Strojniški vestnik - Journal of Mechanical Engineering 54(2008)11, 783-795 Paper received: 17.03.2008
UDC 658.512 Paper accepted: 25.09.2008

Reliability and Efficacy of Identification Systems and Supply Chain Management[1]

Robert Brumnik* - Zvone Balantič
University of Maribor, Faculty of Organizational Science, Kranj

The processes of production and logistics often involve the requirement to reliably identify the individuals responsible for certain operational procedures (complaints, process audits, preventive-corrective actions due to non-conformance). The individuals in charge of these procedures usually have their own way of identity confirmation (signature, PIN codes, chip cards[2], biometric identifications, camera, etc.). It is thereby necessary to reduce the scope of information to the legally acceptable limit that insures personal integrity and confidentiality.

Because of the continuous optimization and automation of processes there is an increasing trend towards »simple identification systems« in the production and logistics processes. Biometry makes the identification process faster and simpler by using people's unique characteristics[3] without the need for any additional identification elements. However, it is necessary to research the reliability and efficacy parameters of this identification method in order to avoid unnecessary complications that could arise from selecting unsuitable technology.

Keywords: production processes, logistic processes, identification, automation, reliability, efficiency, biometry

0 INTRODUCTION

Production logistics must ensure an effective flow of material, tools and services during the whole production process and between companies. Solutions for traceability of products and people (identification and authentication) are very important parts of the production process. The entire production efficacy and final products quality depend on the organization and efficiency of the logistics process. The capability of a company to develop, exploit and retain its competitive position is the key for increasing company value [7].

Globalization dictates to the industrial management an effective, lean[5] manufacturing, downsizing and outsourcing. The requirements of modern times are development and the use of wireless technologies such as the mobile phone. The intent is to develop remote maintenance, remote servicing and remote diagnostics [8]. With the increasing use of new identification technologies, it is necessary to explore their reliability and efficacy in the logistics process.

The new identification systems are achieving extremely fast development in the last ten years with the evolution of microelectronics and it enables practical application in the branch of automation of logistics and production. It is necessary to research and justify every economic investment in these applications.

[1] Supply Chain Management (SCM); the process of planning, implementing, and controlling the operations of the supply chain as efficiently as possible. Supply Chain Management spans all movement and storage of raw materials, work-in-process inventory, and finished goods from point-of-origin to point-of-consumption.

[2] Chip card (Smart card, Integrated Circuit card - ICC or Contact less RFID card) is defined as any pocket-sized card with embedded integrated circuits which can process information. This implies that it can receive input which is processed - by way of the ICC applications - and delivered as an output. There are two broad categories of ICCs. Memory cards contain only non-volatile memory storage components, and perhaps some specific security logic. Microprocessor cards contain volatile memory and microprocessor components.

[3] Characteristics; elements of unique personal identification (fingerprints, cornea, iris, DNK).

[4] Radio-frequency identification (RFID) is an automatic identification method, relying on storing and remotely retrieving data using devices called RFID tags or transponders. RFID tag is an object that can be applied to or incorporated into a product, animal, or person for the purpose of identification using radio waves. Some tags can be read from several meters away and beyond the line of sight of the reader. Most RFID tags contain at least two parts. One is an integrated circuit for storing and processing information, modulating and demodulating a (RF) signal, and other specialized functions.

[5] Lean manufacturing; Lean is essentially a business discipline that is built around obeying only the customer's demand signals (or "pull") and getting rid of waste everywhere in the supply chain, waste in overproduction as well as in inventory [9].

*Corr. Author's Address: University of Maribor, Faculty of Organizational Science, Kidričeva 55a, Kranj, Slovenia, robert.brumnik@metra.si

The production process needs to be efficacious and carefully planned with the support of dynamic analysis and optimization tools (MS Visio, Process Simulator, etc.). In this paper the most important quantitative characteristics of reliability are explained. The authors also show the methodology for defining reliability and efficacy of identification systems in the process of production and logistics and provide experimental research of personal identification systems[6] based on reliability and efficacy parameters. Furthermore, an identification system of a real production-logistics system was upgraded based on automation and informatization.

In a comparative study based on wireless RFID and Biometric Identification Systems (see Figure 1.), the authors:

- show the availability and efficacy analyses in the processes of informatization and automation of production and logistics systems,
- extend reliability estimation of identification systems (RFID and biometric) based on significant reliability characteristics,
- research cost analysis of investment in an identification system,
- provide contribution to science by researching the process of production and logistics to ensure optimal procedures of automated identification.

A review of scientific databases shows that the area of assessing the reliability of identification systems in the process of production and logistics is not well explored. In modern production and logistics processes (automobile industry, aircraft-space industry, pharmacy, forensics, etc.) it is necessary to have a fast and reliable control over the flow of material and people.

