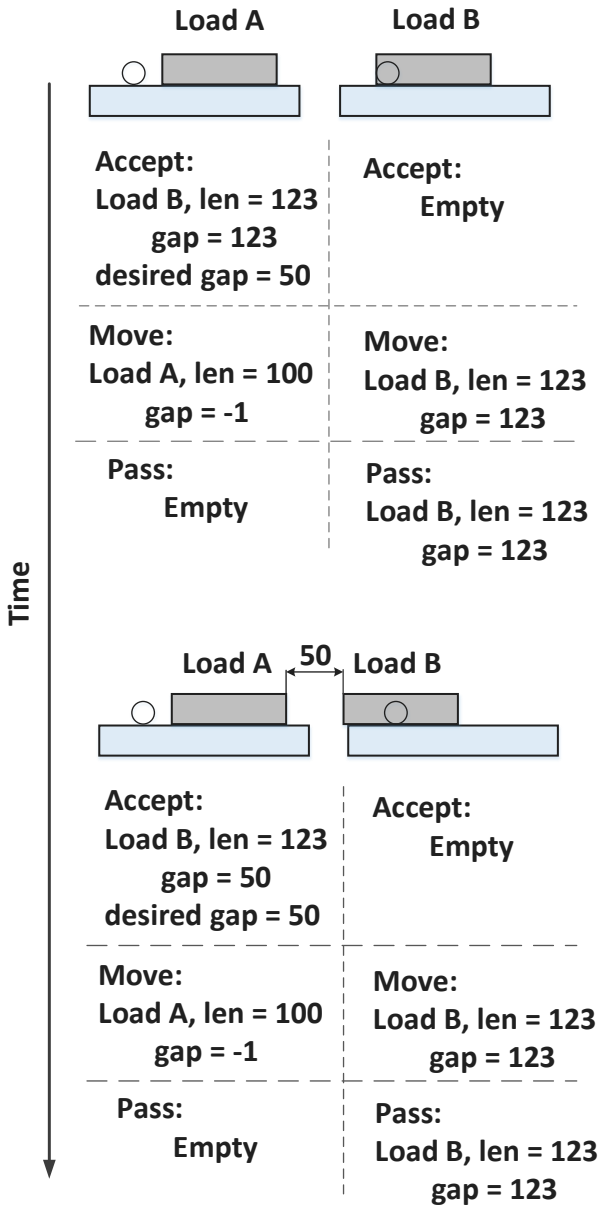

Fig. 8 Shortening the gap during acceptance.

When a zone finds that the desired calculated gap is lower than the current gap for the incoming load reported from its upstream it tries to shorten it with

lowering of the speed and to possibly perform momentary stop during the accept and while the load still does not lie over it as shown on Fig. 8.

The proposed algorithm is suitable for conveyor applications where the backward movement of the loads is undesirable or not allowed. If, however, the application allows for such a movement the zones can further shrink the gap with backward movement of the load until it goes off the downstream zone and continue to move the downstream backwards while keeping the upstream stopped until the gap size gets to the required one. Move both zones back to their previous position but with a load moved forward. This addition to the algorithm should take place after some hysteresis of the required and actual gap difference because as newly loads enter the conveyor the zones will recalculate the required gaps as lower. This will cause movements for gap shrinkage on each newly entered load, which is not energy efficient and is not much worth. The zones can automatically calculate the hysteresis value so the movement of all zones that can shrink gaps will happen when the places (free zones) at the upstream of the linear part are less or equal than two. This will ensure that the linear part will not block its load source part of the system and will store as much loads as possible.

The zone maintains a counter for such consecutive out of range errors and if they happen more times, than a preconfigured limit, the zone can take action for increasing ramp up and ramp down times of the movements.

Such an adaptation of the movement ramps is very efficient on places where slippery is likely to happen because the zone ramps were not configured properly and load has bad adhesion (for example empty paper or plastic trays).

The number of the loads between for example load *j* and the end of the conveyor n and the number of loads between *j* and the beginning of the conveyor give an estimation for the occupied density after $\overrightarrow{d_J}$ and before $\overleftarrow{d_J}$ the example load. However, there is a better estimation if the sum of the load lengths is used relatively to the sum of the gap lengths. For the density before the example load that would be (6).

$$\overleftarrow{d_J} = \frac{\sum_{i=0}^{j} l_i}{\sum_{i=0}^{j} g_i} \tag{6}$$

For the density after the example load respectively (7).

$$\overrightarrow{d_J} = \frac{\sum_{i=j}^{n} l_i}{\sum_{i=j}^{n} g_i} \tag{7}$$

One can calculate the desired gap $\hat{g}$ using the following formula, where k is a coefficient representing the configuration, value and gap scale (8).

$$\hat{g}_j = k \frac{\overleftarrow{d_J}}{\overrightarrow{d_J}} \tag{8}$$

Each zone recalculates this value for each of the load in its “Move:” list when it receives an update from its upstream and its downstream. In order to minimize network traffic zones can exchange partial sum between them so the zone that receives it adds only its values.

II.2 Proposition for improving the power supply

The proposed method allows the usage of power supplies with much lower current capabilities than the nominal current of all installed control modules and significantly reduces the cost of the conveyor system while eliminating the risk of an accidental protection activation.

Usually the generated energy from the modules during a deceleration is 100% converted to heat. With the proposed method a part of it or the whole energy can be reused and thus it is possible to achieve a much better energy efficiency.

The proposed solution benefits from the time synchronization protocol IEEE 1588 that allows for distributed systems connected via Ethernet to have their clocks synchronized within few microseconds. An assumption that no parallel power connections will be made between any two points in the system. That is usually the case in all conveyor systems because of the price of the cables and the labor cost.

