മാതൃഭൂമി
സത്യം സമത്വം സ്വാതന്ത്ര്യം

2019 ജനുവരി 29 • ചൊവ്വാഴ്ച
1194 മകരം 15 • വിശാഖം 20½ • നവമി 19½
1940 മാഘം 09 • 1440 ജമാദുൽ അവ്വൽ 22

ലത്തെ പ്പം കുട്ടുകയാണെങ്കിൽ
ാരിക്കലും വുദരവില്ല
ടോം സ്റ്റൊക്കാഡ് (ഇംഗ്ലീഷ് നാടകകൃത്ത്)

.എസ്.ആർ.ടി.സി.യുടെ അതിജീവനവഴി

തുമേഖലാസ്ഥാപനങ്ങളെന്നാൽ നഷ്ടക്കണക്ക് പറയുന്ന, കെടുകാര്യസ്ഥതയുടെ പ്രതീകം എന്നാ പൊതുധാരണ. അതുകൊണ്ടുതന്നെ കെ.എസ്. സി. അടക്കമുള്ള പൊതുസ്ഥാപനങ്ങളെ പൊ നുള്ള വെമ്പൽ നമ്മുടെ പൊതുബോധത്തിൽ ണ്ട്. തുടർച്ചയായി പുറത്തുവരുന്ന നഷ്ടക്കണ വസ്ഥയില്ലായ്മയും ഇതിന് ആക്കംകൂട്ടുന്നു. നമ്മു തുഗതാഗത രംഗത്തെ നിർണായകശക്തിയായ .ആർ.ടി.സി.ക്ക് ചരമക്കുറിപ്പെഴുതാനുള്ള തിടു തിയുടെ വിമർശനങ്ങളിൽ പോലും പലപ്പോ മാണ്. ഇപ്പോഴത്തന്നെ നാലായിരം കോടി രൂപ ണ്ട അവസ്ഥയിലാണെന്ന് സർക്കാർ അറിയിച്ച ങ്ങനെയെങ്കിൽ കെ.എസ്.ആർ.ടി.സി. അട യാണ് വേണ്ടത് എന്നായിരുന്നു സുപ്രീംകോ അഭിപ്രായം. രണ്ടാഴ്ച മുമ്പ് കെ.എസ്.ആർ.ടി. ഷൻ കേസ് അന്തിമ വാദത്തിനെത്തിയപ്പോ സുപ്രീംകോടതിയിൽനിന്ന് ഇത്ര രൂക്ഷവിമർ ളും ഏറ്റുവാങ്ങിയത്. സ്വന്തംകാലിൽ നിൽക്കാ പ്രത്യാശ നഷ്ടപ്പെട്ട നിലയിലായിരുന്നു ഏറെ എന്നാൽ, അതിനു മാറ്റം വരുത്താനാകുമെ .ആർ.ടി.സി.തന്നെ തെളിയിച്ചിരിക്കുകയാ ാൽ നൂറ്റാണ്ടിനിടെ സർക്കാരിൽനിന്നും കടം സ്വന്തം വരുമാനത്തിൽ നിന്നും മാത്രമായി നൽകാൻ കഴിയുന്ന മാസമായി മാറിയി 2019 ജനുവരി. ജനുവരി 31-ന് ജീവനക്കാ ങ്കിലേക്ക് പണമെത്തുന്നതോടെ തിരുത്ത വർഷത്തെ കെടുകാര്യസ്ഥതയുടെ ചരി കെ.എസ്.ആർ.ടി.സി.യെ ഈ നേട്ടത്തി ർത്തിയ തൊഴിലാളികൾക്കും മാനേജ്മെ തിനും ഒരുപോലെ അഭിമാനിക്കാവുന്ന ത്. ഇച്ഛാശക്തിയുണ്ടെങ്കിൽ, വഴിയി നേർവഴിക്കുതന്നെ ഒരു പൊതുമേഖ ലാ സ്ഥാപനത്തെ നട ത്താനാകുമെന്നതിന്റെ പ്രത്യാശാഭരിതമായ സാ ക്ഷ്യമായി ഇത്.

