Nitric Acid Revamp and Upgrading of the Alarm & Protection Safety System at Petrokemija, Croatia

KUI – 6/2012
Recieved May 30, 2011
Accepted December 16, 2011

N. Zečević,[a*] *I. Hoško,*[a] *and S. Pavlaković*[b]

[a] Petrokemija d. d., Fertilizer Production, Kutina, Croatia
[b] Siemens d. d. Zagreb, Croatia

Every industrial production, particularly chemical processing, demands special attention in conducting the technological process with regard to the security requirements. For this reason, production processes should be continuously monitored by means of control and alarm safety instrumented systems. In the production of nitric acid at Petrokemija d. d., the original alarm safety system was designed as a combination of an electrical relay safety system and transistorized alarm module system. In order to increase safety requirements and modernize the technological process of nitric acid production, revamping and upgrading of the existing alarm safety system was initiated with a new microprocessor system. The newly derived alarm safety system, Simatic PCS 7, links the function of "classically" distributed control (DCS) and logical systems in a common hardware and software platform with integrated engineering tools and operator interface to meet the minimum safety standards with safety integrity level 2 (SIL2) up to level 3 (SIL3), according to IEC 61508 and IEC 61511. This professional paper demonstrates the methodology of upgrading the logic of the alarm safety system in the production of nitric acid in the form of a logical diagram, which was the basis for a further step in its design and construction. Based on the mentioned logical diagram and defined security requirements, the project was implemented in three phases: analysis and testing, installation of the safety equipment and system, and commissioning. Developed also was a verification system of all safety conditions, which could be applied to other facilities for production of nitric acid. With the revamped and upgraded interlock alarm safety system, a new and improved safety boundary in the production of nitric acid was set, which created the foundation for further improvement of the production process in terms of improved analysis.

Keywords: *Nitric acid production, alarm safety system, revamping*

Introduction

The industrial process of nitric acid production is a very demanding process from the standpoint of security requirements. Special attention must be given to power recovery in the turboset and reactor section. The turboset is a mechanical device for the rotation of air and the nitrous oxide compressors. In the reactor section, special precautions must be taken regarding the exothermal oxidation reactions in the gaseous mixture of ammonia and air. In order to prevent disastrous unintended consequences and hazards, the nitric acid production process must be continuously monitored with the help of control and alarm safety instrumented systems. A control system is deemed safety-related if it provides functions that significantly reduce the risk of a hazard, and in combination with other risk reduction measures reduces the overall risk to a tolerable level. These functions are known as safety functions of the system or device, and are able to prevent initiation of a hazard or detect the onset of one, in order to take the necessary actions to terminate the hazardous event, achieve a safe state, or mitigate the consequences of a hazard. All elements of the system, which are required to perform the safety function, including utilities, are safety-related and should be considered part of the safety-related system. Due to the unreliability of the originally installed alarm safety system in nitric acid production at Petrokemija d. d., which consisted of electrical relay safety system and transistorized alarm modules, it had to be revamped and upgraded with a new microprocessor system. Replacement of the existing system consisted of three phases, i.e. the analysis and testing phase, implementation and operation, and maintenance. All three phases were conducted in compliance with the international standards IEC 61508 and IEC 61511, the standards for the functional safety of safety-instrumented systems.[1,2] In the analysis phase, the existing and potential new safety risks were identified. According to the results of these analyses, the architecture of the logical system was made in the shape of a logical diagram, which was the basis for the safety requirements specification of the safety-instrumented system. By means of the safety requirements specifications, and the hazard and operability method,[3] the required safety integrity level was defined as a measure of risk reduction that the safety instrumented functions have to deliver. The

* Corresponding author: Nenad Zečević, dipl. inž.,
e-mail: nenad.zecevic@petrokemija.hr

analysis phase was the basis for selection of hardware architecture and related software for implementing safety functions. The newly selected alarm safety system was Simatic PCS 7 with a safety matrix, which enables safety lifecycle management for safety applications up to safety integrity level 3. The alarm system was developed in accordance with the guidance prescribed in the EEMUA 191[4] and CHID Circular CC Tech safety 9.[5] After the phase of designing and planning, followed the phase of installation, testing, staff training, commissioning, and validation of the nitric acid facility. The installed alarm safety system also became the basis for the second phase of revamping and upgrading the control system, which is still conducted by means of a pneumatic control system.

Experimental

With respect to the existing P&I diagrams of the nitric acid plant, first of all the existing and potential hazardous risks in the production process of the facility were identified, followed by the procedure of the hazard and operability method. On the basis of the identified hazardous risk situations, a logical diagram was made which served for preparation of the safety *cause&effect* matrix[6] and determination of the safety integrity level. The functioning of the logical diagram was first checked with the help of very simple free software, Cedar LS. Cedar LS is an interactive digital logic simulator used in digital logic design classes, or for testing simple digital designs. It features both low-level logic objects, as well as some register-level functions. After the phase of analyzing and testing all the possible hazardous situations and determining the required safety integrity level with the help of safety instrumented functions and risk graph, an alarm safety system was selected. The system consists of 3 kVA ($\cos(\varphi) = 0.9$, 2700 W) uninterruptible power supply with autonomy of 30 min, two redundant central process units CPU 417-4H with integrated safety function, 4 I/O racks ET200M with redundant profibus DP interface whose details are presented in Table 1, industrial ethernet (system bus, terminal bus), and operator interface in the shape of combined operator/engineering station and operator station.

In the erection phase, the old Praxis electrical-relay safety system and transistorized alarm modules system were replaced with the mentioned system. This was followed by the phase of cold and real testing in which the verification system of all safety conditions was implemented. The final phase was staff training for performing the tasks with the new operator interface.

Results and discussion

The originally installed alarm safety system was a combination of an electrical relay safety system and a transistorized alarm module system designed by the company Praxis. According to the safety requirements in the 1960's, this alarm safety system facilitated the following functions: logic inputs and outputs for the first failure sequence, motor off operation, control by normal open contact, and alarm signal repetition with visual and sound control.