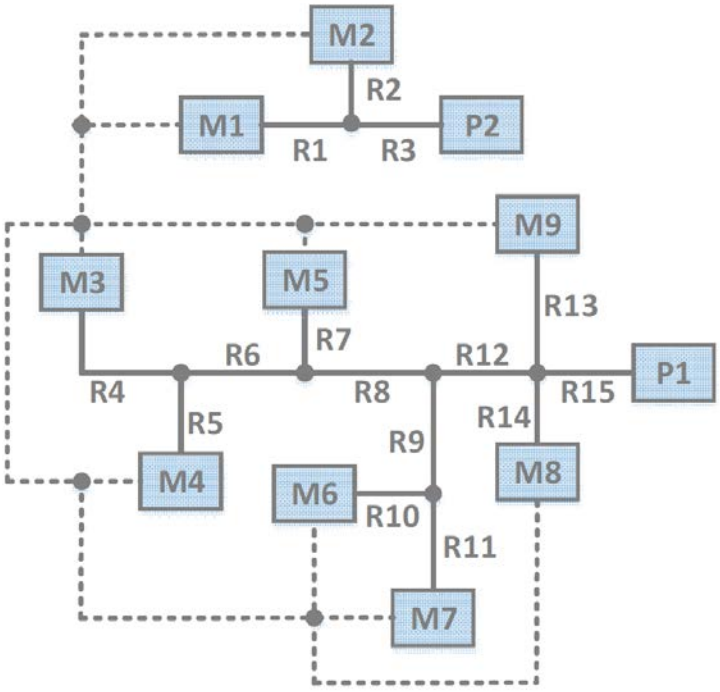

Fig. 9 Example scheme for power supply and communication on a conveyor

This method requires a consistent power consumption during the investigation time so it can be performed once at system startup. At this time, no

motors are allowed to run by the conveyor algorithm. Each module sends a broadcast message with an invitation for power map discovery.

Let us consider the conveyor system shown on Fig. 9. The dashed line shows the communication and the solid line shows the power supply.

Modules that are visible to each other elect a random ordered list of themselves identifiers $L\{m_1, m_2, \dots m_n\}$ according which each one will start to consume power by its compensation circuit for a short period of time initially set for 1ms.

At the end of this short interval the module m_x that did the loading will send a broadcast message over the network with the timestamp of the load test beginning, the measured current consumption from the power supply and the measured voltage before V_0 and during the test V_L.

All other modules are listening for that message and they are continuously measuring the power supply voltage using a sliding window with size 20 values and a resolution of 500us. These values are configurable. Once they receive the broadcast message, they match the timestamp in the message to the specific measured item in the window using their already synchronized clock according to the IEEE 1588 protocol. Listening modules extract the value pointed by the timestamp from the window as V_L and an average value from the rest measurements calculated as V_0.

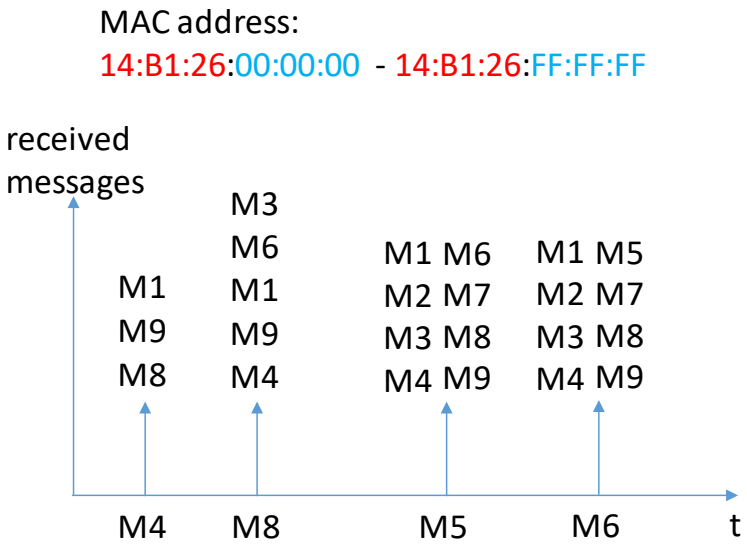

Fig. 10 Timeline of received messages

There are several conclusions that a listening module m_y can do when processing the gathered measurements:

1) *Same or different power supplies.* If V_L of m_y equals to V_0 of m_y different power supplies power the modules. This can be concluded

because there should be some voltage drop in the power supply and in the wires if m_x consumes current.

2) *Further or not from the power supply*. If V_0 of m_y is the same as of V_0 of m_x and V_L of m_y equals to V_L of m_x module m_y is further than m_x from the power supply. Note that V_L is lower than V_0 so it is impossible to have V_L and V_0 of m_y with equal values. That distinguishes this case from the previous one. Module m_y calculates the resistance between the split point S_{xy} and the power supply (including the internal resistance of the power supply) by:

$$R = \frac{V_0 - V_L}{I_L} \tag{9}$$

Here $V_{0m_x} = V_{0m_y} = V_0$ and $V_{Lm_x} = V_{Lm_y} = V_L$. Module m_y creates an id for that split point using its hash value and the hash value of the module that did the test. It records the resistance value and the split point name in a list.

On the path to the power supply or not. If V_0 of m_y is the same as of V_0 of m_x and V_L of m_y is higher than V_L of m_x. Module m_y is between the power supply and m_x. Module m_y can calculate the resistance between the power supply (including its internal resistance) $R_1$and the one between the point where the wires are split s_{yx} and the module m_x R_2

$$R_1 = \frac{V_0 - V_{Lm_y}}{I_L} \tag{10}$$

$$R_2 = \frac{V_0 - V_{Lm_y} + V_{Lm_x}}{I_L} \tag{11}$$

Here $V_{0m_x} = V_{0m_y} = V_0$. Both resistances and the id of the split point, created like in the previous case are recorded to the list.

The described algorithm can't distinguish between the resistance starting from the power supply terminal and the first point or module where the line is split and the impedance into the power supply itself. They are treated as one value (which is the sum of both).

All modules collect the information only if they found that they are connected to the same power supply. They store the resistances in a list with start and end points which are the hashes of the modules calculated before, the created split point number or 0 if that point is the power supply. Modules store the name of the list itself which is the hash of the first module that did a load test (which also happens to be the module with the lowest MAC value connected to this supply unit) and that they found to be connected to the same power supply.