എല്ലാ മാസവും ശരാ ശരി 20 മുതൽ 30 കോടി രൂപ വരെ കെ .എസ്.ആർ.ടി.സി. സർ ക്കാർ സഹായം തേ മാസം ശമ്പ 9 കോടി രൂ പയാണ് വേണ്ടത്. ഡബിൾ ഡ്യൂട്ടി സമ്പ ദായം നിർത്തിയതോ

വോട്ടിങ് യന്ത്രം എത്ര സാധ്യമാണ് ഹാക്കിങ്

ഡോ. സുനിൽ തോമസ് തോണിക്കുഴിയിൽ

തിരഞ്ഞെടുപ്പ് പ്രക്രിയയിൽ വോട്ടിങ്‌യന്ത്രങ്ങൾക്ക് പ്രധാനപ്പെട്ട സ്ഥാനമുണ്ട്. അവയുടെ പ്രവർത്തനം കുറ്റമറ്റതും സുതാര്യവുമാക്കാൻ തിരഞ്ഞെടുപ്പു കമ്മിഷൻ അടിയന്തരമായി ഇതിന്റെ സോഫ്റ്റ്‌വേറും ഹാർഡ്‌വേർ ഡിസൈനും പൊതുജനത്തിന്റെ പരിശോധനയ്ക്കായി തുറന്നു കൊടുക്കണം. നമുക്ക് ഇനി പേപ്പർ ബാലറ്റിലേക്കുള്ള ഒരു തിരിച്ചുപോക്ക് അസാധ്യമാണ്. നമ്മുടെ ഫെഡറൽ സംവിധാനത്തെയും ജനാധിപത്യത്തെയും സംരക്ഷിക്കേണ്ട ബാധ്യത ഓരോ പൗരനുമുണ്ട്. അതിനാൽ സീസറിന്റെ ഭാര്യയെ പോലെ വോട്ടിങ് യന്ത്രങ്ങളും എല്ലാവിധ സംശയങ്ങൾക്കും അതീതമായിരിക്കണം.

ആദ്യമായി വോട്ടിങ് യന്ത്രത്തിന്റെ നിർമാണ സമയത്തെ ഹാക്കിങ് സാധ്യതകളും പരിശോധിക്കാം. ഇതിനായി യന്ത്രം എങ്ങനെയാണ് ഉണ്ടാക്കിയിരിക്കുന്നത് എന്ന് അറിയണം. യന്ത്രത്തിന്റെ നിർമാണത്തിന് ഉപയോഗിച്ചിരിക്കുന്ന സാങ്കേതികവിദ്യ ഡിസൈൻ സോഫ്റ്റ്‌വേർ എന്നിവയെപ്പറ്റി ഒരു വിവരവും തിരഞ്ഞെടുപ്പ് കമ്മിഷൻ ഔദ്യോഗികമായി പുറത്തുവിട്ടിട്ടില്ല. അതിരഹസ്യസ്വഭാവത്തോടെ കൂടിയാണ് ഇവയെല്ലാം കമ്മിഷൻ സൂക്ഷിക്കുന്നത്.

2010-ൽ ഹരി കെ. പ്രസാദ് എന്ന വ്യക്തി അനധികൃതമായി ഒരു യന്ത്രം എവിടെനിന്നോ സംഘടിപ്പിച്ച് യൂണിവേഴ്സിറ്റി ഓഫ് മിഷിഗണിന്റെ സഹായത്തോടെ യന്ത്രത്തിന്റെ സുരക്ഷയെപ്പറ്റി പഠനം നടത്തിയിട്ടുണ്ട്. യന്ത്രത്തിന്റെ ഉൾഭാഗത്തെ സംബന്ധിച്ച് പൊതുസഞ്ചയത്തിലുള്ള പ്രധാന രേഖ ഈ പഠനമാണ്.

കൺട്രോൾ യൂണിറ്റിനുള്ളിൽ രണ്ട് ബോർഡുകളുണ്ട്. മെയിൻ ബോർഡും ഡിസ്പ്ലേ ബോർഡും. മെയിൻ ബോർഡിൽ റൈനെസി എന്ന കമ്പനിയുടെ മൈക്രോകൺട്രോളർ ഉപയോഗിച്ചിരിക്കുന്നു. കൂടാതെ വോട്ടുകൾ സൂക്ഷിച്ചുവെക്കുന്നതിനുള്ള EEPROM (ഇലക്ട്രിക്കലി ഇറേസബിൾ പ്രോഗ്രാമബിൾ റീഡ് ഓൺലി മെമ്മറി) ബാലറ്റ് യൂണിറ്റുള്ള ഇൻറർഫേസ് എന്നിവയാണുള്ളത് . ഒറ്റത്തവണ മാത്രം പ്രോഗ്രാം ചെയ്യാവുന്ന മൈക്രോകൺട്രോളർ ആണ് യന്ത്രത്തിൽ ഉപയോഗിച്ചിരിക്കുന്നത്. ബാലറ്റ് യൂണിറ്റിൽ 16 സ്വിച്ചുകളും അവയ്ക്കു നേരെ ഓരോ എൽ.ഇ.ഡി. ലൈറ്റുകളും ഘടിപ്പിച്ചിട്ടുണ്ട്. ഇവയെ കൺട്രോൾ യൂണിറ്റിലേക്കു ഘടിപ്പിക്കാൻ വേണ്ട കണക്ടറും ഇതിനുള്ളിലുണ്ട്.

