საქართველოს ტექნიკური უნივერსიტეტი

ხელნაწერის უფლებით

ანზორი ბაბუნაშვილი

„ჩაშენებული დაცვის სისტემების პროგრამული ტექნოლოგიები“

სადოქტორო პროგრამა „მართვის სისტემები, ავტომატიზაცია და ტესტ-ინჟინერინგი“

შიფრი 0403

დოქტორის აკადემიური ხარისხის მოსაპოვებლად
წარდგენილი დისერტაციის

ა ვ ტ ო რ ე ფ ე რ ა ტ ი

თბილისი

2019 წელი

სამუშაო შესრულებულია საქართველოს ტექნიკური უნივერსიტეტში

ინფორმატიკისა და მართვის სისტემების ფაკულტეტი

მართვის სისტემების დეპარტამენტი

ხელმძღვანელი: პროფ. ია მოსაშვილი

რეცენზენტები: ----------

დაცვა შედგება ---------- წლის ”------” ----------, --------- საათზე

საქართველოს ტექნიკური უნივერსიტეტის ----------

---------- საუნივერსიტეტო სადისერტაციო

საბჭოს სხდომაზე, კორპუსი ----------, აუდიტორია ----------

მისამართი: 0175, თბილისი, კოსტავას 77.

დისერტაციის გაცნობა შეიძლება სტუ-ის ბიბლიოთეკაში,

ხოლო ავტორეფერატისა - ფაკულტეტის ვებგვერდზე

საუნივერსიტეტო სადისერტაციო საბჭოს მდივანი,

პროფ.თინათინ კაიშაური

ნაშრომის ზოგადი დახასიათება

თემის აქტუალობა. თანამედროვე ცხოვრებაში სულ უფრო მეტი ადამიანი მიდის იმ დასკვნამდე, რომ მხოლოდ სახელმწიფო სამართალდამცავი ორგანოების ძალისხმევა არ არის საკმარისი ისეთი პრობლემის გადასაჭრელად, როგორიცაა სახელმწიფო ობიექტების დაცვა და მათი უსაფრთხოების უზრუნველყოფა.

ჩვენი ეპოქის დამახასიათებელი ნიშანია კრიმინოგენური სიტუაციის მკვეთრი გაუარესება, ძალიან ბევრი შემთხვევაა, როცა საიმედო, მაგრამ არასწორად დაყენებული ტექნიკური საშუალებები ვერ უზრუნველყოფენ საკუთრების დაცვას, ამიტომ სრული დაცვის ორგანიზებისათვის არ არის საკმარისი სამრეწველო ობიექტები გადავტვირთოთ რთული და ძვირადღირებული ელექტრონული საშუალებებით, ასევე აუცილებელია გარკვეული წესებისა და ზომების მიღება, რომელთა შესრულება სულაც არ არის რთული, თუმცა მათ არ შესრულებას მივყავართ მძიმე შედეგებამდე. ობიექტების დაცვის ამოცანის გადაწყვეტა დამყარებულია ისეთ ტექნიკურ საშუალებათა კომპლექსის გამოყენებაზე, რომლებმაც უნდა დააფიქსირონ სხვადასხვა საფრთხის მოახლოება ან დაწყება - ხანძრიდან და ავარიიდან დაწყებული და დამთავრებული ობიექტზე ან კომპიუტერულ ქსელში შეჭრით. ეფექტური დაცვის სისტემის პროექტირება პროგრამულ-აპარატურულ საშუალებათა გათვალისწინებით წარმოადგენს უძნელეს მრავალგანზომილებიან ამოცანას, რომელთა გადაჭრა შეუძლებელია სისტემის სტრუქტურის, ფუნქციონალური შესაძლებლობების და მუშაობის პრინციპების ღრმა შესწავლის გარეშე [31,32,33].

კვლევის საგანი და პრობლემატიკა. კვლევის საგანია სხვადასხვა ტიპისა და სახეობების ობიექტების დაცვის მეთოდებისა და საშუალებების შემუშავება, ხოლო პრობლემატიკაა:

- დასაცავი ობიექტების სახესხვაობების დადგენა;
- თანამედროვე ტექნიკური მოწყობილობების გამოყენებით კომპიუტერულ სისტემებთან თავსებადი დაცვის სისტემების

შემუშავება;

აღნიშნული საკითხების გადასაწყვეტად წარმოდგენილია დაცვის ობიექტის მათემატიკური მოდელი და მისი საშუალებით შევისწავლეთ პრობლემატური საკითხები.

კვლევის მიზანი და ამოცანები. კვლევის მიზანია თანამედროვე ტიპის, მაღალი სიზუსტისა და საიმედობის და სხვადასხვა ტიპის ობიექტებზე გათვლილი დაცვის სისტემის შექმნა, რომელიც მაქსიმალურად იქნება დაცული გარე პირების შეღწევისაგან. ამ მიზნის მისაღწევად გადასაწყვეტია შემდეგი ამოცანები:

- თანამედროვე დაცვის სისტემების შესწავლა;
- ობიექტების ტიპებისა და სახეობების მიხედვით დაცვის სისტემების შეჩევა;
- დაცვის სისტემების ფუნქციონირების შემოწმება ტესტირების მეთოდით;
- პროგნოზირებადი დაცვის სისტემების დამუშავება;

კვლევის მეთოდები. კვლევის მიზნის მისაღწევად გამოყენებულია იდენტიფიკაციისა და აუტენტიფიკაციის მეთოდები.

კვლევის ობიექტს წარმოადგენს სხვადასხვა ტიპისა და სახეობის ობიექტებზე გათვლილი სიგნალიზაციის სისტემა;

მეცნიერული სიახლე. ნაშრომში განხილულია თეორიული და ექსპერიმენტული გამოკვლევების ძირითადი შედეგები, მათ შორის:

1. შემუშავებული სქემა წარმოადგენს სახელმწიფო ობიექტის სიგნალიზაციის ერთ-ერთ შესაძლო ვარიანტს, რომელიც წარმატებით უზრუნველყოფს სხვადასხვა ტიპის ობიექტების დაცვას.
2. იგი აწყობილია მიკროპროცესორულ ბლოკზე და წარმოადგენს მოქნილ მოწყობილობას ფუნქციონალური ცვლილების თვალსაზრისით, მარტივია დასამზადებლად.
3. იაფია თვითღირებულებით, საიმედოა და აკმაყოფილებს თანამედროვე მოთხოვნებს, მისი მხოლოდ უმნიშვნელო ცვლილება უზრუნველყოფს

აგრეთვე ერთდროულად რამდენიმე ობიექტის დაცვას, სისტემა საიმედოა შეუღწევლობის უზრუნველყოფით.

4. შესაძლებელია SMS შეტყობინებების გაგზავნა, მათი დამახსოვრება, ხასიათდება კვების მრავალსაათიანი ავტონომიურობით, მისი გამოყენება მცირე პროგრამული და აპარატურული ცვლილებებით შესაძლებელია საკმაოდ ფართო სპექტრის ობიექტებისათვის.

დაცვაზე გამოტანილი დებულებები:

- დაცვის სისტემების არსებული მეთოდებისა და საშუალებების მიმოხილვა და ანალიზი.
- სამრეწველო ობიექტების დაცვის ვიდეო დაკვირვების სისტემები.
- დაცვის ინტელექტუალური სისტემის პარამეტრების მართვის სიმულაციური მოდელი.