When the last module in the list does the load, test it sends a message that triggers a list information exchange between all modules. Each module considers only the messages with lists containing the same name as the list it just prepared. There will be two lists with the same name shown on Fig. 11:

Reported from m_2:

$$m_2, 0 = R_2 + R_3;\ m_1, s_{21} = R_1;\ s_{21}, 0 = R_3$$

Reported from m_1:

$$m_1, 0 = R_1 + R_3;\ m_2, s_{12} = R_2;\ s_{21}, 0 = R_3$$

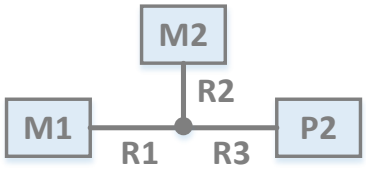

Fig. 11 Simple example of power supply distribution

II.3 Signal encoding method for improving data reliability

When receiving incorrect information about the position of the rotor and performing incorrect switching, the current through the windings can increase significantly, but this is for a short period of time until the controller receives the correct information about the current position or the next. This leads to a deterioration in the quality of movement.

There are two proposed methods for improving the communication:

- Coding the data using equal Hamming distance combinations;
- Prediction of the first most possible next state. The state is sent four times as three bits. Depending of the expected state in the turning direction and the existing of this state in at least in two places, it accepts as a true, because is most popular according to Ockham's razor.

II.4 Securing the devices against cloning

This part proposes several methods and techniques for securing the IoT devices against cloning and respectively, how to design the devices that make copying of the software almost impossible.

Let us consider a device with some amount of flash memory in the microcontroller and some external bus where the new firmware (usually the application part) will come from. The cost of the device is tightly related to the microcontroller memory sizes. There are usually microcontrollers of the same family with the same functionality but with different memory sizes. The cost depends on the memory size needed. Therefore, it is intelligibly that a designer will try to fit in the lowest possible amount of memory.

On the other side, there are two factors: Cheap chips of standalone flash memories and unreliable communication channel for upgrade procedure. In this situation, it is absolutely normal that the designer will try to write the new firmware in such an external memory, verify its integrity and then overwrite the microcontroller's internal firmware. Otherwise, half of the microcontroller flash memory will be wasted for a temporary buffer, fig. 1.

.

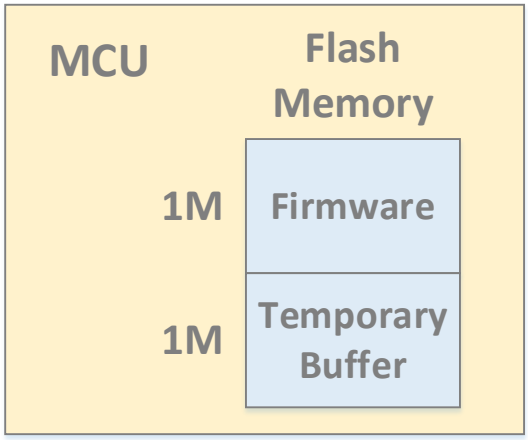

Fig. 12 Half of the MCU Flash memory is wasted for a temporary buffer

Such a design that looks optimal in terms of cost – functionality looks good but in terms of anti-copy means is bad. Sniffer connected to the external bus (usually I2C or SPI) can sniff and record all the firmware and after that use it to make copies of the device, fig. 2.

Other way of recording the firmware program is to sniff the main communication channel that the device supports. This could be Ethernet, USB, Bluetooth, Wi-Fi, Zigbee, etc.

Many times an embedded device that cooperates with other devices from the same manufacturer incorporates some king of self-healing or self-upgrading methods that involves reading the most recent firmware of the freshly connected device from some previously connected one. The channel that transfers that firmware is also a flaw if it is not secured, Fig. 13.

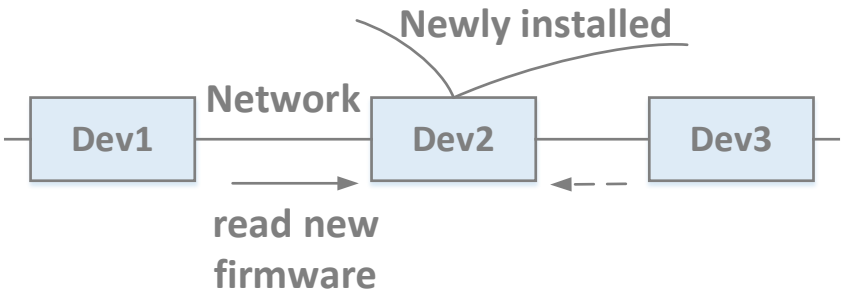

Fig. 13 Reading the most recent firmware of the freshly connected device over unsecured connection

In order to avoid such sniffed data to be useful for copying of the devices the designer decided to encrypt them. So for example before writing to the temporary outside flash memory all the data gets encrypted, transferred, written and when the whole transfer finishes and the writing to the inside memory begins they are read and decrypted back, Fig. 14. Although this seems a good solution since the read data don't contain anything useful like machine instructions for the target processor it won't help against copying of the device, if the encryption doesn't' depend on a value that is different from a part to part. This could be some serial number or unique number that the microcontroller's manufacturers stored during manufacturing. Otherwise even if the data is stored encrypted and if suppose that the bootloader/kernel that do the upgrade procedure exists in the new microcontroller it would decrypt the content of the stored data exactly like the original microcontroller thus allowing for a copy of the device to work identically as the original one.

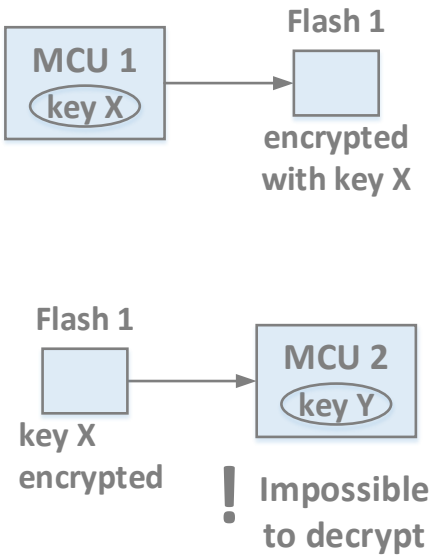

Fig. 14 Encrypting of the data

As mentioned above the encryption of the firmware should depend on the unique value in the chip. Such values are usually available in many of the chips in the system. For example, Ethernet switch, microcontroller, serial flash memory, etc. These can be used to construct a fingerprint of the device that is used in the encryption of the firmware and data, Fig. 15. This will prevent the device to work with replaced chips and if any of the chips were removed, it would not work on another device.