സാധ്യതകളും പ്രായോഗികതയും

തിരഞ്ഞെടുപ്പ് ഹാക്കിങ്ങിനുള്ള ആദ്യ സാധ്യത യന്ത്രത്തിന്റെ സോഫ്റ്റ്‌വേറിൽ ബാക്ക് ഡോർ പ്രോഗ്രാം ചെയ്യുക എന്നതാണ്. തിരഞ്ഞെടുപ്പ് സമയത്ത് ബാലറ്റ് യൂണിറ്റിലെ ഏതെങ്കിലും കികോമ്പിനേഷൻ ഞെക്കിയോ , മറ്റേതെങ്കിലും അനധികൃത മാർഗത്തിലൂടെയോ യന്ത്രത്തിൽ തിരിമറി നടത്തണമെങ്കിൽ ഇത്തരമൊരു ബാക്ക് ഡോർ അത്യാവശ്യമാണ്.

സോഫ്റ്റ്‌വേർ ഡിസൈൻ സമയത്ത് ഇത്തരം ഒരു ബാക്ക് ഡോർ ഇട്ടെങ്കിൽ മാത്രമേ ഇത് സാധ്യമാകൂ. ഇതിന് ഇപ്പോഴത്തെ യന്ത്ര [illegible] കുറവാണ്. ഇത്തരം ഒരു ബാക്ക് ഡോർ ഉണ്ടെങ്കിൽത്തന്നെ പോളിങ് ബൂത്തുകളിൽ കൂടി ഇത് ആക്റ്റിവേറ്റ് [illegible] കണക്കിന് ആളുകളുടെ സഹായം ആവശ്യമായി വരും. അതിനാൽ ഈ സാധ്യത നിലനിൽക്കുന്നുണ്ടെങ്കിൽത്തന്നെ പ്രായോഗികമായി നടപ്പിൽവരുത്താൻ ബുദ്ധിമുട്ടാണ്. ഇത്തരം ബാക് ഡോറുകളും നിലവിലില്ല എന്ന് നൂറു ശതമാനം ഉറപ്പുവരുത്തുന്നതിനായി തിരഞ്ഞെടുപ്പ് കമ്മിഷൻ സോഫ്റ്റ്‌വേറിന്റെ സോഴ്സ് കോഡ് തുറന്നുകൊടുക്കണം. കൂടാതെ ഹാർഡ്‌വേർ ഡിസൈനും സ്കീമാറ്റിക്കുകളും പരസ്യപ്പെടുത്തണം.

മൈക്രോകൺട്രോളർ ഒറ്റത്തവണ പ്രോഗ്രാം ചെയ്യാവുന്ന തരത്തിലുള്ളതാണെന്ന് ആദ്യമേ പറഞ്ഞിരുന്നല്ലോ. ഇന്ത്യയിൽ എഴുതിയുണ്ടാക്കിയ സോഫ്റ്റ്‌വേർ മൈക്രോകൺട്രോളറിലേക്ക് ഇങ്ങനെ സന്നിവേശിപ്പിക്കുന്നത് ഈ മൈക്രോകൺട്രോളർ നിർമിച്ച വിദേശ കമ്പനിയാണ്. ഈ സമയത്ത് വിദേശകമ്പനി മനഃപൂർവം പ്രോഗ്രാം മാറ്റുകയും അതിനുള്ളിൽ ബാക്ക് ഡോർ പ്രോഗ്രാം കയറ്റുകയും ചെയ്യുക എന്നുള്ളതാണ് അടുത്ത സാധ്യത. ഇതൊഴിവാക്കാൻ ഈ ഘട്ടത്തിൽ തിരഞ്ഞെടുപ്പ് കമ്മിഷനെറയും നിഷ്പക്ഷരായ സാങ്കേതിക വിദഗ്ധരുടെയും മേൽനോട്ടത്തിൽ ഈ പ്രോഗ്രാമിങ് പ്രക്രിയ പരിശോധിക്കേണ്ടതുണ്ട്. നിലവിലുള്ള യന്ത്രങ്ങളിൽ ഇത്തരത്തിൽ നിർമാണസമയത്ത് സോഫ്റ്റ്‌വേർ തിരുത്തലുകൾ നടത്തിയിട്ടില്ല എന്ന് കരുതാം.