სამუშაოს შედეგების დასაბუთება მიღწეულია თეორიული და ექსპერიმენტული კვლევითი შედეგების ანალიზით.

სამუშაოს პრაქტიკული ღირებულება მდგომარეობს შემდეგში: განხილული მეთოდები და საშუალებები იძლევა იმის შესაძლებლობებს, რომ შეიქმნას ისეთი სიგნალიზაციის სიტემა, რომელიც იქნება მაღალი საიმედობის, მოქნილი იმგვარად, რომ საჭიროების შემთხვევაში ადვილად მოხდეს მისი მოდიფიცირება, სისტემას ადვილად შეიძლება მიუერთდეს სხვადასხვა დამატებითი მოდულები, რაც ზრდის მის ფუნქციონალურ შესაძლებლობებს და იმის შანსს, რომ იგი ადვილად მოვარგოთ სხვადასხვა დაცვის სისტემებზე.

სამუშაოს აპრობაცია, სადისერტაციო ნაშრომის ძირითადი დებულებები წარმოდგენილი იყო სხვადასხვა ჟურნალებში და გამოცემებში, მათ შორის:

- პერიოდული სამეცნიერო ჟურნალი „ხანძთა“; (2017 წ.)
- საქართველოს ტექნიკური უნივერსიტეტის მართვის ავტომატიზებული სისტემების შრომები; (2017 წ).

- საქართველოს ტექნიკური უნივერსიტეტის სტუდენტთა 87-ე ღია საერთაშორისო სამეცნიერო კონფერენცია. მართვის ავტომატიზებული სისტემების დეპარტამენტი (2019 წ).

პუბლიკაციები. სადისერტაციო თემის ირგვლივ გამოქვეყნებულია ხუთი სამეცნიერო ნაშრომი.

სამუშაოს სტრუქტურა და მოცულობა. დისერტაცია შედგება შესავლის, ოთხი თავის, ძირითადი დასკვნის, ლიტერატურის სიიდან 38 დასახელებით. სამუშაოს ძირითადი მასალა გადმოცემულია 102 გვერდზე, ოთხი ნახაზით.

სადისერტაციო ნაშრომის შინაარსი

შესავალში წარმოდგენილია სადისერტაციო თემის აქტუალობა, ის ძირითადი ამოცანები და პრობლემები, რომლებიც წარმოიშობა კვლევის პროცესში. ჩამოყალიბებულია ნაშრომის მიზანი, კვლევის მეთოდები, მეცნიერული სიახლე და პრაქტიკული ღირებულება. მოცემული ნაშრომის შინაარსის მოკლე ანოტაცია.

დისერტაციის პირველ თავში გადმოცემულია დაცვის სისტემების არსებული მეთოდებისა და საშუალებების მიმოხილვა და ანალიზი. გააანალიზებულია ის გზა, რომელიც გაიარა დაცვის სისტემების იდეამ დღევანდელ დღემდე, რომელთა შედეგად გაჩნდა მომხმარებლის წინაშე მდგარი ამოცანების ჩამოყალიბების საშუალება, მოცემულია დასაცავი ობიექტების კლასიფიკაცია სხვადასხვა ნიშნების მიხედვით, განხილულია უსაფრთხოების კომპლექსური სისტემები და მათი შემადგენელი ქვესისტემები. მოცემულია აგრეთვე ობიექტის დაცვის სისტემის აგების ზოგადი პრინციპები, რომელთა დაცვა უზრუნველყოფს ობიექტების ეფექტურ დაცვას, ეწინააღმდეგება არასაშტატო სიტუაციებს და ხელს უწყობს საფრთხეების გამოვლენას სხვადასხვა დარღვევის მოდელების დროს.

დაცვის სისტემის ნორმალური ფუნქციონირებისათვის აუცილებელია

რამდენიმე პირობის შესრულება;

1. არც ერთი ქვესისტემა არ უნდა უშლიდეს ხელს მთლიანი სისტემის ფუნქციონირებას;
2. ერთობლივად მოქმედი სისტემების ფუნქციები უნდა ავსებდეს ერთმანეთს და არ უნდა ახდენდნენ ხელისშემშლელ გავლენას თავიანთი შემადგენელი ნაწილების მუშაობისუნარიანობაზე.
3. ერთდროულად მოქმედ სისტემებში უზრუნველყოფილი უნდა იყოს ალგორითმული თავსებადობა და ყველა სამსახურეობრივი თუ საგანგაშო სიგნალების რეგისტრაცია.
4. ერთ-ერთი ქვესისტემის მწყობრიდან გამოსვლა არ უნდა იწვევდეს მთლიანი სისტემის მოშლას.
5. დაცვის სისტემა უნდა იმართებოდეს როგორც ცენტრალიზებულად, ასევე დეცენტრალიზებულად პერსონალის დონეების კონტროლის გათვალისწინებით.
6. დაცვის სისტემა უნდა ინარჩუნებდეს გამართულ მდგომარეობას გარე სამყაროს ფაქტორების ზემოქმედების შემდეგაც უნდა შეეძლოს მუშაობისუნარიანობის აღდგენა ამ ფაქტორების შეწყვეტის შემდეგ.
7. დაცვის სისტემა არ უნდა გამოდიოდეს მწყობრიდან ობიექტზე ელექტროენერგიის გათიშვის შემთხვევაშიც და უნდა ინარჩუნებდეს მუშაობისუნარიანობას სხვა ძირითადი წყაროს დაზიანების დროსაც, არ უნდა იძლეოდეს მცდარ სიგნალებს ძირითადიდან სარეზერვო კვებაზე გადართვის მომენტში.

დაცვის სიტემების აგების დროს არა საკმარისია მარტო ფუნქციონალურად დამოუკიდებელი ქვესისტემების შემქნა, არამედ აუცილებელია ინტეგრირებული კომპლექსური სისტემების გამოყენება.

ინტეგრირების მიზანს შეადგენს:

ა) მცდარი გადაწყვეტილებების მიღების რისკების შემცირება და ობიექტზე არასაშტატო სიტუაციის შექმნისას რეაქციის დროის შემცირება;

ბ) ახალი ფუნქციების მიღება, რომელთა მიზანია დაცვის სისტემების

ქვესისტემების ოპერატიული ურთიერთკავშირის უზრუნველყოფა და ამასთან სისტემის შემადგენელი ნაწილების სრული მოცულობით შენარჩუნება;

გ) ამ ფუნქციების რეალიზებისათვის საშუალებათა ეკონომიკა;

დ) ობიექტის დაცვისათვის ყველა მიმართულებით მაქსიმალური ავტომატიზაციის დონე;

ერთი სისტემის ფარგლებში შესაძლებელია მოწყობილობათა ინტეგრაციის რამდენიმე იერარქიული საფეხური:

- **ინტეგრაცია საპროექტო დონეზე** -გულისხმობს საშუალებათა გაერთიანებას კონკრეტული სისტემისათვის პროექტირების ეტაპზე, ეს არის ინტეგრაციის ყველაზე დაბალი დონე, მისი გამოყენების ნაკლოვანებებია „ადამიანური ფაქტორი“, აპარატურათა სახესხვაობები, მომსახურების სირთულე, ავტომატიზაციის არარსებობა და ა.შ.
- **ინტეგრაცია აპარატურულ დონეზე-** გულისხმობს გაერთიანებას უპირატესად აპარატურული უზრუნველყოფის დახმარებით ყოველი სისტემისათვის მართვის კომპიუტერებისა და პროგრამული უზრუნველყოფის გამოყენების გარეშე, ასეთი გაერთიანების კლასიკური მაგალითია სისტემების გაერთიანება სარელეო კონტაქტების დახმარებით. მისი უპირატესობაა გამოყენებული აპარატურის სიმარტივე და საიმედოობა, დაბალი ღირებულება და სხვადასხვა მწარმოებლების მიერ შექმნილი მოწყობილობების გაერთიანების შესაძლებლობა.
- **ინტეგრაცია პროგრამულ დონეზე-** (პროგრამულ-აპარატურულ დონეზე პროგრამული მარდაჭერის პრიორიტეტით)- გულისხმობს ერთიანი პროგრამული უზრუნველყოფის ქვეშ სხვადასხვა მწარმოებლების მიერ შექმნილი ქვესისტემების გაერთიანებას, ასეთი სისტემის აგება მიმდინარეობს ორი გზით: პირველი გზა მდგომარეობს სპეციალური პროგრამული უზრუნველყოფის გამოყენებაში, ხოლო მეორე ითვალისწინებს პროგრამული გარსის გამოყენებას ინტეგრირებადი

პროგრამული მხარდაჭერის მაგიერ[25,26].

- **ინტეგრაცია პროგრამულ-აპარატურულ დონეზე-** გულისხმობს მაქსიმალური ხარისხის ურთიერთკავშირს სისტემის ყველა ელემენტს შორის, მიუხედავად იმისა, თუ რა ფუნქციები აკისრიათ მათ, რითაც მიიღწევა მუშაობის სიმარტივე და ხარჯების შემცირება სისტემის მონტაჟისა და აწყობის დროს.

ინტეგრირებული დაცვის სიტემები წარმოადგენენ მრავალფუნქციონალურ ნაკეთობას, ფუნქციონალური დანიშნულების მიხედვით ის შეიძლება დავყოთ:

- ✓ **უმაღლესი დონე**-გულისხმობს ინტეგრირებული და სხვა ინფორმაციული სისტემების ურთიერთკავშირს, ეს ერთგვარი „კლიენტ-სერვერის“ კომპიუტერული ქსელია ქსელური ოპერაციული სისტემის გამოყენებით, ეს დონე უზრუნველყოფს კავშირს სერვერსა და ოპერატორების მუშა სადგურებს შორის პროგრამული უზრუნველყოფის საშუალებით, მოითხოვება მაღალი საიმედობა და დაცვა არასანქცირებული წვდომისაგან.
- ✓ **პირველი დონე-** გულისხმობს გარკვეული ქვესისტემების ინფორმაციულ ურთიერთკავშირს, თითოეული ქვესისტემა ავტომატურად ასრულებს გარკვეულ მოქმედებას სხვა სისტემიდან მოსული სიგნალის ზემოქმედების შედეგად.
- ✓ **მეორე დონე** -წარმოადგენს ინფორმაციის შეკრებისა და გადაცემის ლოკალური სისტემების ინტეგრაციას, აქ შესაძლებელია ვერტიკალური (ინტეგრაციისა კონტროლერებსა და ქვესისტემების კომპიუტერებს შორის კავშირი) და ჰორიზონტალური (ერთი ტიპის კონტროლერებისა და თითოეული ქვესისტემის კავშირი) ინტერგრაციის კავშირი.

ასევე პირველ თავში განხილულია დაცვის ინტეგრირებული კომპლექსური სისტემები დონეების მიხედვით და დამცავი დეტექტორების მოქმედება, მათი მუშაობის პრინციპების გათვალისწინებით.

დაცვის სისტემების თითოეულ ელემენტს აქვს განსაკუთრებული

მნიშვნელობა სისტემის ფუნქციონირებისათვის, განვიხილოთ მათგან სამი უმთავრესი ჯგუფი, რომლებიც ითვლებიან ძირითადად:

- დაცვისა და განგაშის სისტემები (დგს)
- სახანძრო სიგნალიზაციის სისტემები (სსს)
- დაცვის სატელევიზიო სისტემები (დსს)

დაცვისა და განგაშის სისტემები შეიცავს შემდეგ ძირითად ელემენტებს:

- დეტექტორები
- საგანგაშო სიგნალიზაციის საშუალებები-ღილაკები, სატერფულები, დეტექტორები
- ინფორმაციის შეკრების, დამუშავების, წარმოდგენის და მართვის საშუალებები.

სახანძრო სიგნალიზაციის სისტემები შეიცავენ შემდეგ ძირითად ელემენტებს:

- სახანძრო დეტექტორები (სითბური, კვამლის, ალის, გაზის და ხელის);
- ინფორმაციის შეკრების, დამუშავების, წარმოდგენის და მართვის საშუალებები.

ობიექტის აღჭურვა სახანძრო სიგნალიზაციის ტექნიკური საშუალებებით და ხანძარსაწინააღმდეგო დაცვის ინვენტარით მკაცრად უნდა რეგულირდებოდეს შესაბამისი ნორმატიული დოკუმენტებით, აგრეთვე დაიშვება ისეთი ტექნიკური საშუალებების გამოყენება, რომლებსაც გააჩნიათ სტანდარტებთან შესაბამისობის სერტიფიკატი, დაყენებული სისტემები უნდა უზრუნველყოფდეს სადღეღამისო განუწყვეტელ მუშაობას.

დგს და სსს აგების იდეოლოგიის მიხედვით ძალიან ახლოსაა ერთმანეთთან და მცირე ობიექტებზე, როგორც წესი შერწყმულია ერთმანეთთან ერთიანი კონტროლის ბლოკის ან საკონტროლო პანელის ბაზაზე, ამასთან რეალიზებულია დამცავ-სახანძრო სიგნალიზაცია, რომლის ძირითადი ამოცანაა დასაცავ ობიექტზე ხანძრის ან არასანქცირებული

შეღწევის შედეგად მიღებული ინფორმაციის დამუშავება და გადაცემა, ეს ინფორმაცია მიეწოდება პერსონალს შემდგომი რეაგირებისათვის [30,31].

თითოეული ასეთი სისტემა შეიცავს დეტექტორებს, რომლებიც აკონტროლებენ გარე სამყაროს სხვადასხვა ფიზიკურ პარამეტრებს, საფრთხეების გამოვლენისა და სიგნალების ფორმირების მიხედვით დეტექტორები იყოფიან უმისამართო, მისამართიან და მისამართიან-ანალოგურ დეტექტორებად.

უმისამართო სისტემებში დეტექტორებს აქვთ მგრძნობელობის ფიქსირებული ზღვარი, თანაც დეტექტორების ჯგუფი ირთვება სისტემის საერთო შლეიფში, და ერთ-ერთ მათგანის ამოქმედებისას ყალიბდება განგაშის განზოგადებული სიგნალი.

მისამართიანი სისტემები განსხვავდებიან ინფორმაციის განაცხადში განმცხადებლის მისამართით, რაც საშუალებას იძლევა განისაზღვროს ხანძრის ზონა დეტექტორის განლაგების სიზუსტით.