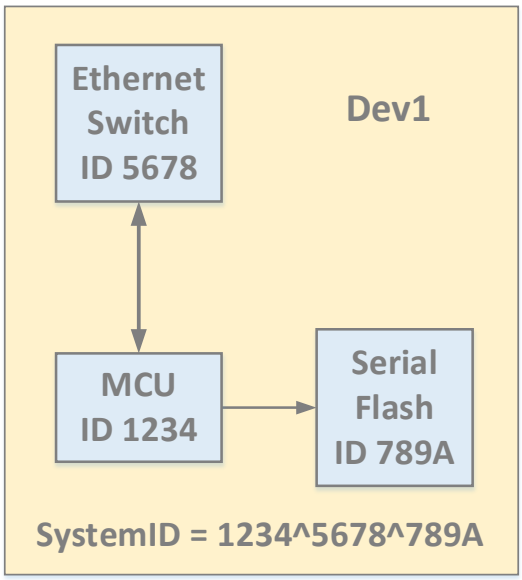

Fig. 15 Constructing a fingerprint of the device that is used in the encryption of the firmware and data.

Usually microcontrollers even with disabled JTAG access still have the ability to be erased either by separate pin or with JTAG “erase chip” command (that would be the only possible command). For the hacker it is possible to record the firmware upgrade communication, erase the chip, which will clear the configuration that disables the JTAG access, then read its ID. Serial numbers of Ethernet switch and serial flash memory can be easily read even if the serial flash has protected page(s). Eventually the device key can be reconstructed. In order to avoid such a possibility, it is good idea to use asymmetric encryption and random numbers based public key.

In case that symmetric encryption is used for the outside world communication, it is good to include in the key some known value for both sides (the IoT device and the computer) like the socket port number TCP window sequence number, MAC addresses etc. This will make the encrypted file always different and it would be much more difficult to the hacker to realize what causes the difference.

III CHAPTER - IMPLEMENTATION OF THE PROPOSED METHODS

III.1 Improving data integrity

When trying to obtain a global position of the rotor where each new state change means also direction of movement any error in the newly received state can lead to accumulating an error in the position and so the whole method can be compromised. Therefore, a filtering techniques and appropriate signal conditioning are used so if the new state is not the expected one in any of the both possible directions of rotation neither the last one some decision has to be done.

On Fig. 16 there is an oscillogram showing the result of the wrong received state drawn with pink over the current consumption of the motor drawn with green line. In the middle, the very upper state is missing and that results in an immediate increase of the consumed current. With dark blue, the communication signal is shown which is zoomed on the lower half of the picture where the disturbance is visible.

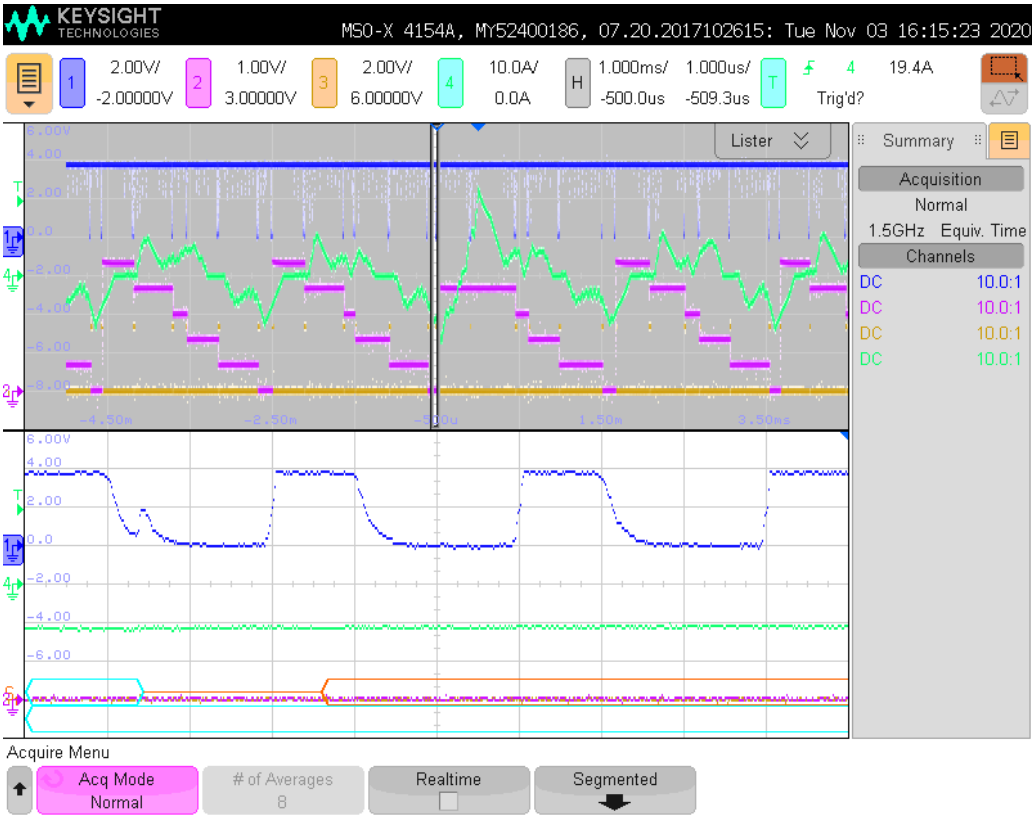

Fig. 16 Current consumption increase because of wrong received state

Software, which finds the combination of bits that are equally spaced by Hamming, is developed. Its results are used in the sensor states transmission. Part of the source code and the user interface are shown on Fig. 17 and Fig. 18.