മൈക്രോ കൺട്രോളറും മറ്റ് അനുബന്ധ ഘടകങ്ങളും പ്രിൻറഡ് സർക്യൂട്ട് ബോർഡിൽ ആക്കി സംയോജിപ്പിച്ചത് ഇന്ത്യയിലെ രണ്ട് കമ്പനികളാണ്. ഭാരത് ഇലക്ട്രോണിക്സ്, ഇലക്ട്രോണിക്സ് കോർപ്പറേഷൻ ഓഫ് ഇന്ത്യ ലിമിറ്റഡ് എന്നിവ. വിവിധ മോഡലുകളായി ഏകദേശം 13 ലക്ഷത്തോളം യന്ത്രങ്ങൾ ഇതുവരെ ഇവർ നിർമിച്ചിട്ടുണ്ട്. നിർമാണവേളയിൽ ഇതിന്റെ സർക്യൂട്ട്ബോർഡിലോ പെട്ടിയിലോ എവിടെയെങ്കിലും പുറത്തുനിന്ന് യന്ത്രത്തിന്റെ നിയന്ത്രണം കൈയടക്കാൻ പറ്റിയ പ്രത്യേക സർക്യൂട്ട് ഒളിപ്പിച്ച് വെക്കുക എന്ന സാധ്യതയാണ് ഇനിയുള്ളത്. ഫാക്ടറിക്കുള്ളിൽ വെച്ച് ഇത്തരം ഒരു മാറ്റംവരുത്തണമെങ്കിൽ വൻതോതിൽ വിഭവങ്ങളുടെയും മനുഷ്യശേഷിയുടെയും ആവശ്യമുണ്ട്. അതിനാൽ ഫാക്ടറികളിൽവച്ച് എല്ലാ മെഷീനുകളിലും ഇത്തരം ഒരു മാറ്റം രഹസ്യമായി ചെയ്യാൻ എളുപ്പമല്ല. ഇനി ഒന്നോ രണ്ടോ യന്ത്രങ്ങളിൽ ഇത്തരമൊരു മോഡിഫിക്കേഷൻ നടത്തിയാൽത്തന്നെ അവ കൃത്യമായി ഏതെങ്കിലും ഒരു ബൂത്തിൽ എത്തുമെന്ന് പ്രവചിക്കാനുമാകില്ല.

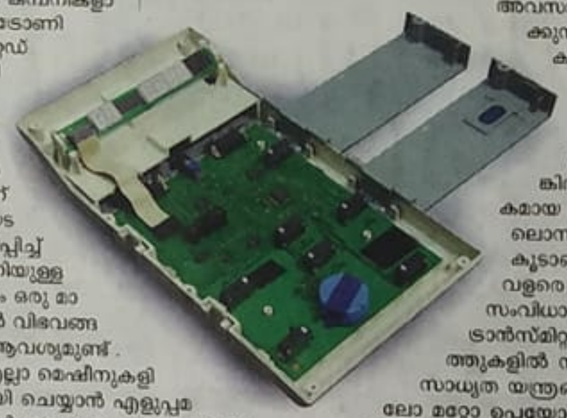
ബാലറ്റിങ് യൂണിറ്റിനെയും കൺട്രോൾ യൂണിറ്റിനെയും തമ്മിൽ ഘടിപ്പിക്കുന്ന കേബിളിൽ സർക്യൂട്ടുകളോ ട്രാൻസിറ്ററുകളോ ഉപയോഗിച്ച് തിരിമറി നടത്തുക എന്ന സാധ്യതയും നിലനിൽക്കുന്നുണ്ട്. ഇതിനും വ്യാപകമായ ആംശേഷി വേണ്ടിവരും. ഇത്തരം മാറ്റങ്ങൾ വരുത്താതിരിക്കാൻ ഈ രണ്ടു യൂണിറ്റുകൾക്കും ഇടയിലുള്ള ഡേറ്റാ ട്രാൻസ്മിഷൻ എൻക്രിപ്റ്റ് ചെയ്യണമെന്ന് തിരഞ്ഞെടുപ്പുകമ്മിഷൻ നിഷ്കർഷിക്കണം.