მისამართიან-ანალოგური სისტემები არიან ყველაზე ინფორმატიული და განვითარებული, მათში გამოიყენება „ინტელექტუალური“ დეტექტორები, რომლებიც გადასცემენ კონტროლირებადი პარამეტრის მიმდინარე მნიშვნელობას შლეიფში მათ მისამართთან ერთად. მონიტორინგის ასეთი მეთოდი გამოიყენება საგანგაშო სიტუაციების ადრეული აღმოჩენისათვის, გარდა ამისა ეს სისტემები საშუალებას იძლევიან სისტემის მუშაობის შეუწყვეტლივ ცვალონ დეტექტორების ფიქსირებული მგრძნობელობის ზღვარი პროგრამულ დონეზე და შეუსაბამონ ისინი ობიექტის ექსპლოატაციის პირობებს.

დეტექტორების თითოეულ ტიპს აქვს ძირითადი მახასიათებლების თავისი ჩამონათვალი, რომელიც შეესაბამებიან სტანდარტებს. ამავე დროს ერთი და იმავე ტიპის დეტექტორებსაც კი აქვთ კონსტრუქციული განსხვავებები ძირითად ნაწილებში, საიმედობაში, დიზაინში, რაც თქმა უნდა მიიღება მხედველობაში ამა თუ იმ ფირმის ან მწარმოებლის მიერ

შექმნილი დეტექტორების ამორჩევისას.

ობიექტზე შეღწევის ან ხანძრის შემთხვევაში ინფორმაციული სიგნალების ჩამოყალიბების პრინციპის მიხედვით დეტექტორები იყოფა ორ ჯგუფად:

- **აქტიური,** რომლებიც ახდენენ დასაცავ ზონაში სიგნალის გენერირებას და რეაგირებენ მისი პარამეტრების ცვლილებაზე;
- **პასიური,** რომლებიც რეაგირებენ გარემომცველი სამყაროს პარამეტრების ცვლილებაზე, რაც გამოწვეულია ხანძრის ან სხვა პირის შეღწევით;

გამოყენების სფეროს მიხედვით დეტექტორები იყოფა დამცავ, სახანძრო-დამცავ და სახანძრო დეტექტორებად.

დამცავი დეტექტორები კლასიფიცირდებიან ფუნქციონალური დანიშნულების შემდეგი ნიშნების მიხედვით:

1. მათი მოქმედებაში მოყვანის მეთოდის მიხედვით- ავტომატურ და ხელის დეტექტორებად;
2. ექსპლოატაციის პირობების მიხედვით-გამთბარ შენობებში დასაყენებელი, გაუთბობელ შენობებში დასაყენებელი, ღია ობიექტებზე და მოედნებზე დასაყენებელი;
3. ავტომატური დეტექტორის მიერ კონტროლირებადი ზონის მიხედვით:
   — წერტილოვანი დეტექტორი-აკონტროლებს ობიექტზე შეღწევას დაყენების წერტილში;
   — ხაზოვანი დეტექტორი-აკონტროლებს წრფის ან მრუდის გასწვრივ ტერიტორიას;
   — ზედაპირული დეტექტორი-აკონტროლებს ზონას სამი განზომილების მიხედვით: სიგრძე, სიგანე და სიღრმე;
4. ფიზიკური პრინციპების მიხედვით, რომლებიც შეადგენს აღმოჩენის საფუძველს: მექანიკური (ელექტროკონტაქტური, მაგნიტოკონტაქტური, დარტყმით-კონტაქტური), ელექტრომაგნიტური უკონტაქტო, პიეზოელექტრული, ტევადური, აკუსტიკური (ინფრაბგერითი,

ულტრაბგერითი, ბგერითი), ვიბრაციული, ოპტიკურ-ელექტრონული (აქტიური, პასიური, რადიოტალღური, ელექტროსტატიკური, რადიოსხივური (მიკროტალღური), კომბინირებული [30].

5. დეტექტორების მიერ აღმოსაჩენი ზონების რაოდენობის მიხედვით-ერთზონიანი და მრავალზონიანი.
6. მოქმედების სიშორის მიხედვით-ულტრაბგერითი, ოპტიკურ-ელექტრონული და რადიოსხივური, დახურული შენობებისათვის განიხილავენ:
   - მცირე მანძილზე მოქმედების-12 მ-მდე;
   - საშუალო მანძილზე მოქმედების-12 მ-დან 30 მ-მდე;
   - დიდ მანძილზე მოქმედების-30 მ -ის ზევით (გარდა ულტრაბგერითებისა);

7. მოქმედების სიშორის მიხედვით არსებობენ ოპტიკურ-ელექტრონული და რადიოსხივური დეტექტორები, ღია მოედნებისა და პერიმეტრებისათვის ისინი იყოფა:
   - მცირე მანძილზე მოქმედების -50 მ-მდე;
   - საშუალო მანძილზე მოქმედების-50-მ-დან 200 მ-მდე;
   - დიდ მანძილზე მოქმედების-200 მ-ზე ზევით;
8. კონსტრუქტორული შესრულების მიხედვით ულტრაბგერითი, ოპტიკურ-ელექტრონული და რადიოსხივური დეტექტორები იყოფიან:
   - ✓ ერთპოზიციური -ერთი ან მეტი გადამცემი და მიმღები შეთავსებულია ერთ ბლოკში;
   - ✓ ორპოზიციური - გადამცემი და მიმღები შესრულებულია ცალკეული ბლოკების სახით;
   - ✓ მრავალპოზიციური- ორზე მეტი ბლოკი (ერთი გადამცემი, ორი ან მეტი მიმღები; ერთი მიმღები, ორი ან მეტი გადამცემი)
9. კვების წყაროს ხასიათის მიხედვით:
   - ❖ დენის არ მომხმარებელი;
   - ❖ სიგნალიზაციის შლეიფიდან მკვებავი;

- ❖ კვების გარე ავტონომიური წყაროდან მკვებავი;
- ❖ ცვლადი დენის ქსელიდან ძაბვით 220 ვ.

სახანძრო დეტექტორები კლასიფიცირდება შემდეგი ფუქციონალური ნიშნების მიხედვით:

1. მოქმედებაში მოყვანის მეთოდის მიხედვით-ავტომატური და ხელის;
2. ინფორმაციის გაცვლის ხასიათის მიხედვით-ზღვრული და ანალოგური
3. ხანძრის საკონტროლო ნიშნის მიხედვით ავტომატური სახანძრო დეტექტორები არსებობენ:
   - — სითბური, რომლებიც რეაგირებენ ტემპერატურის მომატებაზე;
   - — კვამლის, რეაგირებენ კვამლის წარმოქმნაზე;
   - — ალის;
   - — გაზის;
   - — კომბინირებული;
   - — ხანძრის სხვა ნიშნის;
4. ხანძრის თვისებაზე რეაქციის ხასიათის მიხედვით ზღვრული სითბური დეტექტორები იყოფა მაქსიმალურ, დიფერენციალურ და მაქსიმალურ-დიფერენციალურ დეტექტორებად [31].

განვიხილოთ დაცვის დეტექტორების ზოგიერთი ფუნქციონალური თავისებურებები, რომლებიც აქტიურად გამოიყენება პრაქტიკაში:

წერტილოვანი ელექტროკონტაქტური დეტექტორი-გამოსცემს განგაშის სიგნალს ელექტრო კონტაქტის გაღება-ჩაკეტვის დროს, ეს დაცვის დეტექტორების ყველაზე მარტივი სახეობაა, რომელიც წარმოადგენს წვრილ ლითონის გამტარს, რომელიც სპეციალურადაა დამაგრებული საგანზე ან კონსტრუქციაზე.