The old system does not have the necessary diagnostic tools for determination of the first failure sequence and it was therefore almost impossible to carry out corrective measures in case of malfunction. At the same time, the overall maintenance of the equipment was very difficult due to the lack of adequate spare parts. In order to increase the safety requirements and modernize the technological process of nitric acid production, revamping and upgrading of the exi-

Table 1 – *Details of the I/O racks ET200M with redundant profibus DP interface*

Tablica 1 – *Tehničke karakteristike I/O modula ET200M s redundantnim komunikacijskim protokolom "profibus" i sučeljem DP*

No. of the I/O rack ET200M Red. br. modula I/O ET200M	Properties of the rack Tehničke karakteristike modula	No. of the modules/ signals Broj modula/ signala
Rack 1 Modul 1	failsafe digital input SM 326 F-DI 24 × DC 24 V; 1 × 40 PIN sigurnosni digitalni ulaz SM 326 F-DI 24 × DC 24 V; 1 × 40 PIN	4/96
	failsafe digital output SM 326 F-DO 10 × DC 24 V / 2 A PP; 1 × 40 PIN sigurnosni digitalni izlaz SM 326 F-DO 10 × DC 24 V/2 A PP; 1 × 40 PIN	4/40
	failsafe analog input SM 336 6 AI; 15 BIT; 1 × 20 PIN sigurnosni analogni ulaz SM 336 6 AI; 15 BIT; 1 × 20 PIN	1/6
Rack 2 Modul 2	standard digital input SM 321 32 DI; 24 V DC; 1 × 40 PIN standardni digitalni ulaz SM321 32 DI; 24 V DC; 1 × 40 PIN	4/128
	standard digital output SM 322 32 DO; 24 V DC, 0.5 A; 1 × 40 PIN standardni digitalni izlaz SM 322 32 DO; 24 V DC, 0,5 A; 1 × 40 PIN	2/64
	standard analog input SM 331 8 AE; ± 5 / 10 V, 1 – 5 V, ± 20 mA, 0 / 4 to 20 mA 1 × 40 PIN standardni analogni ulaz SM 331 8 AE; ± 5 / 10V, 1 – 5 V, ± 20 mA, 0 / 4 to 20 mA 1 × 40 PIN	3/24
	standardni analogni izlaz SM 332 8 AO; U/I; 1 × 40 PIN standard analog output SM 332 8 AO; U/I; 1 × 40 PIN	1/8
Rack 3 Modul 3	standard analog input SM 331 8 AI thermocouple / 4 AI Pt100; 1 × 20 PIN for EX areas standardni analogni ulaz SM 331 8 AI termočlanak / 4 AI Pt100; 1 × 20 PIN za zone EX	3/24
Rack 4 Modul 4	standard analog input SM 331 8 AI thermocouple / 4 AI Pt100; 1 × 20 PIN for EX areas standardni analogni ulaz SM 331 8 AI termočlanak / 4 AI Pt100; 1 × 20 PIN za zone EX	3/24

sting alarm safety system was initiated with the new microprocessor system. The main role of the process engineer was to determine all the possible security requirements and safety standards in the production of nitric acid that could trigger hazardous situations. This was achieved in the analysis phase in which the logical diagram was built. The derived logical diagram was the foundation for all other tasks. Taking into consideration the security conditions of the old alarm safety system and all other process conditions in the nitric acid production plant, two different sets of defects were identified: defects I and II. Defects I represent the most serious defects in the production of nitric acid, after which the emergency shutdown procedure of the whole process (turboset and process unit) must be conducted as soon as possible. In the case of defects II, the procedure of the process unit's shutdown must be first implemented, while the power recovery by the turboset may stay running for 3 minutes in order to ensure proper blowdown of the all parts of the equipment and pipes in the nitric acid production process unit. The onset of defects I or II will cause appropriate security effects in the production of nitric acid. This will cause the protection of process equipment and process staff in order to avoid every possible hazardous situation. Table 2 shows the main causes and effects, which bring about the emergency shutdown sequence. Table 3 depicts the same for a normal shutdown sequence. Each cause will automatically trigger simultaneously all the effects listed in the right column of Table 2 and Table 3.

Besides the mentioned protection and safety causes and effects, the alarm states, trips and interlocks for process parameters are also recognized, which must be a forewarning to the operator to take necessary action to prevent unwanted shutdown effects. The alarm system is designed according to all the standard conditions and is equipped with audible and visual signs, proper alarm lists, etc. Protective tripping system is designed as a defence against any excursions beyond the safe operating limits. At the same time, it detects any excursions beyond the set points related to safe operating limits (i.e. the onset of a hazard) and acts promptly to maintain or restore the equipment under control to a safe state.

T a b l e 2 – *The main causes and effects which initiate the emergency shutdown procedure in the production of nitric acid*
T a b l i c a 2 – *Glavni uzroci nužnih postupaka obustave proizvodnje dušične kiseline i s njima povezane posljedice*