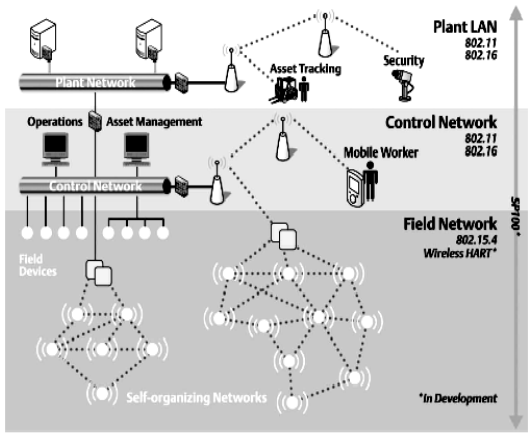

Fig. 1. *Self-organizing wireless network Identification technologies in the production logistic industry*

Companies such as army and automobile equipment suppliers can verify the serviceability of qualified parts. By using unique serial numbers of business events and transactions, connected to individual parts, it is possible to prevent any imitations or construction parts without warranty.

This paper deals with the systematical relations within identification systems. Statistical processing and conclusion forming were conducted using a tools for statistical treatment and reliability defining - Weibull++7. The aim of this research is improvement of the theoretical model, which will enable a better stability of identification in real dynamic systems. The theoretical research is followed by optimization including dynamic changes that can occur in the production-logistics process. Optimization as a function of automation will happen with linear programming[7] and numerical methods in order to minimize the production costs. Simultaneously, empirical data processing and development of a mathematical model take place.

[6] Personal Identification Systems; Recent events have heightened interest in implementing more secure personal identification (ID) systems to improve confidence in verifying the identity of individuals seeking access to physical or virtual locations in logistic process. A secure personal ID system must be designed to address government and business policy issues and individual privacy concerns. The ID system must be secure, provide fast and effective verification of an individual's identity, and protect the privacy of the individual's identity information.

[7] Linear programming; in mathematics, linear programming (LP) problems involve the optimization of a linear objective function, subject to linear equality and inequality constraints. More formally, given a polytope (for example, a polygon or a polyhedron), and a real-valued affine function.

1 DEFINING THE PROBLEM AND RESEARCH PARAMETERS

The availability of a production-logistic process is the probability that the system is functioning well at a given moment or is capable of functioning when used under certain circumstances. Reliability by definition is probability (capability) of the system to perform under stated conditions defined by function and time [4]. It is one of the most important characteristics of efficacy of identification systems and has an impact on safety and efficiency of the system. Increasing the system's reliability means less improper uses, higher safety, less repair procedures and shorter identification time and consequently causes higher system availability. Implementing higher reliability in early development phases and its assurance during the use of the identification system requires the knowledge of methods and techniques of reliability theory and their interactions.

Many different characteristics are used to measure the reliability of identification systems and their components. Some of them are connected to time functions; others represent average time functions. Which of these characteristic are relevant in specified cases depends on the set goals, selected method of analysis, and the availability of data.

Characteristics of reliability are based on mean time intervals to the occurrence of failure. Time to failure is a random magnitude and we will mark it with symbol ti. In this paper we give definitions and statistical estimations of basic reliability characteristics.

Reliability characteristics used in this research are:

- MTTF - mean time to failure
- MTBF - mean time between failures
- MTTR - mean time to repair
- *F(t)* - unreliability function
- $\lambda_{(t)}$- failure rate
- β - shape parameter
  a. β<1 temporary failure frequency $\lambda_{(t)}$ decreases (early period, system implementation)
  b. β=1 temporary failure frequency $\lambda_{(t)}$ is constant (normal system operation)
  c. β>1 temporary failure frequency $\lambda_{(t)}$ increases (exploitation, ageing)

The shape parameter (β) changes the configuration of the temporal distribution of operational failures.

1.1. Quantitative Reliability Characteristics

Unreliability function *F(t)* is defined by the equation:

$$F(t) = P(t_i \le t) \tag{1}$$

F(t) is therefore the probability of a system to become non-functional in the interval between 0 and *t*.