მაგნიტოკონტაქტური დეტექტორები - აყალიბებენ სიგნალს მაგნიტური კონტაქტის გაღებისას, გამოიყენება გაღების ბლოკირებისათვის სხვადასხვა სამშენებლო კონსტრუქციებში.

დარტყმით-კონტაქტური დეტექტორები - რეაგირებენ და გამოსცემენ განგაშის სიგნალს ობიექტზე დარტყმითი ზემოქმედების დროს,

ძირითადში გამოიყენება შემინული კონსტრუქციების ბლოკირებისათვის.

პიეზოელექტრული დეტექტორები - გამოსცემენ განგაშის სიგნალს დრეკადი ტალღის ზემოქმედების დროს, გამოიყენება სამშენებლო კონსტრუქციების და ცალკეული საგნების ბლოკირებისათვის.

ოპტიკურ-ელექტრონული აქტიური დეტექტორები -სიგნალს აყალიბებენ ხანძრის ან ობიექტზე შეღწევის დროს არეკვლილი ნაკადის ცვლილებისას ან შეწყვეტისას, რაც შეიძლება გამოწვეული იყოს დამრღვევის მოძრაობით აღმოჩენის ზონაში, ძირითადად გამოიყენება შიგა და გარე პერიმეტრების, ფანჯრების, ვიტრინების დასაცავად.

ოპტიკურ-ელექტრონული ინფრაწითელი პასიური დეტექტორი - რეაგირებს ინფრაწითელი გამოსხივების დონის ცვლილებაზე, რაც გამოწვეულია ადამიანის გადაადგილებით აღმოსაჩენ ზონაში, გამოიყენება ნებისმიერი კონფიგურაციის შენობების დაცვისათვის.

ტევადური დეტექტორები - რეაგირებენ მგრძნობიარე ელემენტის ტევადობის შეცვლაზე, რაც განპირობებულია ობიექტზე შეჭრით. ძირითადად გამოიყენება კარადების, სეიფების ბლოკირებისათვის.

კომბინირებული დეტექტორები - საშუალებას იძლევიან გამოვლენილ იქნას დამრღვევი ორი ან მეტი სხვადასხვა მოქმედების ფიზიკური პრინციპის მიხედვით, ისინი შეიცავენ სხვადასხვა ტიპის არხებს, მაგრამ იცავენ ერთ და იმავე ზონას. თითოეული არხი ასრულებს მუშაობის თავის ფიზიკურ პრინციპს და შესაბამისად აქვს თავისი ფაქტორების ნაკრები, სხვადასხვა არხების არსებობა ამცირებს მცდარი რეაგირების ალბათობას.

დისერტაციის მეორე თავში განხილულია დაცვის ვიდეო დაკვირვების სისტემები და მათი ფუნქციები:

- საკონტროლო ზონის პირდაპირი ვიდეო დაკვირვება ოპერატორის მიერ, დანიშნულების მიხედვით დაკვირვების ობიექტების აღმოჩენა და იდენტიფიკაცია, მათ შორის ხალხი, სატრანსპორტო საშუალებები, ქონება, ობიექტების ინფრასტრუქტურის ელემენტები;

- დასაცავი ზონების მდგომარეობის შესახებ ვიზუალური ინფორმაციის გადაცემა ობიექტის პერიმეტრის, დაცვის პუნქტისა და გადაადგილების შესახებ განგაშის ვიდეოვერიფიკაციისათვის;
- დასაცავი ობიექტის მდგომარეობის ანალიზისათვის ვიდეოინფორმაციის არქივის შექმნა საგანგაშო სიტუაციების შეფასებისათვის, ასევე დამრღვევის იდენტიფიცირებისა და სხვა ამოცანების შესასრულებლად.

განხილულია სისტემის ძირითადი კომპონენტები და მათი პარამეტრები, ინფორმაციის გადაცემის სხვადასხვა საშუალებები, მათ მიერ გადმოცემული გამოსახულებების სხვადახვა სახეობები.

ასეთი სისტემების მთავარი კომპონენტია ვიდეო კამერები, განხილულია მათი სხვადასხვა სახეობები და მათი გამოყენების პირობები, ხაზგასმულია თითოეული მათგანის უპირატესობა, რაც განაპირობებს მათი გამოყენების შესაძლებლობებს.

ციფრული ვიდეო დაკვირვების სისტემების განვითარების ერთ-ერთი მთავარი მიმართულებაა ვიდეოდაკვირვების სისტემები IP-კამერების ბაზაზე, რომელსაც ხშირად უწოდებენ ქსელური ვიდეოდაკვირვების სისტემებს, ისინი იყენებენ ვიდეო და აუდიო სიგნალების გადაცემისათვის სადენიან ან უსადენო ქსელს.

IP-ვიდეოდაკვირვების აქტიური დანერგვა განპირობებულია მთელი რიგი მიზეზებით:

- IP-ინდუსტრიის მიღწევების გამოყენების შესაძლებლობით;
- ციფრული სახით ინფორმაციის გადაცემის ან შენახვისას არ აქვს ადგილი ინფორმაციის დამახინჯებას;
- დიდი ვიდეოსისტემებისათვის ეკონომიკური ეფექტურობით;
- ვიდეოანალიზის შესაძლებლობის გამო ახალი ფუნქციების რეალიზებით;

ქსელური ვიდეოდაკვირვების სისტემების საბაზო კომპონენტს წარმოადგენს ქსელური კამერები, ვიდეოკოდერები და პროგრამული

უზრუნველყოფა, ვიდეოს მართვისათვის, დანარჩენი კომპონენტები, მათ შორის ქსელი, შენახვის სისტემები, სერვერი წარმოადგენს სტრანდარტულ მოწყობილობებს [28, 25,26].

ქსელური ვიდეოკოდერის საშუალებით ანალოგური ვიდეოკამერების მიერთებით მომხმარებელი იღებს იმ უპირატესობას, რომ აღარ არის საჭირო ვიდეოგამოსახულების მისაღებად უკვე არსებული ანალოგური მოწყობილობების (ვიდეოკამერები, კოაქსიალური კაბელი) შეცვლა.

IP-კამერების ქვეშ იგულისხმება ციფრული ვიოდეოკამერა, რომელიც იძლევა ინფორმაციას ვიდეონაკადის სახით ციფრულ ფორმატში, მათ შეუძლიათ ინფორმაციის მოცემა როგორც შეკუმშული, ისე გაშლილი სახითაც, ამისათვის ისინი იყენებენ TCP, UDR და სხვა ტიპის პროტოკოლებს.