Possible causes Mogući uzroci	Effects Posljedice
emergency STOP pushbutton in the control room tipkalo za nuždu STOP u komandnoj sobi	1. closing of the two electrical solenoid valves of gaseous ammonia pipe and opening of the start-up relief valve before it zatvaranje dvaju električnih solenoidnih ventila na cjevovodu plinovitog amonijaka i otvaranje odušnog ventila ispred njih
emergency STOP pushbutton at the local control panel of turboset tipkalo za nuždu STOP na lokalnoj komandnoj ploči turboseta	2. closing of the extraction valve of nitric acid from absorption tower zatvaranje ventila za crpljenje kiseline iz apsorpcijske kolone
electrical power failure nestanak električne energije	3. closing of the quenching water inlet valve before steam superheaters zatvaranje ulaznog ventila vode za hlađenje pare prije predgrijača
steam turbine overspeed prekoračenje brzine vrtnje parne turbine	4. stop of recirculation pump for steam superheaters zaustavljanje recirkulacijske crpke za predgrijače pare
tailgas turbine overspeed prekoračenje brzine vrtnje plinskog ekspandera	5. emergency shutdown procedure of the turboset, quick trip, which consists of: nužna obustava rada turboseta koju čine:
axial displacement of air compressor rotor aksijalni pomak rotora zračnog kompresora	5.1. closing the steam inlet valve for steam turbine zatvaranje ulaznog ventila pare za parnu turbinu
axial displacement of nitrous gas compressor rotor aksijalni pomak rotora kompresora dušikovih oksida	5.2. opening the relief valve of air compressor to the atmosphere otvaranje ventila za rasterećenje zračnog kompresora prema atmosferi
axial displacement of steam turbine rotor aksijalni pomak rotora parne turbine	5.3. opening the relief valve of nitrous gas compressor to the atmosphere otvaranje ventila za rasterećenje kompresora dušikovih oksida prema atmosferi
axial displacement of tailgas turbine rotor aksijalni pomak rotora plinskog ekspandera	5.4. closing the inlet valve for tail gas turbine zatvaranje ulaznog ventila za plinski ekspander
low pressure of lubrication oil for the turboset nizak tlak ulja za podmazivanje turboseta	5.5. opening the by-pass valve of tail gas turbine for its relief otvaranje obilaznog ventila za rasterećenje plinskog ekspandera
too low pressure in the steam turbine condenser prenizak tlak u kondenzatoru parne turbine	6. closing of the control valve of liquid ammonia for the $DeNO_x$ system – the cause marked with ** triggers only this effect zatvaranje kontrolnog ventila tekućeg amonijaka za sustav za uklanjanje NO_x – uzrok označen s ** izaziva samo ovu posljedicu
low temperature of tail gas before the $DeNO_x$ reactor** niska temperatura otpadnog plina prije reaktora za uklanjanje NO_x**	
low temperature of tail gas after the tailgas turbine** niska temperatura otpadnog plina nakon plinskog ekspandera**	

T a b l e 3 – *Main causes and effects which initiate normal shutdown procedure in the production of nitric acid*
T a b l i c a 3 – *Glavni uzroci i posljedice koji uzrokuju normalni postupak obustave proizvodnje dušične kiseline*

Possible causes Mogući uzroci	Effects Posljedice
very high level of liquid ammonia in the ammonia evaporator vrlo visoka razina tekućeg amonijaka u isparivaču amonijaka	1. closing of the two electrical solenoid valves at the pipe of gaseous ammonia and opening of the start-up relief valve before it zatvaranje dvaju električnih solenoidnih ventila na cjevovodu plinovitog amonijaka i otvaranje odušnog ventila ispred njih
high pressure of gaseous ammonia after ammonia evaporator visok tlak plinovitog amonijaka nakon isparivača amonijaka	2. closing of the extraction valve of nitric acid from the absorption tower zatvaranje ventila za crpljenje kiseline iz apsorpcijske kolone
low pressure of air for the oxidation with gaseous ammonia nizak tlak zraka za oksidaciju s plinovitim amonijakom	3. closing of the quenching water inlet valve before the steam superheaters zatvaranje ulaznog ventila vode za hlađenje pare prije predgrijača
malfunction of the boiler feed water recirculation jackets of the burners kvar u cirkulaciji kotlovske vode za vodene džepove reaktora	4. stop of recirculation pump for steam superheaters zaustavljanje recirkulacijske crpke za predgrijače pare
malfunction of boiler recirculation feed water in the boiler kvar u cirkulaciji napojne vode za kotao	5. normal shutdown procedure of the turboset after 3 min, slow trip, which consists of: nužna obustava rada turboseta nakon 3 min koju čine:
very high level of nitric acid in the separator before the inlet of nitrous gas compressor vrlo visoka razina dušične kiseline u odvajaču prije ulaza u kompresor dušikovih oksida	5.1. closing the steam inlet valve for steam turbine. zatvaranje ulaznog ventila pare za parnu turbinu
low pressure of cooling water nizak tlak rashladne vode	5.2. opening the relief valve of air compressor to the atmosphere otvaranje ventila za rasterećenje zračnog kompresora prema atmosferi
low pressure of instrumental air nizak tlak instrumentnog zraka	5.3. opening the relief valve of nitrous gas compressor to the atmosphere otvaranje ventila za rasterećenje kompresora dušikovih oksida prema atmosferi
high temperature of catalytic gauzes visoka temperatura katalizatorskih mreža	5.4. closing the inlet valve for tail gas turbine zatvaranje ulaznog ventila za plinski ekspander
normal STOP pushbutton in the control room tipkalo STOP za normalnu obustavu u komandnoj sobi	5.5. opening the by-pass valve of tail gas turbine for its relief otvaranje obilaznog ventila za rasterećenje plinskog ekspandera
normal STOP pushbutton on the local control panel of turboset tipkalo STOP za normalnu obustavu na lokalnoj kontrolnoj ploči turboseta	6. closing of the control valve of the liquid ammonia for the $DeNO_x$ system – the cause marked with ** triggers only this effect zatvaranje kontrolnog ventila tekućeg amonijaka za sustav za uklanjanje NO_x – uzrok označen s ** izaziva samo ovu posljedicu
low temperature of tail gas before the $DeNO_x$ reactor** niska temperatura otpadnog plina prije reaktora za uklanjanje NO_x**	
low temperature of tail gas after the tailgas turbine** niska temperatura otpadnog plina nakon plinskog ekspandera**	

Trips are not self-resetting unless adequate justification has been made. Protective interlocks are conducted to prevent those control actions, which might initiate a hazard from being undertaken, by an operator or process control system, and are by nature self-resetting. The possible alarm states, trips and interlocks are presented in Table 4. The list of alarm states, trips and interlocks refers to the common states for both production lines and for each separately. Regarding the phase of analysis of all the possible hazardous process states in the nitric acid production, which have been identified until now, a logical diagram was made. It determines the recognized causes and consequential safety effects of the security equipment and devices.