തിരഞ്ഞെടുപ്പ് കഴിഞ്ഞാൽ

ഇനി നമുക്ക് തിരഞ്ഞെടുപ്പ് നടന്നതിന് ശേഷമുള്ള അട്ടിമറി സാധ്യതകളും പരിശോധിക്കാം. യന്ത്രത്തിലെ വോട്ടുകൾ EEPROM എന്ന ഒരു ചിപ്പിലാകും സൂക്ഷിച്ചിരിക്കുക. യന്ത്രം തുറക്കാൻ പറ്റിയാൽ ഈ ചിപ്പിലെ ഡേറ്റ മാറ്റിമറിക്കാൻ പറ്റും. 2010-ൽ ഹരി കെ. പ്രസാദ്, അലക്സ് ഹാൽഡർമാൻ എന്നിവർ ഈ സാധ്യത ഉപയോഗിച്ച് വോട്ടിങ് യന്ത്രത്തിൽ തിരുത്തലുകൾ വരുത്താമെന്ന് കണ്ടെത്തിയിരുന്നു. ഒരു യന്ത്രം തുറന്ന് അതിലെ EEPROM ചിപ്പിന് മുകളിൽ ഒരു ചെറിയ സർക്യൂട്ട് പിടിപ്പിച്ച് വോട്ട് മാറ്റുന്ന രീതിയാണ് അവർ പ്രദർശിപ്പിച്ചത്. ഈ രീതിയിൽ മാറ്റണമെങ്കിൽ യന്ത്രം തുറക്കേണ്ടതായി വരും. ഇങ്ങനെ യന്ത്രം തുറക്കാതിരിക്കാൻ തിരഞ്ഞെടുപ്പു കമ്മിഷൻ ഒട്ടേറെ മുൻകരുതലുകളും എടുത്തിട്ടുണ്ട്.