იმის გამო, რომ ასეთ კამერებს არ სჭირდებათ ანალოგური სიგნალის გადაცემა, მათში გამოყენებულია მეგაფიქსელური გარჩევადობა, სტანდარტულია 640X480, მაგრამ არსერბობენ მეგაფიქსელური გარჩევადობის კამერებიც 1280X1024, 1600X1200 და უფრო მაღალიც.
ქსელური ვიდეოდაკვირვების სისტემები ფლობენ ფუნქციონალურ უპირატესობებს ანალოგურ სისტემებთან შედარებით:

- გამოსახულების მაღალი ხარისხის მიღწევა და მკვეთრი დაფიქსირების საშუალება, შედეგად ადვილია მოვლენის მონაწილეთა იდენტიფიცირება, ხოლო კამერებში მეგაფიქსელური ტექნოლოგიების გამოყენება იძლევა გამოსახულების უკეთეს ხარისხს და მაღალ გარჩევადობას, ვიდრე ანალოგურ კამერებში.
- ქსელურ სისტემებში გამოსახულების მაღალი ხარისხის მიღწევა უფრო ადვილია, ვიდრე ანალოგურში, ანალოგურ სისტემებში მიმდინარეობს რამდენიმე ანალოგურ-ციფრული გარდაქმნა, ხოლო ყოველი გარდაქმნისას გამოსახულების ხარისხი უარესდება, უარყოფითად მოქმედებს გამოსახულების ხარისხზე გადაცემის სიშორეც, რაც მეტია

გადაცემის მანძილი, მით უფრო სუსტია სიგნალი, ხოლო ციფრულ სატელევიზიო სისტემებში გამოსახულება ერთხელ ციფრულდება და რჩება ამ ფორმით, ასეთი სახით ის ადვილად ინახება და მისდამი წვდომაც უფრო ადვილია.

- ხშირად ჩაწერილი ვიდეოინფორმაციის დიდი მოცულობის გამო, შეუძლებელია ხარისხიანი ვიდეოანალიზის გაკეთება, ხოლო ქსელური კამერები ჩაშენებული ინტელექტუალური და ანალიტიკური ფუნქციებით ადვილად უმკლავდებიან ამ პრობლემას, ამცირებენ არასაჭირო ჩაწერების რაოდენობას და იყენებენ წინასწარ განსაზღვრულ მოვლენებს. ასეთი შესაძლებლობები არ გააჩნიათ ანალოგურ სისტემებს [2,3].

შეიძლება განვაზოგადოთ და ჩამოვაყალიბოთ ქსელური კამერების უპირატესობები ანალოგურთან შედარებით;

- მასშტაბირებადი განაწილებული სისტემების აგების შესაძლებლობა;
- ვიდეოკამერის მუშაობისათვის საჭირო პარამეტრების ფართო დიაპაზონი:
- არ არის „მიბმული“ ანალოგურ სტანდარტებზე, ამიტომ შესაძლებელია IP-კამერების დანერგვა მაღალი გარჩევადობით;
- ასეთი კამერები შეიძლება ვარეგულიროთ მოცილებულად, მივცეთ საშუალება რამდენიმე ავტომატიზებულ მომხმარებელს დაათვალიეროს გამოსახულება რეალური დროის რეჟიმში და ჩაიწეროს ვიდეოგამოსახულებები მსოფლიოს ნებისმიერი წერტილიდან.
- აუდიო და ვიდეონაკადის ერთდოულად გადაცემის შესაძლებლობა ქსელში პარალელურ რეჟიმში;
- ნაკადების შეკუმშულ რეჟიმში გადაცემის შესაძლებლობა, რაც იძლევა ვიდეომატარებლებზე ადგილის ეკონომიის საშუალებას, თანაც ამ დროს არ არის საჭირო მაღალმწარმოებლური ვიდეორეგისტრატორი.

მაგრამ IP-კამერებს აქვთ ნაკლოვანებებიც ანალოგურთან შედარებით;

- IP-კამერების ფასი გაცილებით მაღალია, ვიდრე ანალოგურების,

მაგრამ თუ განვიხილავთ ობიექტის მოწყობილობას დაკვირვების სისტემებთან ერთად მაშინ ფასები თავსებადია ერთმანეთთან;

- IP-კამერების მგრძნობელობა გაცილებით დაბალია, ვიდრე ანალოგურის;
- ვიდეონაკადის დეკომპრესიის აუცილებლობა კომპიტერულ პლატფორმაზე;
- კომპიუტერული ქსელის „გატეხვის“ შესაძლებლობა;
- აპარატურული „ჩამოკიდების“ შესაძლებლობა.

დაცვის ვიდეო დაკვირვების სისტემების ერთ-ერთი ძირითადი ფუნქციაა-ვიდეოჩაწერა, რომელიც შეიძლება რეალიზებული იქნას ვიდეოჩაწერის მოწყობილობებით-ციფრული ვიდეორეგისტრატორებით ან პროგრამული მეთოდით პერსონალური კომპიუტერების ბაზაზე შესაბამისი პროგრამული უზრუნველყოფით

ასევე მეორე თავში გადმოცემულია ანალოგური და ქსელური კამერების შედარებითი დახასიათება, მათი ნაკლოვანებები და უპირატესობები, გაანალიზებულია თანამგზავრული ნავიგაციური სისტემების მოქმედება და მათი პრინციპები.

დისერტაციის მესამე თავში განხილულია იდენტიფიკაციისა და აუტენტიფიკაციის მეთოდები.

ნებისმიერი ინფორმაციული სისტემების დაცვის საფუძველს წარმოადგენს იდენტიფიკაცია და აუტენტიფიკაცია, რადგანაც ინფორმაციის დაცვის ყველა მექანიზმი გათვლილია სახელდებული სუბიექტებისა და ავტომატიზებული სისტემის ობიექტებთან მუშაობაზე.

სუბიექტებისა და ობიექტებისათვის პირადი იდენტიფიკატორის წვდომის მინიჭება და მისი შედარება მოცემულ ჩამონათვალთან არის იდენტიფიკაცია, იგი უზრუნველყოფს შემდეგი ფუნქციების შესრულებას:

- ✓ ნამდვილობის დადგენასა და სუბიექტის უფლებამოსილების განსაზღვრა სისტემისადმი წვდომის დროს;
- ✓ დადგენილი უფლებამოსილებების კონტროლი მუშაობის სეანსის დროს;

მოქმედებათა რეგისტრაცია და ა.შ.

აუტენტიფიკაცია (ნამდვილობის დადგენით) ეწოდება სუბიექტის მიერ წარმოდგენილი იდენტიფიკატორის სინამდვილის შემოწმებას ანუ ეს არის სუბიექტის შემოწმება მის ნამდვილობაზე.

სისტემის კონტროლირებადი კომპონენტის მიხედვით აუტენტიფიკაციის მეთოდები შეიძლება დავყოთ საკონტაქტო პარტნიორებისა და მონაცემთა წყაროს აუტენტიფიკაციად. პირველ შემთხვევაში აუტენტიფიკაცია გამოიყენება სეანსის დროს დამყარებული შეერთების დროს, იგი ემსახურება ისეთი საფრთხეების თავიდან აცილებას, როგორიცაა შენიღბვა ან კავშირის წინა სეანსის გამეორება. მონაცემთა წყაროს აუტენტიფიკაცია კი მონაცემთა წყაროს ნამდვილობის დადასტურებაა.

განხილულია აგრეთვე აუტენტიფიკაციის საპაროლო სისტემები და ის ძირითადი რეკომენდაციები, რომლებიც გამოიყენება ასეთ სისტემებში, მოცემულია ერთჯერადი და მრავალჯერადი პაროლების სისტემების ანალიზი და თავისებურებები.

ძალიან მნიშვნელოვან მიმართულებას წარმოადგენს იდენტიფიკაციისა და აუტენტიფიკაციის ელექტრონული საშუალებები, რომლებშიც საიდენტიფიკაციო ნიშნები წარმოდგენილია კოდის სახით, რომელიც ინახება იდენტიფიკატორის დაცულ მეხსიერებაში და განსაკუთრებული გამონაკლისების გარდა არ ტოვებს მას.