The results are used in the firmware in the motorized drive roller and the controller that do the commutation for encoding and decoding the communication.

```
        /* mask off anything above the top bit */
        x &= ((uint)1 << bits) - 1;

        /* Align to 4-bits */
        bits = (bits + 3) & ~0x3;

        /* Calculate crc4 over four-bit nibbles, starting at the MSbit */
        for (i = bits - 4; i >= 0; i -= 4)
            c = crc4_tab[c ^ ((x >> i) & 0xf)];

        return c;

    }
    int iHammingDistance(byte b1, byte b2) {
        byte diff = (byte)(b1 ^ b2);
        int dist = 0;
        for (int i = 0; i < 8; i++)
            if ((diff & 1 << i) != 0)
                dist++;
        return dist;
    }
    List<byte> lbGetBytesOnHamming1dist(byte b) {
        List<byte> lb = new List<byte>();
        for (int i = 0; i < 8; i++) {
            lb.Add((byte)(b ^ (1 << i)));
        }
        return lb;
    }
    string sPrintByteList(List<byte> bl, bool bPrep0x) {
        string s = "";
        foreach (byte b in bl) {
            if (bPrep0x)
                s += "0x";
            s += b.ToString("X2") + ", ";
        }
        return s;
    }
}
```

Fig. 17 Software for generation of equally spaced by Hamming combinations

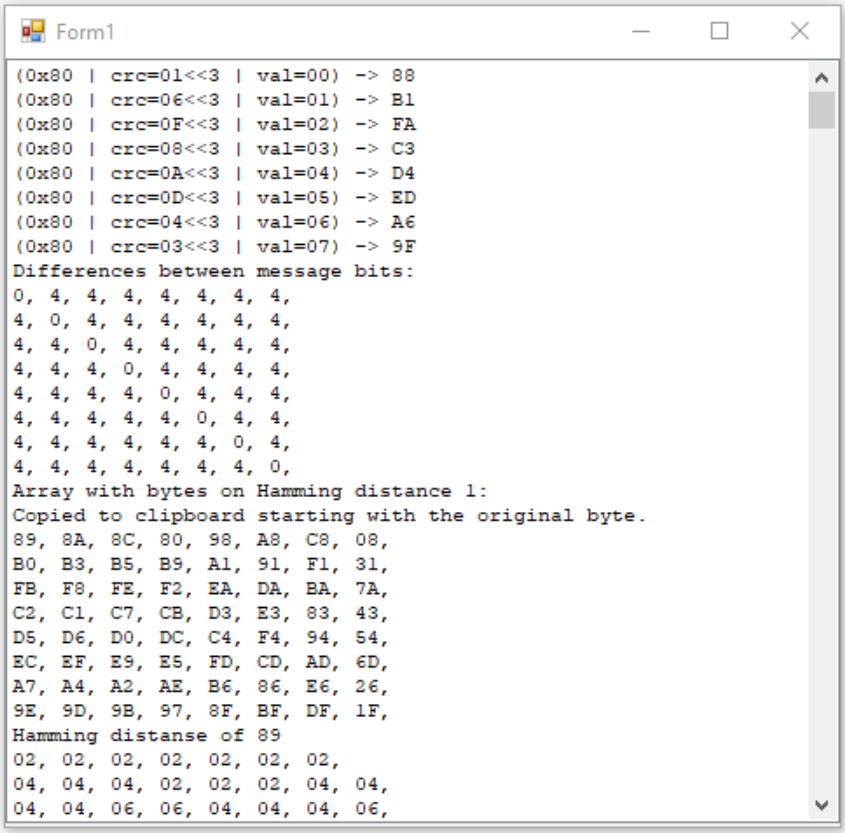

Fig. 18 Results of the software for generation of equally spaced by Hamming combinations

III.2 Improving the powering of the conveyer systems

On any module connected to each power, supply two configuration values are set. The first one is the maximal current that the power supply can provide without tripping an overload protection. The second one is the maximal voltage it can tolerate on its output terminals without tripping an overvoltage protection. The module updates with that information all other modules in the same power group.

Each module accounts for the total current drawn from the power supply. It updates the value from the broadcast messages from the rest of the modules in the power group. A module is obliged to send an update if its current consumption changes outside a preconfigured threshold initially set to 0.5A.

There are three places in the message for the total value I_T, the actual module current I_M and the incremental part I_I that triggered the update Fig. 19. A module only gets the total value and updates its internal value if a predefined timeout has elapsed before and after the message reception initially set to 100ms. Otherwise, it uses only the incremental value I_I to update its internal value. This mechanism ensures that if two messages are send with a very short delay between them the recipient will not mess the value of the total current. This could happen if the last

sending module has not received and decoded the previous message and sends a total current without including the increment of the previous module.

Message data

Total current	Module current	Incremental current

Fig. 19 Format of the message for the consumed current

All modules maintain a list with the consumptions of the rest of the modules in the group in order to verify the total current at a predefined regular intervals initially set to 10sec. Modules are sending an update message with their I_M and I_I currents once per this interval.

The first keystone of the algorithm is that if a module needs to draw current it checks the total current drawn at the moment and the total permissible current from the power supply and if the current is insufficient it uses only the available part of it. This ensures that the power supply will not trip its current protection.

The second keystone is that when a module tries to decelerate its motor and generates an energy it can return to the power line the part that is equal to the total consumed currently current I_T subtracting some predefined margin initially set to 0.5A. A margin is necessary because if the total current is close to zero it can go negative for short period. If so, the voltage of the power line can rise and an overvoltage protection of the power supply can be a trip. The module that returns energy does calculation of voltage drops starting from the power supply while plugging its maximal permissible voltage previously set. Continuing down the line using the resistances of each part of the line calculated before and the list with the currents that each module consumes currently according to Kirchhoff's and Ohm's laws the module calculates the maximal current it can return limited by the voltage I_{MV}. The module chooses the lower value between $I_T - 0.5$ and I_{MV} and sets I_M to the negative of that value. The values I_I and I_T are calculated accordingly. The module sends a message with these values. If the module needs to return more current than the value it calculated it uses its compensation circuit and dissipates it as heat.

Fig. 20 shows how the power supply voltage increases when objects of different weights are deaccelerated. In the case of a heavier object, that has accumulated significantly kinetic energy, the increase is also significant.