If we observe a number of systems or system components we can calculate the statistical estimation for the unreliability function by the equation:

$$\widehat{F}(t) = \frac{N_0 - N(t)}{N_0} \tag{2}$$

$N_{(t)}$ - number of working/functional samples in the interval (0,t)

N_0 - number of samples at the start of observation at $t = 0$

Reliability function *R(t)* is complementary to unreliability function. We can define it using the equation:

$$R(t) = 1 - F(t) = P(t_t > t) \tag{3}$$

$R_{(t)}$ is the probability for a system or a component to become non-functional after a time period t. A statistical estimation of the reliability function we can define using the equation:

$$\widehat{R}(t) = \frac{N(t)}{N_0} \tag{4}$$

The product of the time to failure function and dt is the probability of the system or its component to become non-functional in the interval (t, t+dt). We can calculate the function F(t) by differentiation of the unreliability function by time:

$$F(t) = \frac{dF(t)}{dt} \tag{5}$$

The statistical estimation for f(t) can be calculated with the equation:

$$\hat{f}(t) = \frac{N(t) - N(t + \Delta t)}{N_0 \cdot \Delta t} \tag{6}$$

where Δt is interval $(t, t + \Delta t)$.

Product of Failure rate $\lambda_{(t)}$ and dt is the conditional probability of a system/part of system to become non-functional in the interval (*t, t+dt*).

Momentary frequency of failure rate can be written as:

$$\lambda(t) = \frac{f(t)}{R(t)} \tag{7}$$

The statistical estimation for $\lambda_{(t)}$ is defined with the equation:

$$\hat{\lambda}(t) = \frac{N(t) - N(t + \Delta t)}{N(t) \cdot \Delta t} \tag{8}$$

For many systems or system parts the function $\lambda_{(t)}$ has a characteristic "bathtub" configuration (Figure 2.). The life cycle of systems can be divided into three periods: early damaging period, normal working period and ageing or exploitation period. $\lambda_{(t)}$ in first period decrease in second period $\lambda_{(t)}$ is constant and $\lambda_{(t)}$ growth in third period.

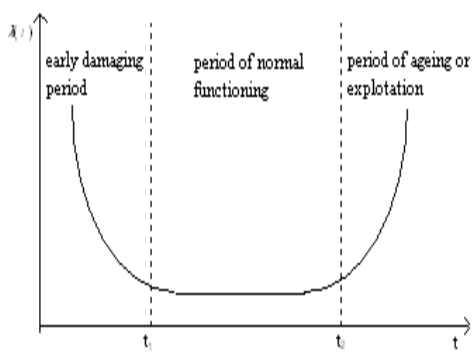

Fig. 2. *"Bathtub" curve* [4]

2 THE METHODOLOGY OF RESEARCHING THE RELIABILITY OF IDENTIFICATION SYSTEMS IN THE PRODUCTION-LOGISTIC PROCESS

2.1. Reliability of RFID Identification Systems

The research was conducted on Memory and Microprocessing identificators that can be installed onto the construction elements in the production-logistic process. Identification of persons in production-logistic processes is provided by biometric identificators which are unique to every person. Memory Identificators do not have a processor and therefore can not dynamically process data. Cards are designed to save the value or tokens for one time or continuous use.

Microprocessing identificators usually contain a processor, input-output unit and various kinds of data storage. They are able to dynamically process data. At the moment 8-, 16-, and 32-, bit processors are in use and have in average 16 to 32 Kb EEPROM and 3 Kb RAM. Input-output unit transmits 9.6 to 115 Kbits per second (only half duplex mode is possible). In terms of processor power they can be compared to the IBM-XT computer and cards with Crypto coprocessor in some function significantly exceed the 50 MHz 486 computer.

With adequate construction [1], the majority of operations and logs can be transferred from smart cards to PCs that have better working and process capabilities. For the cryptosystem RSA[8] with public keys, the recommended key length is 2000 bits. Adding components (e.g. coprocessor) increases the cost of cards and at the same time their reliability and safety are reduced. The conditions caused by the deficiency of data storage capacities or processing power can be improved with new technology (such as Cryptosystems with Elliptical Curves[9]).

[8] RSA; The mathematical details of the algorithm used in obtaining the public and private keys are available at the RSA Web site. Briefly, the algorithm involves multiplying two large prime numbers (a prime number is a number divisible only by that number and 1) and through additional operations deriving a set of two numbers that constitutes the public key and another set that is the private key.

[9] Elliptical curve cryptography (ECC) is a public key encryption technique based on elliptic curve theory that can be used to create faster, smaller, and more efficient cryptographic keys. ECC generates keys through the properties of the elliptic curve equation instead of the traditional method of generation as the product of very large prime numbers. The technology can be use in conjunction with most public key encryption methods, such as RSA.

They enable shorter safety keys and faster processing (with existing processor) and keep the same level of safety.

2.2. Reliability of Biometric Identification Systems

Definitions used in reliability calculation of biometric identification systems and terminology:

- FAR[10] is defined as the percentage of identification instances in which false acceptance occurs,
- FRR[11] is defined as the percentage of identification instances in which false rejection occurs,
- Mean time to failure (MTTF), mean time between failures (MTBF) and mean time to repair (MTTR),
- classification of failures,
- failures data bases.