The constructed logical diagram is shown in Fig. 1, in which every possible hazardous state, shown in Table 2 and Table 3, is clearly represented. These possible causes were implemented into an interactive digital logic simulator, Cedar LS, in order to verify the correctness and performance of the constructed logical diagram. After the phase of testing the logical diagram, the safety integrity level in the selection process was determined using the safety instrumented functions and risk graph technique[7,8,9,10,11] in a systematic team approach. First of all, the list of the safety-instrumented functions[12] was analyzed and identified. In nitric acid production, in compliance with the prescribed safety instructions, the following safety instrumented functions were identified:

1. Consequence severity of an accident being prevented – C function
2. Pre-safeguard likelihood of an accident – W function
3. Occupancy in the hazardous zone – F function
4. Probability of avoiding a hazardous event – P function

The required risk reduction can take place by any combination of safeguards, either instrumented or non-instrumented. The required risk reduction is a value that defines the

T a b l e 4 – *List of the alarm states, interlocks and trips for common situations and for each production line separately*

T a b l i c a 4 – *Popis zajedničkih i pojedinih uzbunjujućih stanja, međustanja i blokirajućih stanja na postrojenju za proizvodnju dušične kiseline*

Possible alarms, trips and interlocks Mogući alarmi, međustanja i blokadna stanja	Processing of the alarms, trips and interlocks Obrada alarma, međustanja i blokadnih stanja
low and high level of liquid ammonia in the ammonia evaporator niska i visoka razina tekućeg amonijaka u isparivaču amonijaka	
low temperature of gaseous ammonia after ammonia evaporator niska temperatura plinovitog amonijaka nakon isparivača amonijaka	
high temperature of high pressure steam after heat superheater visoka temperatura visokotlačne pare nakon pregrijača pare	
clogging of oil filter in the turboset oil system začepljenje uljnog filtra u uljnom sustavu turboseta	
high temperature of oil in the turboset oil system visoka temperatura ulja u uljnom sustavu turboseta	audio and visual warnings with the necessary information as: zvučna i vidljiva upozorenja s neophodnim informacijama izražena kao: 1. alarm condition uzbunjujući uvjet 2. part of the plant affected dio ugroženog postrojenja 3. description of the required action opis potrebne preventivne radnje 4. alarm priority prvenstvo uzbune 5. time of alarm vrijeme uzbune 6. status of alarm stanje uzbune 7. grouping and first-up alarms grupiranje prvih uzbuna 8. eclipsing the lower grade alarms (e.g. suppression of the high alarm when the high-high activates) potiskivanje uzbuna manje važnosti (npr. gašenje uzbuna velike važnosti kada se uključi uzbuna vrlo velike važnosti) 9. suppression of the out-of-service plant alarms gašenje alarma ako postrojenje ne radi 10. suppression of the selected alarms during certain operating modes gašenje odabranih uzbuna tijekom određenih načina rada 11. automatic alarm load shedding and shelving automatsko popunjavanje uzbunjujućih stanja
high level of condensate in the steam turbine condenser visoka razina kondenzata u kondenzatoru parne turbine	
low pressure of instrumental air nizak tlak instrumentnog zraka	
low temperature of catalytic gauzes in the burners niska temperatura katalizatorskih mreža u gorionicima	
low and high level of boiler feed water in the steam drum niska i visoka razina kotlovske vode u parnom domu	
low and high level of nitric acid in the bleaching tower niska i visoka razina dušične kiseline u koloni za bijeljenje	
low level of nitric acid in the oxidation tower niska razina dušične kiseline u koloni za oksidaciju	
high level of nitric acid in the separator at the inlet of nitrous gas compressor visoka razina dušične kiseline u odvajaču na ulazu u kompresor dušičnih plinova	
low and high level of nitric acid in the absorption tower niska/visoka razina dušične kiseline u koloni za apsorpciju	
low/high level of nitric acid in the condenser of the weak nitric acid niska/visoka razina dušične kisline u kondenzatoru razrijeđene dušične kiseline	
low volume flow of demineralised water for the absorption tower mali protok demineralizirane vode u koloni za apsorpciju	
low pressure of high and low pressure steam nizak tlak visokotlačne ili niskotlačne pare	
low level of boiler feed water in the deaerator niska razina kotlovne vode u otplinjaču	
low and high level of nitric acid in the nitric acid storage reservoirs niska/visoka razina dušične kiseline u spremnicima dušične kiseline	
malfunction of the boiler feed steam pump kvar crpke kotlovne vode	
malfunction of nitric acid pump for end users kvar crpke dušične kiseline za krajnje korisnike	
malfunction of nitric acid circulation pump through the oxidation tower kvar crpke za cirkulaciju dušične kiseline u koloni za oksidaciju	
malfunction of the extraction pump for weak nitric acid from the weak nitric acid condenser kvar crpke za crpljenje razrijeđene dušične kiseline iz kondenzatora razrijeđene dušične kiseline	
malfunction of the extraction pump for the condensate from the steam turbine condenser kvar crpke za crpljenje kondenzata iz kondenzatora parne turbine	
malfunction of the boiler feed water circulation pump kvar crpke za cirkulaciju kotlovne vode	
malfunction of the nitric acid circulation pump through absorption tower kvar crpke za cirkulaciju dušične kiseline kroz kolonu za apsorpciju	
malfunction of the demineralised water pump for absorption tower kvar crpke demineralizirane vode	
low and high temperature of all process streams (air, ammonia, nitric acid, steam, etc.) niska/visoka temperatura u svim procesnim tokovima (zrak, amonijak, dušična kiselina, para, itd.)	