എങ്കിലും ഇന്ത്യയിലെ എല്ലാ ഭാഗത്തും ഈ മുൻകരുതലുകളും നടപ്പാക്കുന്നുണ്ടോ എന്ന് ഉറപ്പുപറയാനാകില്ല. പ്രത്യേകിച്ചും തിരഞ്ഞെടുപ്പിനും വോട്ടെണ്ണലിനും ഇടയിൽ ദീർഘമായ ഇടവേളകളുള്ളപ്പോഴും. ഈ രീതിയിൽ തിരിമറി വ്യാപകമായി നടത്താൻ വൻതോതിൽ പരിശീലനം സിദ്ധിച്ച ആംശേഷിയും ലോജിസ്റ്റിക്കും ആവശ്യമാണ്. നമ്മുടേതുപോലെയുള്ള ഒരു ഫെഡറൽ ജനാധിപത്യ സമ്പ്രദായത്തിൽ രഹസ്യമായി ഇത്തരം ഒരു പ്രവർത്തനം നടത്താൻ ബുദ്ധിമുട്ടാണ്. മറ്റൊരു സാധ്യത യന്ത്രം തുറന്ന് ഡിസ്പ്ലേ മാത്രം മാറ്റിവെക്കുക എന്നതാണ്. ഇതിനും മുകളിൽ പറഞ്ഞ EEPROM തിരുത്തുന്നതിന്റെ പ്രശ്നങ്ങളുണ്ട്. വോട്ടിങ് യന്ത്രം തുറക്കാൻ കഴിഞ്ഞാൽ പല രീതിയിലും തിരഞ്ഞെടുപ്പ് ഫലം മാറ്റിമറിക്കാൻ കഴിയും. ഇതിനാൽ തിരഞ്ഞെടുപ്പിനും എണ്ണലിനും ഇടയിൽ യന്ത്രങ്ങളുടെ സുരക്ഷ അതിപ്രധാനമാണ്. അവസാനമായി ഷൂജ എന്ന വ്യക്തി ആരോപിക്കുന്ന ലോ ഫ്രീക്വൻസി ട്രാൻസ്മിറ്ററിന്റെ കാര്യം പരിഗണിക്കാം. ഇതിനായി യന്ത്രത്തിനുള്ളിൽ ഒരു റിസീവറും അതിനുവേണ്ടി ആൻറിനയും ഘടിപ്പിക്കേണ്ടതുണ്ട്. നിർമാണസമയത്ത് ഇത്തരം ഒരു സംവിധാനം പിടിപ്പിച്ചിട്ടില്ലെങ്കിൽ മുമ്പ് സൂചിപ്പിച്ചതുപോലെ വ്യാപകമായ ആംശേഷി ഉണ്ടെങ്കിലേ ഇത്തരത്തിലൊന്ന് യന്ത്രത്തിനുള്ളിൽ കയറ്റാൻ ആകൂ. കൂടാതെ ലോഫ്രീക്വൻസി ആൻറിനകൾക്ക് വളരെ നിളം വേണം. പുറത്തുനിന്ന് ഇത്തരം സംവിധാനങ്ങളെ നിയന്ത്രിക്കാൻ ശക്തിയേറിയ ട്രാൻസ്മിറ്റർ വേണം. ഇത്തരം ഒന്ന് പോളിങ് ബൂത്തുകളിൽ നടപ്പാക്കാൻ എളുപ്പമല്ല. പക്ഷേ, ഈ സാധ്യത യന്ത്രങ്ങളം സൂക്ഷിച്ചിരിക്കുന്ന ഗോഡൗണിലോ മറ്റോ ഉപയോഗിക്കാൻ പറ്റിയേക്കും. സാങ്കേതികമായി ഇത്തരം ഒരു സാധ്യത നിലനിൽക്കുന്നുണ്ടെങ്കിലും ഇപ്പോഴത്തെ യന്ത്രങ്ങളിൽ ഇത് ഇല്ല എന്ന് ഉറപ്പിക്കാം. തിരഞ്ഞെടുപ്പ് സംവിധാനവും നടപടി ക്രമങ്ങളും ഈ സാധ്യതയെ ഇല്ലാതാക്കുന്ന വിധത്തിലാണ് ക്രമീകരിച്ചിരിക്കുന്നത്. ഈ രീതിയിൽ റിമോട്ടായി ഫലം മാറ്റാനുള്ള സാധ്യത ഒഴിവാക്കാൻ തിരഞ്ഞെടുപ്പ് കമ്മിഷൻ യന്ത്രത്തിന്റെ കവർ അലുമിനിയം ഉപയോഗിച്ച് നിർമിച്ചാൽ നന്നായിരിക്കും. അലുമിനിയം പോലെയുള്ള ഒരു വൈദ്യുതിപാലകം കൊണ്ടുണ്ടാക്കിയ പെട്ടിക്കുള്ളിൽ റേഡിയോ സിഗ്നലുകൾക്ക് എത്തിപ്പെടാൻ ആവില്ല. ഒട്ടേറെ രീതികളിൽ യന്ത്രം ഹാക്ക് ചെയ്യാനുള്ള സാധ്യതകൾ പലരും പറയുന്നുണ്ടെങ്കിലും യന്ത്രത്തിന്റെ ഡിസൈൻ സമയത്ത് ഇതിനുള്ള സാധ്യത തുറന്നുവെച്ചിട്ടില്ല എന്ന് നമുക്ക് വിശ്വസിക്കാം. ഇവയെ മൊബൈൽ നെറ്റ് വർക്കിലോ വയർലസ് നെറ്റ്‌വർക്കിലോ ഘടിപ്പിക്കാത്തിടത്തോളം കാലം സുരക്ഷയെക്കുറിച്ച് അധികം ആശങ്കപ്പെടേണ്ടതില്ല. ഈ യന്ത്രങ്ങത്തിന്റെ ഡിസൈൻ നടന്ന കാലത്ത് ഇപ്പോഴും പറയുന്ന പല സാങ്കേതികവിദ്യകളും നിലവിൽ വന്നിട്ടുണ്ടായിരുന്നില്ല.

ഒട്ടേറെ രീതികളിൽ യന്ത്രം ഹാക്ക് ചെയ്യാനുള്ള സാധ്യതകൾ പലരും പറയുന്നുണ്ടെങ്കിലും യന്ത്രത്തിന്റെ ഡിസൈൻ സമയത്ത് ഇതിനുള്ള സാധ്യത തുറന്നുവെച്ചിട്ടില്ല എന്ന് നമുക്ക് വിശ്വസിക്കാം. ഇവയെ മൊബൈൽ നെറ്റ് വർക്കിലോ വയർലസ് നെറ്റ്‌വർക്കിലോ ഘടിപ്പിക്കാത്തിടത്തോളം കാലം സുരക്ഷയെക്കുറിച്ച് അധികം ആശങ്കപ്പെടേണ്ടതില്ല



(ആറ്റിങ്ങൽ കോളേജ് ഓഫ് എൻജിനീയറിങ്ങിലെ പ്രിൻസിപ്പലാണ് ലേഖകൻ)