In contrast to the classic methods of identification, in biometric methods probability needs to be considered. All sensors are subject to noise and errors. The largest problem is the development and implementation of a safe crypto algorithm. All limitations are summarized in the two terms: FRR and FAR. It a system is highly sensitive, the FAR value is low, but FRR is higher. In a system of low sensitivity the situation is reversed. Such us system accept almost everyone (FAR > FRR). It is therefore necessary to make compromise in the sensitivity of a system. It can also be regulated so that the FAR and FRR values are equal, the so-called EER (Equal Error Rate). Lower EER means a more accurate system. In application where the speed of identification is more important than safety (e.g. hotel rooms), the high FAR value can be allowed [3].

2.3. Identification and Verification (Authentication)

It often happens that we use the term identification when we talk about verification and vice versa. Identification is a term used for identifying a person based on their biometrical data. This mostly involves a database of biometric data with which the momentary information is compared until the most similar or same image is found. We search among N persons in the database so this way is called »1:N« or »One to many comparison«. With personal identification we look for a person's identity (e.g. name). In verification however, we ascertain if this is indeed the person they claim to be [6], so there is only one comparison (1:1). Since we know the person's name, we compare the data read by the sensor with the data stored in the database.

2.4. Fingerprint

Fingerprint recognition is the oldest form of all the biometric methods and they are secure from mutations. Fingerprint images are skin folders and furrows and have different details which can easily be read by a biometric module (Fig. 3.). Details are located on the end of furrows or on the joints of folders. The global images made by skin folders, furrows and details on a finger are different for each person and are therefore very adequate for recognizing a person. To recognize a fingerprint, approximately 100 bits are enough for detail searching methods, while high security systems store information in few Mbytes per image. We never store real fingerprints in the database. There is no possible way to recognize a person from the stored images without the use of special equipment. In correlation methods, the amount of data is higher.

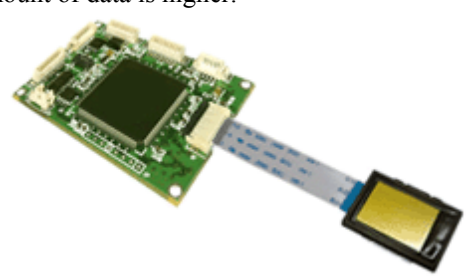

Fig.3. *Fingerprint Reader Module (Suprema Technical Manual, 2007)*

[10] AR (False Aceptance Rate); This can be expressed as a probability. For example, if FAR is 0.1 percent, it means that on average, one out of every 1000 impostors attempting to breach the system will be successful.

[11] FRR (False Recetion Rate); For example, if FRR is 0.05 percent, it means that on average, one out of every 2000 authorized persons attempting to access the system will not be recognized by that system.

3 RESULTS AND DISCUSSION

For the duration of research it is necessary to define reliability characteristics of RFID and biometric identification systems. Reliability characteristics of system components can be determined by testing, changing the functioning in the exploitation phases, catalogues and test reports or reference books (most known is the MIL HDBK 217[12]).

3.1. Reliability Parameters MTTF, MTBF of a RFID System Reader

$$\text{MTTF} = \int_0^\infty R(t)dt = \frac{1}{n}\sum_{i=1}^{n} t_i = 76.5 \text{ days}$$

$$\text{MTBF} = \int_0^\infty R(t)dt = \frac{1}{n}\sum_{i=1}^{n} t_i = 78.6 \text{ days}$$

The failures that were considered for defining MTTF, MTTR and MTBF (See Table 1.) of a RFID system are the following:

- Failures in Software operating (reader can not read RFID Tags).
- Failures in Hardware operating (RFID reader/antenna, impossible programming of RFID Tags or Microchips).

3.2. Reliability parameters MTTF, MTBF of Biometric Identification Reader

$$\text{MTTF} = \int_0^\infty R(t)dt = \frac{1}{n}\sum_{i=1}^{n} t_i = 88.8 \text{ days}$$

$$\text{MTBF} = \int_0^\infty R(t)dt = \frac{1}{n}\sum_{i=1}^{n} t_i = 90.1 \text{ days}$$

The failures that were considered for defining MTTF and MTBF of a Biometric system are following (See Table 2).

- Failures in Software operating (impossible read or recognition of fingerprint images)
- Failures in Hardware operating (Biometric Reader, PCBs[13]).
- Failures as a consequence of sensor operating: FAR, FRR.

3.3. Failure Rate $\lambda(t)$ of RFID and Biometric Identification Systems

Reliability of the RFID module can be defined with the Failure Rate parameter λ(t) in different periods:

- early damaging period,
- period of normal functioning,
- period of ageing or exploitation.