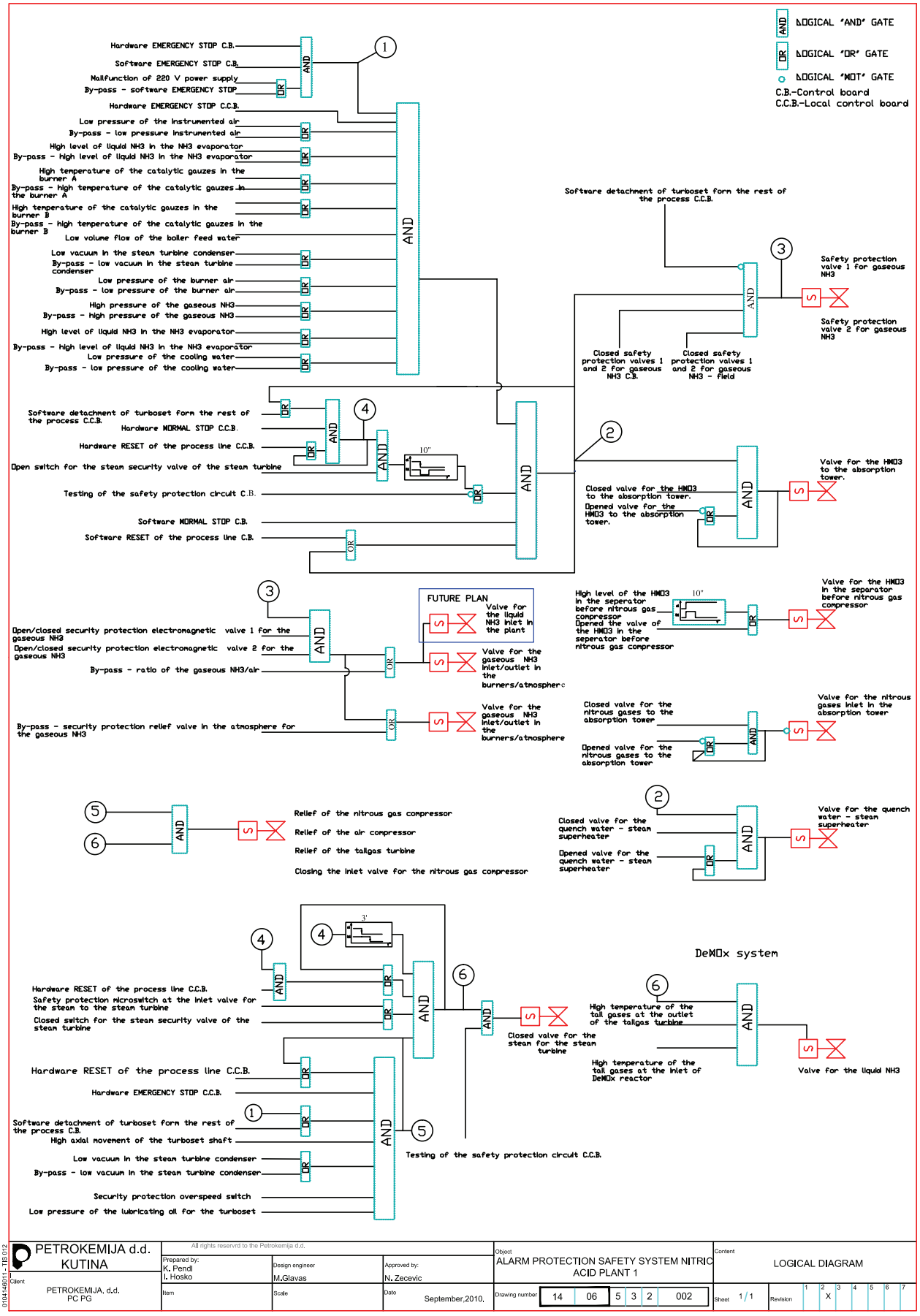


Fig. 1 – *Constructed logical diagram of the alarm safety system in the nitric acid production of Petrokemija d. d.*

Slika 1 – *Izvedeni logički dijagram uzbunjujuće-sigurnosno-blokirajućeg sustava u proizvodnji dušične kiseline Petrokemije d. d.*

number of order-of-magnitude decreases in either the consequence severity or likelihood of the unwanted accident that are required. The required risk reduction was typically accomplished using a combination of instrumented and non-instrumented safeguards. In order to find out what amount of risk reduction was required from the safety instrumented function, one must know the total amount of risk reduction provided by the other protection layers. This was accomplished by summing the number of independent protection layers that were available to prevent the hazard.

An independent protection layer was defined as a specific safeguarding category. Independent protection layers were evaluated and must meet all the following criteria to be utilized in the SIL selection process:

Specificity – An independent protection layer must be specifically designed to prevent the consequences of one potentially hazardous event.

Independence – The operation of the protection layer must be completely independent from all other protection layers, no common equipment can be shared with other protection layers.

Dependability – The device must be able to dependably prevent the consequence from occurring. Both systematic and random faults need to be considered in its design. The probability of failure of an independent protection layer must be demonstrated to be less than 10 %.

Audit ability – The device should be proof tested and maintained. These audits of operation are necessary to ensure that the specified level of risk reduction is being achieved.

Some common independent layers of protection utilized on the project included: coaxial piping systems, relief valves, check valves, electromagnetic valves and operator response. Once the independent protection layers were identified, the total number of protection layers represents the amount of risk reduction that was provided by non-safety instrumented system means. The difference between the risk reduction provided by the independent protection layers and the required risk reduction that was determined from Table 4 and Fig. 2 is the risk reduction contribution that must be provided by the safety instrumented function. The SIL that is assigned to a safety instrumented function protecting against a specific hazard is then the difference between the required risk reduction determined from the pre-safeguard risk ranking and the number of independent protection layers:

$$\text{SIL} = \begin{matrix}\text{required risk} \\ \text{reduction}\end{matrix} \_ \begin{matrix}\text{number of independent} \\ \text{protection layers}\end{matrix}$$

If the SIL calculated using the equation above is either zero or negative, then a safety instrumented function was not required for risk reduction purposes. If the calculated SIL was greater than 2, then it was felt that an expert should review the scenario. In Table 5 the values of the determined safety instrumented functions are given, from which the safety integrity level of the nitric acid process at Petrokemija was determined with the help of the risk graph technique presented in Fig. 2.