იდენტიფიკაციისა და აუტენტიფიკაციის ელექტრონული სისტემების შემადგენლობაში შედის კონტაქტური და უკონტაქტო სმარტ-ბარათები და უსბ-გასაღებები.

უსბ-გასაღებები მუშაობენ კომპიუტერის უსბ-პორტებთან და დამზადებულია გასაღებ-ჯაჭვის სახით-ეს არის მონაცემების შენახვისა და აუტენტიფიკაციის პერსონალური საშუალება. უსბ-გასაღებები შეიძლება დამზადებული იყოს სტანდარტული სმარტ-ბარათების სახითაც, ხოლო სმარტ-ბარათებს უნდა ჰქონდეთ კომპიუტერთან შეერთებისას სმარტ-

ბარათების წამკითხველი მოწყობილობა, იგი შეიძლება გამოიყენებოდეს როგორც ვიზუალური იდენტიფიკაციის საშუალება, მასზე შეიძლება ინახებოდეს მფლობელის შესახებ ინფორმაცია და ფოტოგრაფია სამსახურეობრივი გამოყენებისათვის.

ასევე ამ თავში განხილულია ბიომეტრული სისტემები, მეთოდები, რომლებსაც იყენებენ ბიომეტრულ ტექნოლოგიებში და ამოცნობის კატეგორიები.

მეოთხე თავში განხილულია ავტომატური პროექტირების სისტემები, რომლებიც გამოიყენება სქემების ანალიზისა და მოდელირებისათვის.

სპეციალიზებული ციფრული მოწყობილობის შექმნისას QuartusII სისტემის გამოყენებისას სქემის შემქმნელი მიუთითებს საჭირო მოწყობილობას და ღებულობს პროგრამირებად ფაილს, რომელიც შემდგომში გამოიყენება პროგრამირებადი ლოგიკური სქემის კონფიგურაციისათვის, პროგრამირებაში იგულისხმება ფუნქციონალური გარდამქმნელებისათვის სპეციალური ფუნქციის მინიჭება და მათ შორის აუცილებელი კავშირის დამყარება. დიდი ინტეგრალური სქემის გამოყენება უზრუნველყოფს აგრეთვე მოდიფიკაციის ისეთ მოქნილობას, როგორიცაა პროგრამული გადაწყვეტილებების დროს.

ავტომატური პროექტირების სისტემა QuartusII-ი უზრუნველყოფს შემდეგ ძირითად ფუნქციებს:

— მოწყობილობათა ქცევისა და სტრუქტურის აღწერის სხვადასხვა მეთოდებს;
— რთული პროექტებისათვის დახმარების ინტეგრირებული საშუალებათა შექმნას;
— სინთეზის ქვესისტემებს;
— ინტეგრალური სქემების განლაგებისა და რესურსების ქვესისტემას;
— მოდელირების ქვესისტემის შექმნას;
— მოხმარებული ენერგიის ანალიზისა და დროითი ანალიზის შექმნას;

— დიდი ინტეგრალური სქემების პროგრამირების ქვესისტემის არსებობას;

— პროექტის სწრაფქმედებისა და ოპტიმიზაციის ქვესისტემის შექმნას;

— სიგნალების ციფრული დამუშავების ბლოკების შექმნას;

— IP-მოდულების მხარდაჭერის გამოყენებას;

— ოპერაციული სისტემების Windows, Solaris და Linux-ის მხარდაჭერას;

პროექტირების სისტემა LabVIEW- გრაფიკული პროგრამირების სივრცეა, რომელსაც იყენებენ გაზომვის, გამოცდის, სამეცნიერო და პრაქტიკული ექსპერიმენტების მართვის ამოცანების სწრაფი გადაწყვეტისათვის. ტრადიციული ტექსტური პროგრამირების ენებთან შედარებით გრაფიკული პროგრამირების ენა და მისი კონცეფცია საშუალებას იძლევა უფრო ეფექტურად გადაიჭრას ბევრი რთული ამოცანა. პროექტირების სისტემა LabVIEW-ს საფუძვლად უდევს გრაფიკული პროგრამირების კონცეფცია: ბლოკ-დიაგრამაზე ფუნქციონალური ბლოკების მიმდევრობითი შეერთება. კონკრეტულად ინტუიტიურად გასაგები და თვალნათლივი გრაფიკული კოდი, ასევე პროგრამის შესრულებისას მონაცემთა ნაკადის მართვის ვიზუალური მონიტორინგის შესაძლებლობები ადამიანისათვის უფრო გასაგებს ხდის მთელ პროცესს.

პროექტირების სისტემა LabVIEW-ს აქვს მოწყობილობის უდიდესი სპექტრი სხვადასხვა მწარმოებლების მიერ შექმნილი მოწყობილობებისა და დამატებით კომპონენტების ძალიან დიდი ბიბლიოთეკა.

მძლავრი გრაფიკული პროგრამირების ენა საშუალებას იძლევა ასჯერ გაიზარდოს შრომის ნაყოფიერება. დასრულებული დანართის შექმნა ჩვეულებრივი პროგრამირების ენით ძალიან დიდ დროს მოითხოვს, მაშინ როცა პროექტირების სისტემა LabVIEW-ს სჭირდება სულ რამდენიმე საათი, რადგანაც პაკეტი შექმნილია სპეციალურად სხვადასხვა განზომილების დაპროგრამებისათვის, მას აქვს მოქნილი გრაფიკული ინტერფეისი და მარტივია პროგრამირებისათვის, იგი საუკეთესოა პროცესის მოდელირებისათვის, დანართების შექმნისათვის და უბრალოდ თანამედროვე პროგრამირების შესწავლისთვისაც.

LabVIEW-ის პროგრამები ადვილად პორტირდება სხვა პლატფორმებზე, შესაძლებელია დანართები შეიქმას სხვა სისტემაქში და შემდეგგაუშვათ ისინი Windows-ზე, თანაც ისე, რომ მასში მნიშვნელოვნად არაფერი შეცვალოთ, ისინი ადამიანის მოღვაწეობის ბევრ სფეროში აუმჯობესებენ მუშაობას, მათ შორის ტექნოლოგიური პროცესების ავტომატიზაციაში, ქიმიაში, ფიზიკაში და ა.შ.

პროგრამაა PROTEUS-ი, რომლისთვისაც ელემენტების სიმულაცია არა ერთადერთი უნარია, წარმოადგენს ე.წ. „გამჭოლი პროექტირების“ გარემოს, რაც ნიშნავს მოწყობილობის შექმნას მისი გრაფიკული გამოსახულებიდან მოწყობილობის დამზადებამდე წარმოების ყოველ ეტაპზე კონტროლის შესაძლებლობით. იგი თავის თავში აერთიანებს ორ ძირითად პროგრამას: ISIS-ელექტრონული სქემების რეალურ დროში დამუშავების და აწყობის საშუალებებს და ARES-ნაბეჭდი დაფების დამუშავების საშუალებებს. სხვა ანალოგური პროგრამული პაკეტებისაგან განსხვავებით, ისეთები როგორიცაა Multisim, Microcap და სხვა Proteus-ს აქვს კომპონენტების ძალიან ფართო ბიბლიოთეკა, მათ შორის პერიფერიული მოწყობილობებისთვისაც: შუქდიოდები და ინდიკატორები, ტემპერატურული გადამწოდები, რეალური დროის საათები, ასევე შეტანა-გამოტანის ინტერაქტიური ელემენტები: ღილაკები, გადამრთველები, ვირტუალური პორტები და გამზომი ხელსაწყოები, ხოლო მთელი რიგი მიკროკონტროლერების, კომპონენტებისა და მიკროსქემების დამატებით იგი გახდა უფრო ძლიერი და საშუალებას იძლევა მთლიანად შემოწმდეს მიკროკონტროლერების ბაზაზე შექმნილი მოწყობილობები.