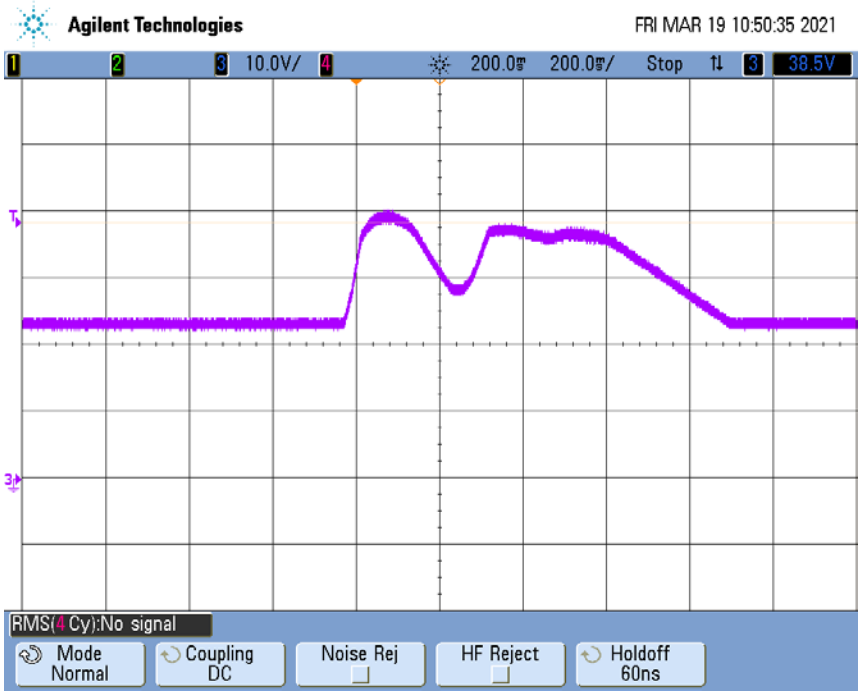

Fig. 20 Increasing the supply voltage when deaccelerating a heavy object

III.3 Creating the computer simulation

The simulation software FlexSim gives an opportunity for a script to be written which can do calculations when event happen somewhere on the conveyor system. The source that is shown on Fig. 21 performs a dynamic change of the length of the gap distance between the objects.

```
Conveyor current = ownerobject(c);
Object item = param(1);
{   // Cv2
    Object involved = item;
    //current.targetSpeed = current.currentSpeed * 0.7;
    int traysNum = current.subnodes.length;
    int i;
    double len = 0.0;
    for (i = 1; i <= traysNum; i++) {   // find the total box len
        Object o = current.subnodes[i];
        len += o.size.x;
    }
    if (len > current.size.x)
        len = current.size.x - traysNum * 0.04;
    double lenUp = (current.prev.trayUp? == nullvar) ? 0.01 : current.prev.trayUp;
    double gapUp = (current.prev.gapUp? == nullvar) ? 1 : current.prev.gapUp;
    double lenDn = (current.next.trayDn? == nullvar) ? 0.01 : current.next.trayDn;
    double gapDn = (current.next.gapDn? == nullvar) ? 1 : current.next.gapDn;
    current.labels.assert("gapUp", 0).value = gapUp + current.size.x - len;
    current.labels.assert("trayUp", 0).value = lenUp + len;
    current.labels.assert("gapDn", 0).value = gapDn + current.size.x - len;
    current.labels.assert("trayDn", 0).value = lenDn + len;
```

Fig. 21 Code for dynamic change of the length of the gap between the objects

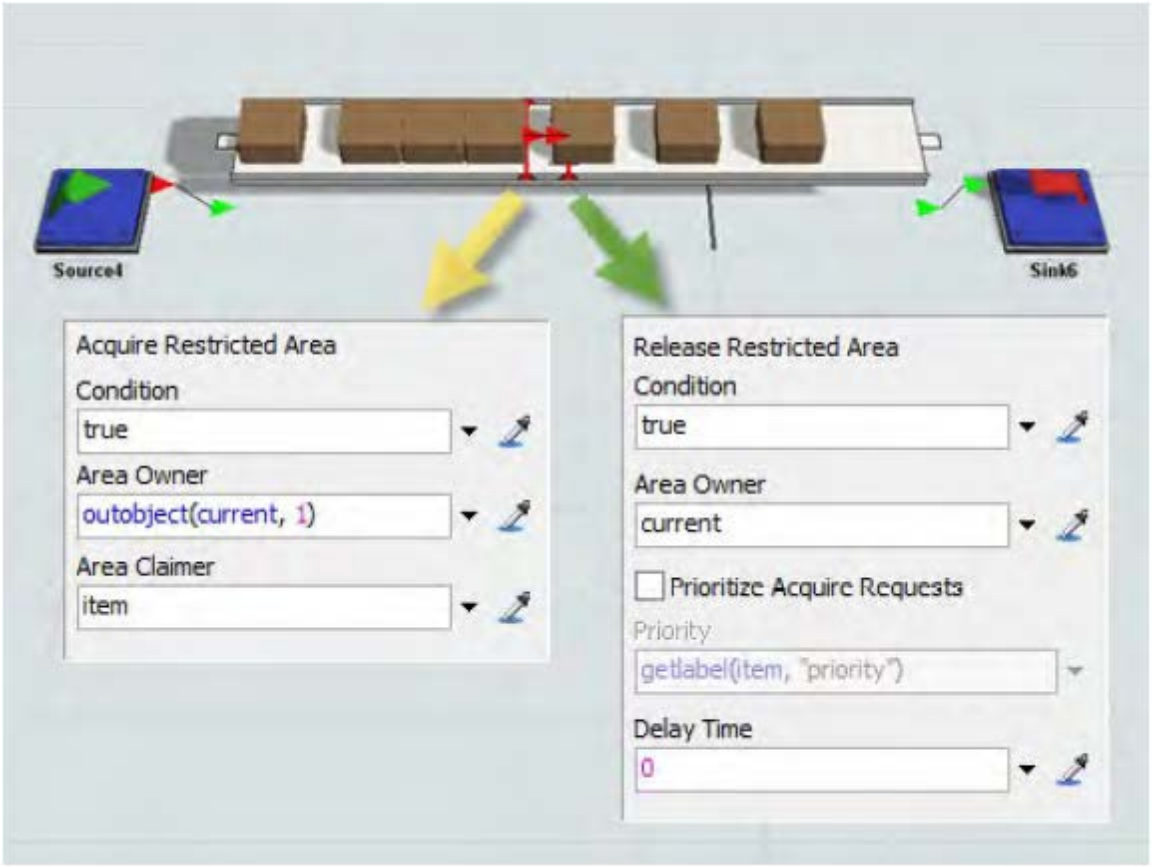

Fig. 22 Adjusting parameters on built-in control blocks

There are some built-in functionalities that can be used out of the box with only adjustments of some parameters as shown on Fig. 22.