To define Failure Rate the Weibull model was used. It can also be used for models where $\lambda(t)$ can not be illustrated by constant or linear functions. The reliability parameters were defined using graphic method (Weibull++7 Software) and the results of the graphic methods are presented on the following figures:

- Reliability Function $R(t)$ of RFID system by β=2.6535 (Fig. 4.).
- Failure rate $f(t)/R(t)$ of RFID system by β=2.6535 (Fig. 5.).
- Reliability Function $R(t)$ of BIOMETRIC system by β=2. 6024 (Fig.6.).
- Failure rate $f(t)/R(t)$ of BIOMETRIC system by β=2. 6024 (Fig. 7.).

3.3.1 Times to failures (see Table 1) of RFID identification system samples and corresponding appraisal

Pairs $\left[t_i, \hat{F}(t_i)\right]$ (See Table 3.) were drawn in the probability web of a chosen (Weibull) probability distribution.

Times to failures and belonging point estimations (Fig .4.) shown during the ageing period or exploitation phase of RFID system β=2.6535 (β >1).

[12] MIL HDBK 217 [10]; this military standard is used to estimate the inherent reliability of electronic equipment and systems based on component failure data. It consists of two basic prediction methods: Parts-Count Analysis and Part-Stress Prediction. The general failure model in MIL-HDBK-217 and Bellcore TR-332 is the form: $\lambda_P = \lambda_b \pi_Q \pi_E \pi_A$ [11].

[13] PCB (Printed Circuit Board) is used to mechanically support and electrically connect electronic components using conductive pathways, or traces, etched from copper sheets laminated onto a non-conductive substrate. Alternative names are printed wiring board (PWB), and etched wiring board. A PCB populated with electronic components is a printed circuit assembly (PCA), also known as a printed circuit board assembly (PCBA).

Measured time parameters to terminal damage of the RFID system (t_i, i=1,2,3):

Table 1. *MTTF - MTTR - MTBF for RFID System*

Ser. no.	Time to Failure[1]	Time to Failure[2]	Time to Failure[3]	MTTF	Average value
22345	13	139	48	66.7	76.5
22359	27	106	42	58.3	
22346	54	106	58	72.7	
22347	54	110	83	82.3	
22348	72	96	73	80.3	
22349	90	82	88	86.7	
22360	116	28	93	79.0	
22375	87	29	115	77.0	
22381	51	40	145	78.7	
22387	60	36	155	83.7	
Ser. no.	Service procedure trial[1]	Service procedure trial[2]	Service procedure trial[3]	MTTR	Average value
22345	1	1	1	1.0	2.1
22359	1	1	1	1.0	
22346	2	3	2	2.3	
22347	2	0	3	1.7	
22348	5	3	7	5.0	
22349	1	1	1	1.0	
22360	4	1	2	2.3	
22375	4	2	1	2.3	
22381	4	3	4	3.7	
22387	1	0	1	0.7	
Ser. no.	Time to repeated start[1]	Time to repeated start[2]	Time to repeated start[3]	MTBF	Average value
22345	14	140	49	67.7	78.6
22359	28	107	43	59.3	
22346	56	109	60	75.0	
22347	56	110	86	84.0	
22348	77	99	80	85.3	
22349	91	83	89	87.7	
22360	120	29	95	81.3	
22375	91	31	116	79.3	
22381	55	43	149	82.3	
22387	61	36	156	84.3	

Measured time parameters to terminal
damage of the biometric system (t_i, i=1,2,3):

Table 2. *MTTF - MTTR - MTBF fo BIOMETRIC System*

Ser. no.	Time to Failure[1]	Time to Failure[2]	Time to Failure[3]	MTTF	Average value
36365	53	89	88	76.7	88.8
36359	60	106	73	79.0	
36366	87	106	88	93.0	
36364	86	161	88	106.3	
36368	102	130	13	81.7	
36369	99	102	98	99.7	
36360	56	150	93	99.7	
36345	57	90	126	91.0	
36381	81	52	117	83.3	
36384	90	65	105	80.0	
Ser. no.	Service procedure trial[1]	Service procedure trial[2]	Service procedure trial[3]	MTTR	Average value
36365	1	1	1	1.0	1.2
36359	0	1	0	0.3	
36366	1	3	2	2.0	
36364	1	0	1	0.7	
36368	1	3	1	1.7	
36369	2	1	1	1.3	
36360	2	1	1	1.3	
36345	3	1	1	1.7	
36381	2	1	1	1.3	
36384	2	0	1	1.0	
Ser. no.	Time to repeated start[1]	Time to repeated start[2]	Time to repeated start[3]	MTBF	Average value
36365	56	90	89	77.7	90.1
36359	60	105	73	79.3	
36366	88	107	90	95.0	
36364	85	161	89	105.0	
36368	103	133	16	83.3	
36369	101	103	99	101.0	
36360	58	151	96	101.0	
36345	60	91	127	92.7	
36381	83	53	118	86.7	
36384	92	65	106	81.0	

3.3.1 Times to failures (see Table 1) of RFID identification system samples and corresponding appraisal

Pairs $[t_i, \hat{F}(t_i)]$ (See Table 3.) were drawn in the probability web of a chosen (Weibull) probability distribution.