Proteus-ის საშუალებით გადავწყვიტე სიგნალიზაციის სქემის აწყობა, ამ სქემის ერთ-ერთი მთავარი მოწყობილობაა მიკროკონტროლერი, სქემის საიმედობისათვის და ფუნქციონალურად სრულყოფისათვის გადავწყვიტე შემერჩია მიკროკონტროლერი Arduino Mega 2560.

ჩემს მიერ აწყობილი სქემა შეიძლება გამოყენებული იქნას, როგორც სახელმწიფო ობიექტებზე, ასევე კერძო შენობებისა და ფართების

დაცვისათვის. სქემაში გამოყენებულია შესასვლელი ერთჯერადი პაროლი, თუმცა შეიძლება მისი შეცვლაც, კარის გაღებისას სიგნალი აქტიურია 10 წამის განმავლობაში, შემსვლელი პირი სიგნალის განგაშის შესაჩერებლად კრებს 4 ციფრიან პაროლს (ჩვენს შემთხვევაში 1234). B ღილაკზე ხელის დაჭერისას ჩვენ შევდივართ პაროლის ცვლილების მენიუში, პაროლის შეცლის შემდეგ განგაშის შეჩერებას შევძლებთ მხოლოდ ახალი პაროლის აკრებით, თუ პაროლი შეყვანილია არასწორად, ეკრანზე მივიღებთ შეტყობინებას „კიდევ სცადეთ“. პროგრამის მუშაობის საწყის ეტაპზე ხდება ბიბლიოთეკის ინიციალიზაცია, მიკროკონტროლერის თითოეულ ფეხს ენიჭება გარკვეული ფუნქცია, ასევე მიმდინარეობს საწყისი პაროლის შეყვანა, კარის გაღებისას განგაშის სიგნალის გააქტიურება და ღილაკებისთვის ფუნქციონალური დატვირთვის მინიჭება. დაცვის სისტემა ძალიან სწრაფად რეაგირებს კარის გაღებაზე, კვამლზე და მინის გატეხვაზე. შესაძლებელია აგრეთვე მისთვის ფუნქციების დამატება, ასევე მასთან დამატებითი მოდულების მიერთების შედეგად სრულყოფა.

დასკვნა

1. შემუშავებული სქემა წარმოადგენს სახელმწიფო ობიექტის სიგნალიზაციის ერთ-ერთ შესაძლო ვარიანტს, რომელიც წარმატებით უზრუნველყოფს სხვადასხვა ტიპის ობიექტების დაცვას.
2. იგი აწყობილია მიკროპროცესორულ ბლოკზე და წარმოადგენს მოქნილ მოწყობილობას ფუნქციონალური ცვლილების თვალსაზრისით, მარტივია დასამზადებლად.
3. იაფია თვითღირებულებით, საიმედოა და აკმაყოფილებს თანამედროვე მოთხოვნებს, მისი მხოლოდ უმნიშვნელო ცვლილება უზრუნველყოფს აგრეთვე ერთდროულად რამდენიმე ობიექტის დაცვას, სისტემა საიმედოა შეუღწევლობის უზრუნველყოფით.
4. შესაძლებელია SMS შეტყობინებების გაგზავნა, მათი დამახსოვრება, ხასიათდება კვების მრავალსაათიანი ავტონომიურობით, მისი

გამოყენება მცირე პროგრამული და აპარატურული ცვლილებებით შესაძლებელია საკმაოდ ფართო სპექტრის ობიექტებისათვის.

Abstract

Software technologies of the embedded security systems

Security systems of the organization, company, office, industrial, housing and other types of buildings are the guarantee of their stable functioning. Complex control facilities are used for the safety of the entire unit: fire and security alarms, video-audio control and access systems.

Demands of the object by means of security depends on its category, architectural solution, working mode and many other factors that should be taken into account when designing a security system. The object of each group should be in compliance with certain security class and technical means of security system.

Modern complex security systems consider the protection of the object through four integral subsystems: protective and alarm systems, fire alarm systems, entry permission and access systems, and TV-video surveillance and control systems, various helper devices can be added to them.

High-technological base - programmable, logical integration schemes, have long been used to create specialized digital devices in the sphere of specialized controllers, communication systems, digital processing of signals, etc. Their usage is particularly actual in the realization of schemes of high productivity that are oriented to hardware realization . The hardware realization of different tasks ensures the parallelization of the process and thus increases the productivity compared to the software solution.

I have used "penetrating" system of "PROTEUS" for creating and designing security systems, which allows to sort out the work of the scheme without building a real device, find the errors that have been made during designing, remove the necessary features and many more. Proteus has a wide range of components, including those for peripheral devices: LEDs and indicators, temperature sensors, real time clocks, as well as input-output interactive elements: buttons, switches, virtual ports and measuring devices, but by adding a range of microcontrollers, components and microschemes, it has become more powerful and it gives an opportunity to completely check the microcontroller-based devices. Also, the advantage of this system is a flexible simulation environment, in particular it can create real systems, and the designer can create the proper and effective design before the system is actually created. The phases and the time of creating a particular design reduces the system cost price. The advantage of the system is also the simplification of replacing the components and connecting lines' easy route, it has the ability to study the abstraction of different levels and if the error occurs it will detect and correct it at the lower level, which will rectify the final result.

It is an architecture in which any additional models can be created in any case, most of their types can be used without addressing to coding, accordingly PROTEUS allows professional engineers to start the interactive simulation of real projects and get the result as an award, which corresponds to the scheme simulation. If this is not enough, the simulation models of a number of popular microcontrollers have been created, by mens of which it's possible to simulate the whole systems of microcontrollers and develop programs without addressing to their physical prototypes.

With the help of the Proteus I've decided to set up a scheme for signaling, one of the main devices of this scheme is the microcontroller, for the scheme reliability and its functional improvement I have chosen the microcontroller Arduino Mega 2560, with the help of this particular microcontroller not only signaling schemes but many other projects are managed, such as "smart" home, automated boiler, greenhouse industries with automatic control of soil moisture and salt composition, meteo stations and many more.

The scheme set up by me, can be used for the protection of state buildings, as well as private buildings and spaces. In the scheme, one time password is used to enter, but it can be changed with the help of the program, the signal is active for 10 seconds, while opening the door, the entrants are able to pick up a 4-digit password in order to stop the alarm. If the password is entered incorrectly, We'll get a message "try again" on the scream.

Thus, we may say that:

1. The designed scheme is one of the possible options of signaling on the state unit which successfully ensures the protection of different types of objects.
2. It is made on a microprocessor block and is a flexible device by means of function changing, its easy to make.
3. The cost is low, it's reliable and it satisfies modern requirements, the only minor change in it ensures the protection of several objects at the same time, the system is reliable by providing impenertability.
4. It's possible to send SMS messages, remember them, it is characterized by multi-hour feed authentication, it can be used for a wide range of objects with small software and hardware changes.