IV CHAPTER - EXPERIMENTS AND TESTINGS

IV.1 Results of the applied method for improving data integrity

The following log file shows the corrections that are performed on the rotor positions. For example, on the first line there are errors in the three of the four 3bit fields and they are corrected based on the list of the expected stated „ExpHall:6,2,3“ which keeps the states in a descending by probability order.

```
MotMain:[81819028]Old(hall:2,  pos:5),  ExpHall:6,2,3,  New(hall:6,
pos:0), RX:[00|4|7][10|3|6]<-[10|2|2][10|2|2]<-[10|3|3][10|3|3]

MotMain:[81819760]Old(hall:2,  pos:5),  ExpHall:2,6,3,  New(hall:2,
pos:5), RX:[10|2|2][00|4|4]<-[10|2|2][10|2|2]<-[10|2|2][10|2|2]

MotMain:[81820636]Old(hall:2,  pos:5),  ExpHall:2,6,3,  New(hall:2,
pos:5), RX:[10|2|2][00|4|4]<-[10|2|2][10|2|2]<-[10|2|2][10|2|2]
```

By virtue of the suggested method error in the received information are successfully corrected and thus the overall performance of the motorized drive roller is improved.

IV.2 Results of the applied method for improving the power supply

Energy return to the power supply unit from a typical controller for zone control while stopping a heavy object is shown on Fig. 9. In case of heavier object, which has gained higher kinetic energy the voltage, increase is high. The nominal supply voltage is 24V and the vertical resolution of the oscillogram is 10V/division. The graphic shows that the voltage can rise up to 40V, which almost double the nominal value. This is the limit that the electronic components in the controller and the power supply unit can sustain.

Fig. 12 shows an oscillogram for the case where intelligent energy distribution is taking place where the slowing down of an object can be delayed in order to let the rest of the zones to consume that excessive energy.

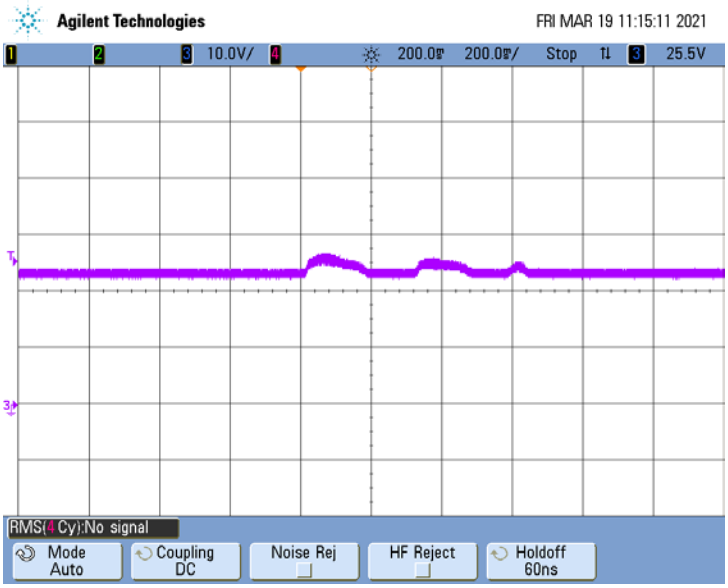

Fig. 23 Voltage change when distribution of energy is used

Usually the generated energy from the modules during a deceleration is 100% converted to heat. With the described algorithm a part of it or the whole energy can be reused and thus achieving a much better energy efficiency. As many modules to one power supply are connected as more energy is recovered because there is a higher chance that another module will need the energy at the time it is returned. Moreover more modules mean more operating current – that is also supplied from the returned power.

IV.3 Simulation results of the applied method for distributed control

A conveyor using this algorithm will have large calculated gaps and good throughput if the number of loads between the beginning and the end is lower. If the number of incoming loads increase, the gaps between the recently incoming loads will get lower allowing for better storage density as shown on Fig. 23 and Fig. 24.

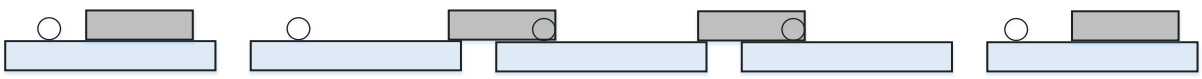

Fig. 24 Conveyor with low density.

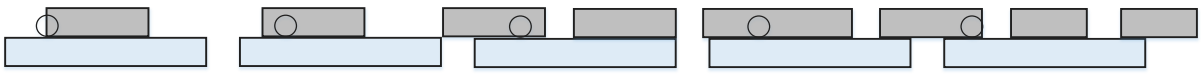

Fig. 25 Conveyor with higher density.

The zones can continue measuring the load sizes and gaps and do statistical averaging of the value in order to get closer to the real one. Together with the value for any size (of the load or the gap), the zones can exchange an additional value showing how likely is that this value represents the real size. If a zone finds that during its statistical averaging its value is very different from a received one that has higher received reliability coefficient (which means that many zones have proved this value as correct), it can assume that there is some slippery or external intervention over the load and that its odometer is wrong.

The results of the simulations show an increase in the efficiency of the system Fig. 25 and Fig. 26, which can be achieved through relatively simple distributed calculations, which allows the use of existing hardware.

Increasing the efficiency of the system is achieved without the need for additional settings.