Times to failures and belonging point estimations (Fig .4.) shown during the ageing period or exploitation phase of RFID system β=2.6535 (β >1).

Table 3. *Times to failures and belonging appraisal for RFID system*

Mean time to first failure (RFID)										
i	1	2	3	4	5	6	7	8	9	10
t_i	13	27	54	54	72	90	116	87	51	60
$\hat{F}(t)$	0.05	0.12	0.19	0.26	0.33	0.4	0.48	0.55	0.62	0.66

Mean time to second failure (RFID)										
i	1	2	3	4	5	6	7	8	9	10
t_i	139	106	106	110	96	82	28	29	40	36
$\hat{F}(t)$	0.05	0.12	0.19	0.26	0.33	0.4	0.48	0.55	0.62	0.66

Mean time to third failure (RFID)										
i	1	2	3	4	5	6	7	8	9	10
t_i	48	42	58	83	73	88	93	115	145	155
$\hat{F}(t)$	0.05	0.12	0.19	0.26	0.33	0.4	0.48	0.55	0.62	0.66

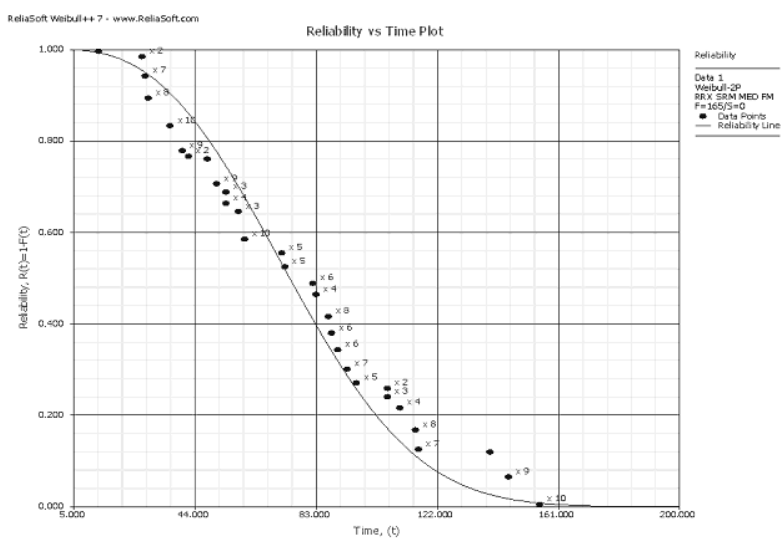

Fig. 4. *Reliability function of RFID system by ß=2.6535*

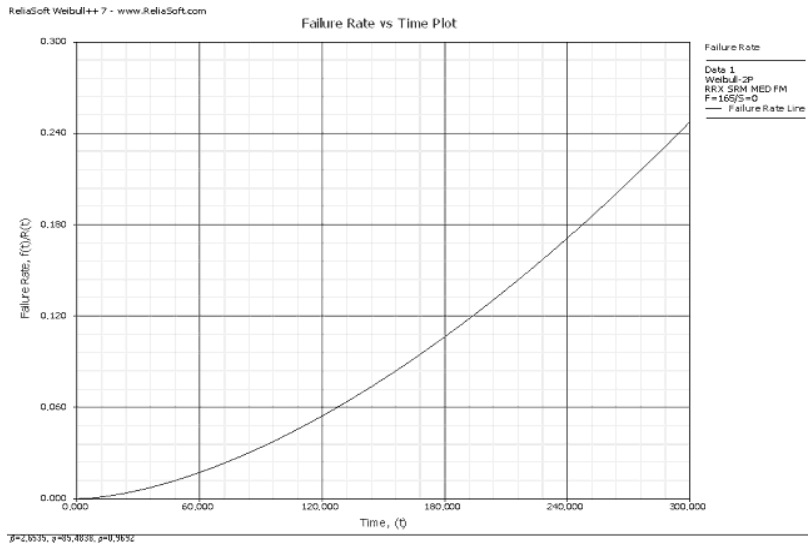

Fig.5. *Failure rate f(t)/R(t) of RFID system by ß=2.6535*

3.3.2 Times to failure (see Table 2.) of Biometric identification system samples and corresponding appraisal

Pairs $\left[t_i, \hat{F}(t_i)\right]$ (Table 4.) were drawn in the probability web of a chosen (Weibull) probability distribution.

Table 4. Times to failures and corresponding appraisal for BIOMETRIC system

Mean time to first failure(BIOMETRIC)										
i	1	2	3	4	5	6	7	8	9	10
t_i	53	60	87	86	102	99	56	57	81	90
$\hat{F}(t)$	0.05	0.12	0.19	0.26	0.33	0.4	0.48	0.55	0.62	0.66

Mean time to second failure (BIOMETRIC)										
i	1	2	3	4	5	6	7	8	9	10
t_i	89	106	106	161	130	102	150	90	52	65
$\hat{F}(t)$	0.05	0.12	0.19	0.26	0.33	0.4	0.48	0.55	0.62	0.66

Mean time to third failure (BIOMETRIC)										
i	1	2	3	4	5	6	7	8	9	10
t_i	88	73	88	88	13	98	93	126	117	105
$\hat{F}(t)$	0.05	0.12	0.19	0.26	0.33	0.4	0.48	0.55	0.62	0.66

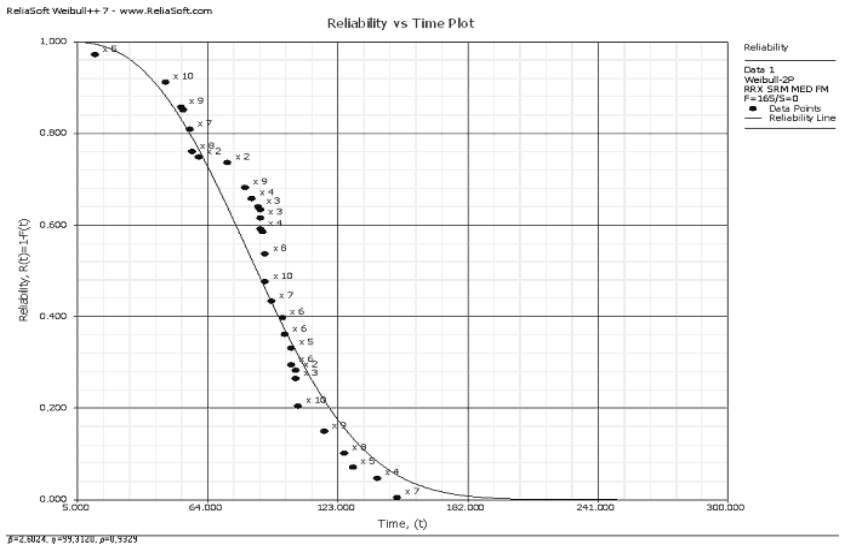

Fig. 6. *Reliability function R(t) of BIOMETRIC sytem by ß=2.6024*

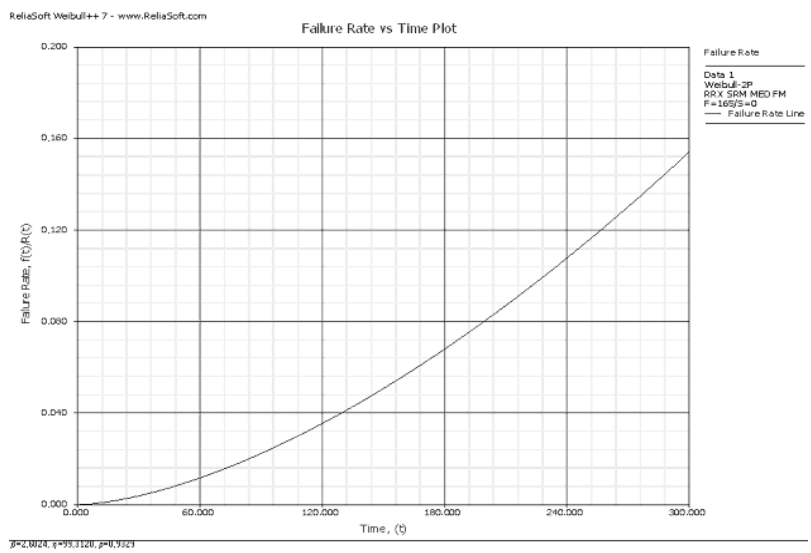

Fig. 7. *Failure rate f(t)/R(t) of BIOMETRIC system by ß=2.6024*

4 CONCLUSIONS

Biometric methods are becoming a very popular alternative to traditional identification systems in production-logistic processes where identification of people is necessary. Our research has shown that the ageing of biometric system begins later compared to RFID identification systems. The results indicate high availability the biometric identification systems and lower maintenance costs. There are many benefits to using biometric systems, such as no need for any additional identification elements. The use of biometric methods simplifies identification and increases reliability because biometric identification elements are not portable (fingerprints) and prevent non-authorized uses. Results of this research indicate the following:

1. better reliability of biometric systems regarding reliability parameters MTTF, MTBF and λ(t);

- MTTF of biometric systems are improved by 12.3 days.
- MTBF of biometric systems are improved by 11.5 days.
- The most critical parameter of the RFID systems – $\lambda(t)$, does not need to be considered in biometric systems. In a biometric system, there is no need for RFID cards or RFID tags for identification.

2. For biometric identification there is no need for RFID cards or tags which are the most critical parts in RFID Identification System. Experiments show that most cards fail within one year.
3. Time of servicing biometric readers is shorter than time of servicing RFID readers by an average of 1 day. This is a better result by 30% and consequently biometric systems have better availability.

4.1 Return of investment with optimizing production logistic

On the basis of the results of this research and customer feedback information, it can be concluded that the investment into automation of personal identification in the production-logistic processes is returned within 10 to15 months. The exact time depends on the degree of automation and the quantity of identification places). Of the many industrial branches these advantages and solutions will be a necessity for the pharmaceutical sector, where the processes must ensure safe distribution. Pharmaceutical companies have to deal with the problem of fake and altered medicaments (the estimated loss of is 75 billion dollars a year until 2010). According to predictions, biometric identification technology will reach vast rates of development. An indication of maturity of the biometric system is the amount of investments in the field. In the year 2002, the US government invested 16.63 million dollars into the biometric industry. The expected income of biometric industry in USA in 2007 was 153 million dollars. Expected growth of income between the years 2000 and 2007 is 67% [6].

5 SUMMARY AND FUTURE WORK

The usefulness of biometric systems is shown in production-logistic environment where personal identification is needed. From this research it is evident that the ageing period of biometric systems begins later compared to RFID (card identification) systems. The results also show that the availability of biometric identification systems is higher and therefore maintenance costs are lower. Functional and ergonomic advantages of biometry are clear because there is no need for any cards or other elements of identification in the production-logistic process. The use of biometric systems will make identification simple and at the same increase reliability due to non-transferability of identification elements (fingerprints) and prevent improper use. It can be expected that biometric technology will attain Slovenia in spite of doubts expressed by some institutions (office for personal data protection). Many open ethical questions arise, mostly on human personality, privacy and control. However researches such as this on reliability and availability unequivocally show that biometric technology has an advantage both in practical use and data safety.

Personal responsibility and accuracy in fields such as legislation, regulation adjustment, and production and supply chain management in global technical operations are more easily controlled using automated identification.

With the automation of identification there are also the possibilities of merging and comparing current process data with data from integral information systems (ERP, MRII, etc.) or other business applications.

6 REFERENCES

[1] Balantič, Z. (2006) Multimedia spiral architecture development for effective medical education. WSEAS Transactions on Computers, Athens, Greece, vol. 5, no. 10, 2293-2300.

[2] Bigun, E.S., Bigun, J., Duc, B., Fischer, S. (1997) Expert Conciliation for Multi Modal Person Authentication Systems by Bayesian Statistics. Personal Authentication, Crans-Montana, Switzerland, pp. 327-336.

[3] Hicklin, A., Watson, C., Ulery, B. (2005) The Myth of Goats: How many people have fingerprints that are hard to match? NIST Interagency Report 7271.

[4] Hudoklin, A., Rozman, V. (2004) Reliability and availability of systems human-machine. Publisher: Moderna organizacija, Kranj.

[5] Hong, L., Jain, A. (1998) Integrating Faces and Fingerprints for Personal Identification. IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 20, no. 12, pp. 1295-1307.

[6] Mraović, M. Biometric methodes in access control systems. University of Ljubljana, Faculty of Electrical Engineering, Ljubljana, Slovenia, 2003.

[7] Polajnar, A. (2005) Excellence of toolmaking firms : supplier - buyer - toolmaker: Collection of Conference consultation, Portorose, 11.-13. october 2005.

[8] Polajnar, A. (2003) Exceed limits on new way : supplier - buyer - toolmaker: Collection of Conference consultation, Portorose, 14.-16. october 2003.

[9] Kerr, J. What does »lean« really mean?. Special report, Logistics Management, 2006 URL: http://www.logisticsmgmt.com/article/CA6334579.html (acquired:17.05.2008).

[10] MIL-HDBK-217, Reliability Prediction of Electronic Equipment. U.S. Department of Defense URL:http://www.itemuk.com/milhdbk217.html (acquired: 12.05.2008)

[11] Jones, J. and Hayes, J. (1999) A Comparison of Electronic-Reliability Prediction Models. IEEE Transactions on Reliability, vol. 48, no. 2, pp. 127-134.