According to the determined safety instrumented functions from Table 5 and risk graph in Fig. 2, it can be concluded

Table 5 – *Description of the determined safety instrumented functions in the nitric acid production at Petrokemija d. d.*

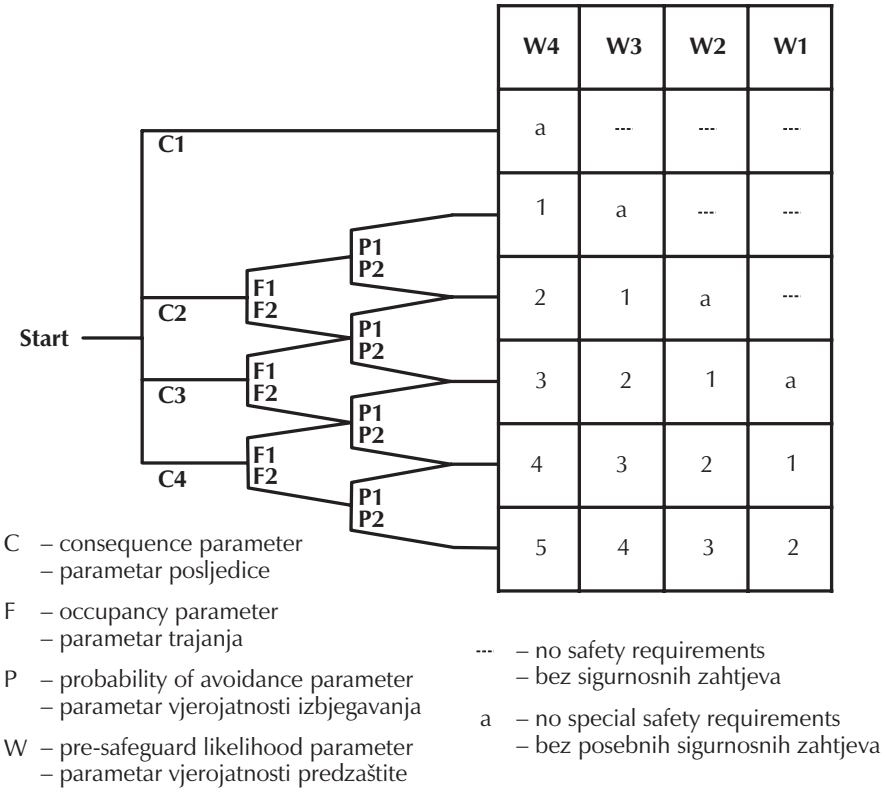
Tablica 5 – *Određene vrijednosti sigurnosnih instrumentnih funkcija u proizvodnji dušične kiseline u Petrokemiji d. d.*

Vrijednost sigurnosne instrumentne funkcije Category of safety instrumented function	Opis Description
C_2	no-lost-time injury or occupational illness zabilježene ozljede ili profesionalna oboljenja, bez izgubljena vremena
W_4	expected to occur frequently (e.g. once a month) očekivanje da se često pojavljuju (npr. jedanput mjesečno)
F_1	rare to more frequent exposure in the hazardous zone rijetko do učestalo izlaganje u opasnoj zoni
P_1	possible under certain conditions moguće pod određenim uvjetima

that in the nitric acid production at Petrokemija d. d. the safety integrity level is 1. This means that the probability of failure on demand is between 10^{-2} and 10^{-1} per year with risk reduction factor between 10 to 100.[13]

Based on the constructed logical diagram, determined safety integrity level, numbers of the digital and analog outputs and inputs, necessary electrical power supply and operator interface for achieving the best alarm processing conditions, the Simatic PCS 7 system was chosen to replace the old electrical relay safety and transistorized alarm system. The chosen alarm safety system implemented the safety *cause&effects* matrix. The *cause&effect* method has proven to be an extremely effective option for the description of safety functions and definition of marginal and shutdown conditions. The method specified by the American Petroleum Institute in the API RP 14C guideline, is currently employed in many sectors of the processing industry. The safety matrix can manage the safety applications up to level 3, in accordance with IEC 61508 and IEC 61511. Therefore, it is obvious that the chosen system can be applied to every industrial process, which must fulfil safety requirements up to integrity level 3.

The base of the new system consists only of the necessary hardware and software platform for the implementation of all foreseen scenarios according to the previously described procedure. All process security conditions from tables 2, 3 and 4 and Fig. 1, were implemented in the safety *cause&effect* matrix, which is the basis of the new alarm safety system. Besides the main highlights and advantages of the safety matrix, the most acceptable condition for Petrokemija d. d. was the recognition of the first alarm responsible for the shutdown sequence, regardless of whether it begins with the emergency or normal shutdown procedure. Another very challenging demand and request was the implementation of the software solution for switching of indivi-



F i g. 2 – *Risk graph for determination of safety integrity level (SIL) from safety instrumented functions (SIF). C1 – no injury or occupational illness, first aid; C2 – no-lost-time injury or occupational illness; C3 – lost-time injury or occupational illness; C4 – death or severe occupational illness; W1 – not expected to occur during plant lifetime; W2 – expected to occur several times during plant lifetime; W3 – expected to occur once a year; W4 – expected to occur frequently (once a month); F1 – rare to more frequent exposure in the hazardous zone; F2 – frequent to permanent exposure in the hazardous zone; P1 – possible under certain conditions; P2 – almost impossible.*

S l i k a 2 – *Određivanje sigurnosne razine integriteta grafom rizika te sigurnosnim instrumentnim funkcijama. C1 – nema ozljeda ili profesionalnih oboljenja, prva pomoć; C2 – zabilježene ozljede ili profesionalna oboljenja bez izgubljena vremena; C3 – ozljede i profesionalna oboljenja s izgubljenim vremenom; C4 – smrt ili teška profesionalna oboljenja; W1 – ne očekuje se pojava tijekom radnog vijeka postrojenja; W2 – očekuje se pojava nekoliko puta tijekom radnog vijeka postrojenja; W3 – očekuje se pojava jedanput godišnje; W4 – učestalo pojavljivanje (jedanput mjesečno); F1 – rijetko ili često izlaganje u opasnom području; F2 – učestalo do stalno izlaganje u opasnom području; P1 – moguće pod određenim uvjetima; P2 – gotovo nemoguće.*

dual process causes during the start-up procedure, which were originally solved through the hardware by-pass. Namely, during the start-up procedure, some of the possible process causes from Table 3 must be by-passed until the proper process conditions are accomplished. It is allowed to switch off the by-pass of the causes and put their function into the alarm safety system to trigger the protection effect, only after reaching adequate process values of the corresponding process causes. The problem was solved by handling of by-pass conditions as easy as possible in a way that the original hardware switching operator interface was copied to the virtual one, taking all the advantages of the software tool and safety *cause&effect* matrix. In the installation and commissioning phase, the old alarm safety system was replaced, which involved the following:

1. Replacement of the 110 V uninterrupted power supply with a new one of 230 V AC;

2. Replacement of the 230 V AC to 110 V DC power supply with that of 230 V AC to 24 V DC:

3. Replacement of all 110 V DC electrical solenoids with those of 24 V DC, approved by the EX Agency;

4. Replacement of the electrical relay safety system with the Simatic PCS 7 AS 417-FH redundant system;

5. Replacement of the Praxis transistorized alarm system with the Simatic PCS 7 AS 417-FH redundant system;

6. Installation of the failsafe "yellow" I/O modules for the digital/analog outputs and inputs of the process variables;

7. Installation of the standard I/O modules for the digital/analog inputs and outputs of the process variables, including EX protection;

8. Replacement of all electrical supplies (wirings, fuses, communication cables, etc.);

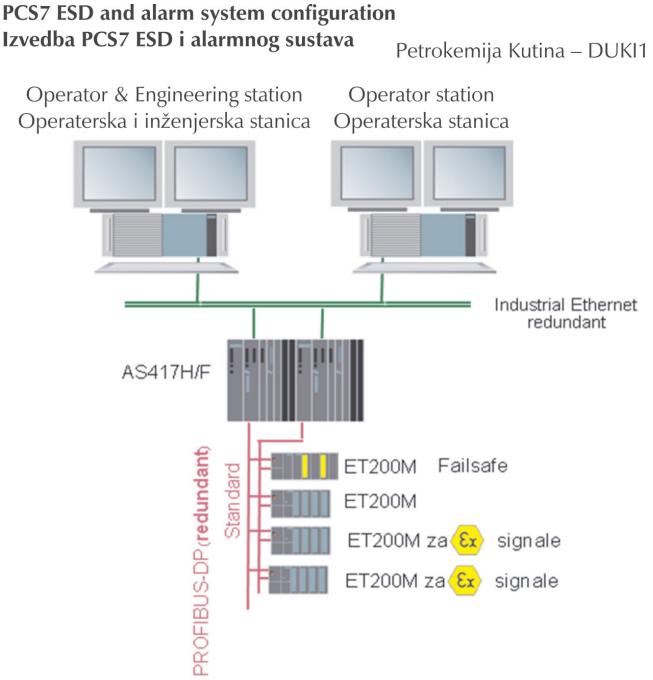
9. Software programming of the safety matrix with all possible causes and effects;

10. Configuration of the engineering/operator and operator stations (connection with the redundant CPU, failsafe "yellow" and standard I/O modules for the digital and analog inputs and outputs, defining the operator interface in the shape of process diagrams, alarm and working groups);

11. Connection of the erected system with the process safety equipment in the process field.

The block scheme of the newly installed alarm safety system is presented in Fig. 3. From Fig. 3 it can be seen that the control room was equipped with two control stations for operator interface, of which one is an engineering&opera-

tor station, while the other is only an operator station. The stations are connected through the industrial ethernet with two redundant central process units AS417H/F. The CPU is connected through redundant profibus with four ET200M modules, of which one is a failsafe module and other three are normal modules for digital and analog input and output of process parameters. After the installation and commissioning phase, the phase of cold and real testing of the newly derived alarm safety system followed. The phase of cold and real testing was divided into three steps. The first step was to check the emergency shutdown procedure, the second step was to check the normal shutdown procedure, whereas the third step was to check the alarm states, trips and interlocks of the process parameters (temperatures, levels) and process equipment (pumps, relief valves). All three mentioned steps were conducted simultaneously for cold and real conditions. The testing procedure of the alarm safety system consisted of the start-up of every possible cause listed in Table 2 and Table 3 and the logical diagram in Fig. 1, followed by checking, with the help of the derived safety *cause&effect* matrix, whether this cause triggered the necessary protection effect prescribed by the logical diagram. Verification of the triggered protection effect was also checked through appropriate action of the safety process equipment in the process field. During the phase of testing, the occurrence of the first alarm, responsible for the shutdown procedure, was also verified. By the same methodology, testing of all possible prescribed alarm states, interlocks and trips listed in Table 4 was conducted. All the tested causes and alarms triggered audio and visual warnings with the operation of all necessary actions in accordance with the EEMUA 191 – Alarm systems – a guide to design, management and procurement. The whole derived system was also tested against random hardware faults to check the redundant function of the central process unit and operator interface.



F i g. 3 – *Main hardware architecture of the newly installed alarm safety system SIMATIC PCS 7*

S l i k a 3 – *Izvedena arhitektura novopostavljenog uzbunjujuće-sigurnosno-blokirajućeg sustava Simatic PCS 7*

After testing, the phase of training and familiarizing the process staff with the new alarm safety system followed. The process staff, consisting of 20 operators of an average age of 51.2 years, had no experience with any other kind of microprocessor alarm safety or control system, either old or new generation. Therefore, the training was very challenging, but owing to the very friendly environment of the new system, especially the protection *cause&effect* matrix and the excellent knowledge of the nitric acid process, training was completed very successfully. A minor disadvantage of the new alarm safety system was overcome during the testing and training phase. Except for the commissioning of the alarm system, the foundations for the second phase of replacing the existing pneumatic control system with a modern one were also laid, using transformation of the current signal (4 to 20 mA) to pneumatic force for the movement of control valves. On this basis and with regard to the necessary conditions in the process field, the two cascade PID control circuits for managing the $DeNO_x$ system were implemented. The control system consists of a control valve and Coriolis magnetic flow-meter for dosing the liquid ammonia and continuous analysis of the NO_x volume concentration in the tail gases.

The entire project, from analysis to erection, commissioning, testing, validation and training lasted approximately one year, and was conducted by Petrokemija's process and maintenance staff. The phase of erection, testing and training was conducted in January 2011, lasting 25 working days, with the newly installed alarm system. Both production lines have been running successfully since the beginning of February 2011, with no malfunctions of the constructed alarm safety logic or/and equipment.

Conclusion

In accordance with good engineering practice, the revamping and upgrading of the existing alarm safety system with a new microprocessor system was conducted in the nitric acid production at Petrokemija d. d. The entire project was implemented in three phases, i.e. analysis and testing phase, implementation phase, and operation and maintenance phase. With the constructed architecture of the logical diagram of the nitric acid process, the minimum required safety integrity level was determined with the help of the safety instrumented functions and a risk graph technique. On this basis, a new alarm safety system was chosen, in the form of the Simatic PCS 7 system with the safety *cause&effect* matrix. Replacement of the electrical relay safety system and the transistorized alarm system with a microprocessor system was implemented using own know-how with the supervision of Siemens Croatia. The newly installed system was successfully tested and verified in accordance with the determined safety requirements and put into real process conditions with no malfunction. The proposed system of testing performance of the erected alarm safety system on the logical diagram basis, may serve its implementation in other nitric acid plants. The successful execution of the alarm safety system also laid the foundations for the second phase of revamping and upgrading of the nitric acid process in Petrokemija d. d. in the segment of replacing the existing pneumatic control system with a microprocessor system of the last generation.

List of abbreviations
Popis kratica

CPU – central process unit
– središnja procesorska jedinica

DCS – distributed control system
– raspodijeljeni sustav upravljanja

EX – explosive
– eksplozivno

I/O – input/output
– ulaz/izlaz

SIL – safety integrity level
– razina cjelovitosti sigurnosti

SIF – safety instrumented function
– instrumentna sigurnosna funkcija

P&I – process&instrumental
– procesno & instrumentno

References
Literatura

1. Functional safety of electrical/electronic/programmable safety-related systems, IEC/TR 61508-0, Ed. 1.0, International Electrotechnical Commision, 2005.
2. Functional safety: Safety Instrumented Systems for the process industry sector, IEC/TR 61511-0, Ed. 1.0, International Electrotechnical Commision, 2004.
3. *F. Crawley, M. Preston, B. Tyler,* HAZOP: Guide to Best Practice, 2nd Ed., IChemE, Rugby, 2008.
4. EEMUA 191 Alarm systems – a guide to design, management and procurement, The Engineering Equipment and Materials Users' Association, London, 2007.
5. CHID Circular CC/Tech/Safety/9 Alarm systems guidance for CHID inspectors, UK Health and Safety Executive, 2011.
6. API RP 14C (R2007) – Recommended Practice for Analysis, Design, Installation, and Testing of Basic Surface Safety Systems for Offshore Production Platforms, Ed. 7.0, American Petroleum Institute, 2001.
7. ANSI/ISA S84.01-1996 – Application of Safety Instrumented Systems for the Process Industries, International Society for Measurement and Control, 1996.
8. SEMI S2-0200 Environmental, Health, and Safety Guideline for Semiconductor Manufacturing Equipment, SEMI, 2000.
9. SEMI S10-1296 – Safety Guideline for Risk Assessment, SEMI, 1996.
10. SEMI S14-0200 – Safety Guidelines for Risk Assessment and Mitigation for Semiconductor Manufacturing Equipment, SEMI, 2000.
11. *E. Marszal*, Guideline for the Selection of Safety Integrity Levels, Instrumentation, Systems, and Automation Society, 2002.
12. *M. D. Scott, K. O'Malley,* Identifying Required Safety Instrumented Functions For Life Safety Systems In The High-Tech And Semiconductor Manufacturing Industries, International Society of Automation, 2002.
13. *M. Charlwood, S. Turner, N. Worsell*, RR216 – A Methodology For The Assignment Of Safety Integrity Levels (Sils) To Safety-Related Control Functions Implemented By Safety-Related Electrical, Electronic And Programmable Electronic Control Systems Of Machines, UK Health and Safety Executive, 2004.

SAŽETAK

Poboljšanje i nadogradnja uzbunjujuće-sigurnosno-blokirajućeg sustava u proizvodnji dušične kiseline Petrokemije d. d.

N. Zečević,[a*] *I. Hoško*[a] *i S. Pavlaković*[b]

Svakom industrijskom procesu, osobito kemijskom, potrebno je posvetiti posebnu pažnju s obzirom na sigurnosne zahtjeve. Zbog toga se proizvodni procesi trebaju kontinuirano pratiti kontrolnim i uzbunjujuće-sigurnosno-blokirajućim sustavima. U proizvodnji dušične kiseline Petrokemije d. d. izvorni uzbunjujuće-sigurnosno-blokirajući sustav bio je izveden u obliku električno-relejnog sigurnosno-blokirajućeg sustava i tranzistorskog uzbunjujućeg sustava. Radi povećanja sigurnosnih zahtjeva i poboljšanja postojećeg uzbunjujuće-sigurnosno-blokirajućeg sustava provedena je nadogradnja postojećeg s novim mikroprocesorskim sustavom. Novi uzbunjujuće-sigurnosno-blokirajući sustav, Simatic PCS 7, povezuje funkcije klasičnih logičkih kontrolnih sustava s uzbunjujuće-sigurnosno-blokirajućim funkcijama u zajedničku bazu kako bi se zadovoljili minimalne sigurnosne norme do razina sigurnosnih integriteta 2 i 3 s obzirom na standarde IEC 61508 i IEC 61511. Prikazan je pristup nadogradnje logike uzbunjujuće-sigurnosno-blokirajućeg sustava u proizvodnji dušične kiseline u obliku logičkog dijagrama koji je bio osnova za daljnje izvođenje radova. Na temelju izrađenog logičkog dijagrama i definiranih sigurnosnih zahtjeva, projekt je proveden u tri faze koje su bile faza analize i testiranja, ugradnje nove opreme te puštanje u pogon cijelog izvedenog sustava. Razvijen je sustav provjere svih sigurnosno-blokirajućih uvjeta, koji se može primijeniti i na druga postrojenja za proizvodnju dušične kiseline. S obnovljenim i nadograđenim uzbunjujuće-sigurnosno-blokirajućim sustavom postavljene su nove poboljšane sigurnosne granice te je osigurana osnova za daljnje unaprjeđenje proizvodnog procesa.

[a] *Petrokemija d. d., Proizvodnja gnojiva, Kutina, Hrvatska*
[b] *Siemens d. d. Zagreb, Hrvatska*

Prispjelo 30. svibnja 2011.
Prihvaćeno 16. prosinca 2011.