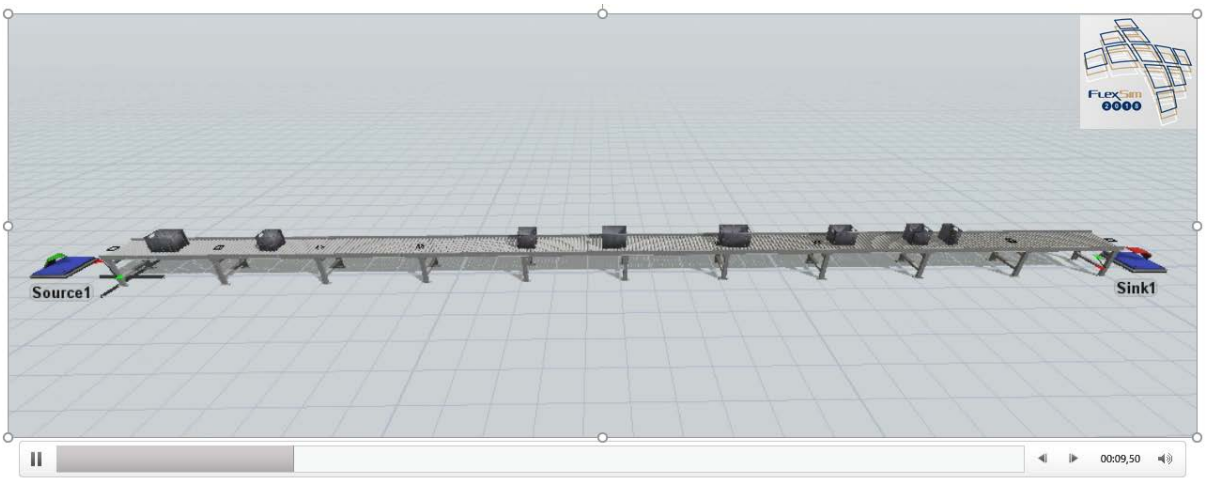

Fig. 26 Operation of the conveyor without accumulation of objects

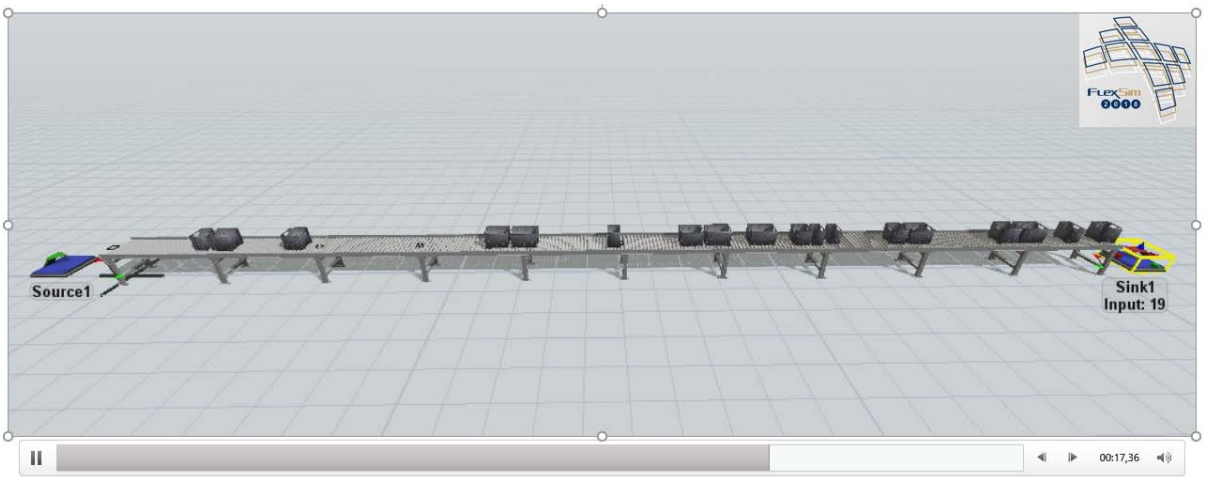

Fig. 27 Accumulation of the conveyor after passing 20 objects

IV.4 Experiments and tests of the entire system

We had an opportunity to do testing and experiments on a real-life system, which was rather small, but with everything that we need Fig. 27.

Fig. 28 Experimental conveyor

Computer simulations and the experiments performed gave fairly good results.

IV.5 Conclusion

The proposed innovative method for distributed control improves the performance and reliability while using the same hardware.

The novel algorithm buffers more loads on the conveyer while keeping the throughput high by dynamically change the gabs between the loads.

The proposed methods for enhancing the subsystems for measuring, power supply and communication add extra value to the work.

The proposed method for securing controllers against cloning was presented at the 9th Balkan Conference on Informatics, 2019.

The research, development and implementation of the method for map discovering and distribution of the energy consumed from the power sources were presented at the international conference IEEE-IS'2020.

The research, development and implementation of the method for distributed control of conveyer systems based on software agents was presented at the international conference IEEE-IS'2018.

As a future development, the creation of a method for automatic configuration of parameters through the use of IA methods is envisaged.

Thesis contributions

- Research analys of the methods and techniques for control of the conveyer systems;
- Proposed solution for improving the efficiency of the conveyer systems by using advanced method for distributed control;
- Proposed new methods for enhancing the subsystems for measuring, power supply and communication;
- Modeling and computer simulation of the proposed method for distributed control;
- Design and implementation of the prototype for testing the functionality of the proposed solutions;
- Test cases for verification and evaluation the effectiveness of the methods, which confirm the achieved level of improvement in reliability and performance.

Publications

- Andonov, I, Tsvetanov, S, **A Novel Algorithm for Distributed Control of Conveyor Systems**, IEEE-IS'2018 Conference, Madeira Island, Portugal, pages: 379-372, Sep. 2018, DOI: 10.1109/IS.2018.8710518
- *Ivailo Andonov*, *Simeon Tsvetanov*, *Stefan Dimitrov*, **Securing IoT devices against cloning**, COMPUTER & COMMUNICATIONS ENGINEERING, vol:13, issue:2, 2019, pages:25-28, ISSN (print):1314-2291
- *Андонов, И.,* ***Разпределено управление на конвейерни системи***, ISI Journal, issue: 1, 2020, ISSN 2534-8531, (под печат)
- *Andonov, I, Tsvetanov, S,* **Power supply map discovering and efficient energy distribution method for distributed conveyor systems**, IEEE-IS'2020 Conference, Varna, Bulgaria, pages: 1541-1672, Sep. 2020, DOI: 10.1109/IS48319.2020.9200130

Declaration of Originality

I declare that this thesis, conducted for the purpose of receiving the academic title “Doctor of Philosophy” (PhD) in the field of 4.6 Informatics and Computer Science is my work and no foreign publications and developments have been used in violation of their copyright. Quotations of all sources of information, text, illustrations, tables, figures are marked by standards. The results and contributions of this thesis obtained are original and are not borrowed from research and publications in which I have no participation.

Signature: