



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2020-0085309
(43) 공개일자 2020년07월14일

- | | |
|--|--|
| <p>(51) 국제특허분류(Int. Cl.)
G05B 19/042 (2006.01)</p> <p>(52) CPC특허분류
G05B 19/0425 (2013.01)
G05B 19/042 (2013.01)</p> <p>(21) 출원번호 10-2020-7016241</p> <p>(22) 출원일자(국제) 2018년10월22일
심사청구일자 없음</p> <p>(85) 번역문제출일자 2020년06월05일</p> <p>(86) 국제출원번호 PCT/EP2018/078893</p> <p>(87) 국제공개번호 WO 2019/096545
국제공개일자 2019년05월23일</p> <p>(30) 우선권주장
10 2017 220 380.3 2017년11월15일 독일(DE)</p> | <p>(71) 출원인
케이에스비 에스이 엔드 코. 카게아아
독일연방공화국, 프랑켄트할 데-67227, 요한-클라인-스트라쎄 9</p> <p>(72) 발명자
보스바흐 프란츠 게르하르트
독일 프랑켄트할 67227 요한-클라인-슈트라쎄 9
케이에스비 에스이 엔드 코. 카게아아
브로테르젠 쾨케
독일 프랑켄트할 67227 요한-클라인-슈트라쎄 9
케이에스비 에스이 엔드 코. 카게아아</p> <p>(74) 대리인
리엔목특허법인</p> |
|--|--|

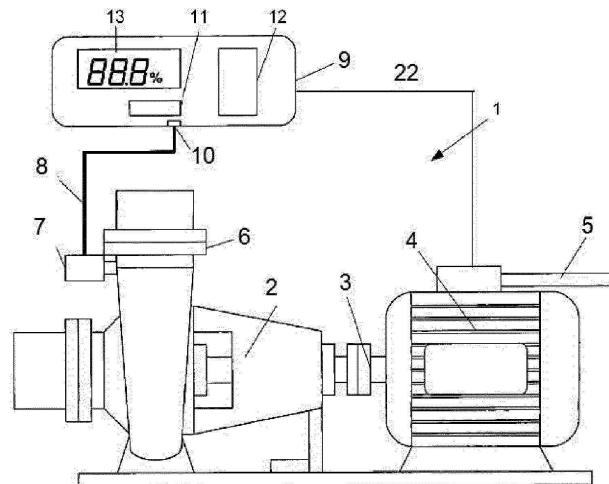
전체 청구항 수 : 총 12 항

(54) 발명의 명칭 **사이버 공격으로부터 펌프 유닛을 보호하기 위한 방법 및 장치**

(57) 요약

본 발명은 사이버 공격 발생시 변속 유체 전달 기기(2)(특히 원심 펌프), 구동기 및 제어 시스템을 포함하는 펌프 유닛을 보호하기 위한 방법에 관한 것이다. 상기 방법에 따르면, 상기 유체 전달 기기(2)의 속도 및/또는 속도 조절에 관한 신호들이 먼저 검출된다. 그 다음, 상기 펌프 유닛의 악의적으로 발생된 비정상적인 작동(사이버 공격)을 검출하기 위해 상기 신호들이 평가된다. 그 다음, 상기 분석된 신호로부터 유도된 적어도 하나의 실제 변수 및 적어도 하나의 공칭 변수가 비교된다. 그 후, 유닛(9)은 규칙들에 따라 유체 전달 기기(2)의 작동을 수행하기 위해 그리고 유체 전달 기기(2)가 현재 및/또는 다른 사이버 공격들로부터 보호되는 상태를 생성하기 위해, 상기 펌프 유닛의 컴포넌트들에게 신호들을 전송한다.

대표도 - 도1



명세서

청구범위

청구항 1

펌프 유닛을 보호하기 위한 방법으로서,

상기 펌프 유닛은 속도 제어되는 유체 전달 기기(2), 특히 속도 제어되는 원심 펌프, 구동기 및 제어 시스템을 포함하며,

상기 방법은, 사이버 공격들 동안 :

(i) 바람직하게는 적어도 하나의 센서에 의해, 상기 유체 전달 기기(2)의 속도 및/또는 속도 제어에 관한 적어도 하나의 제1 신호를 검출하는 단계;

(ii) 유닛(9)에 의해 상기 제1 신호를 평가하는 단계로서, 상기 평가 동안, 상기 제1 신호로부터 유도된 적어도 하나의 실제 변수 및 적어도 하나의 타겟 변수가 서로 비교되는, 단계;

(iii) 상기 유닛(9)이 상기 제1 신호의 평가에 기초하여 상기 펌프 유닛의 고의적인 불법 작동을 결정하면, 상기 유닛(9)에 의해 적어도 하나의 제2 신호를 출력하는 단계;

(iv) 상기 제2 신호에 반응하여, 상기 유체 전달 기기(2)의 제어-적합 작동을 야기하고 그리고 현재 및/또는 추가 사이버 공격으로부터 보호되는 상기 펌프 유닛의 상태를 야기하기 위해, 상기 유체 전달 기기(2) 및/또는 상기 제어 시스템 및/또는 상기 구동기의 컴포넌트들을 조정하는 단계를 포함하는, 방법.

청구항 2

청구항 1에 있어서,

상기 유닛(9)은 로컬 제어 및/또는 조절 기기이며, 바람직하게는 유체 전달 기기(2) 상에 또는 내부에 배열되고, 그리고 더 바람직하게는 컴퓨터 네트워크에 연결되거나 연결될 수 있는 것을 특징으로 하는, 방법.

청구항 3

청구항 1 또는 청구항 2에 있어서,

상기 유체 전달 기기(2)의 속도 제어는 상기 구동기에 연결된 주파수 변환기에 의해 제어되며, 상기 구동기는 전기 모터인 것을 특징으로 하는, 방법.

청구항 4

청구항 1 내지 청구항 3 중 어느 한 항에 있어서,

상기 유닛(9)은 상기 유체 전달 기기(2)의 저장된 행동 및/또는 학습된 행동과 비교하여 유체 전달 기기(2)의 스위칭 사이클, 제한 속도, 속도 변화의 기울기, 진동 및/또는 이상(anomaly)을 검출하는 것을 특징으로 하는, 방법.

청구항 5

청구항 1 내지 청구항 4 중 어느 한 항에 있어서,

상기 유닛(9)은 상기 유체 전달 기기(2) 및/또는 상기 구동기(4) 및/또는 상기 제어 시스템의 데이터를 위한 데이터 메모리를 갖는 것을 특징으로 하는, 방법.

청구항 6

청구항 1 내지 청구항 5 중 어느 한 항에 있어서,

상기 단계 (iv)는 사이버 공격 동안 상기 펌프 유닛의 전력 공급을 유지하기 위한 에너지 저장 기기의 활성화를

포함하는 것을 특징으로 하는, 방법.

청구항 7

청구항 1 내지 청구항 6 중 어느 한 항에 있어서,

상기 제1 신호의 평가가 상기 펌프 유닛의 정상 작동시 발생하지 않는 경미한 및/또는 영구적으로 작용하는 그리고/또는 규칙적으로 발생하는 그리고/또는 짧은, 집중적인 그리고/또는 증가하는 그리고/또는 구조적으로 발생하는 이상(anomaly)을 검출한다면, 상기 유닛(9)은 상기 펌프 유닛의 고의적인 불법 작동을 결정하는 것을 특징으로 하는, 방법.

청구항 8

청구항 1 내지 청구항 7 중 어느 한 항에 있어서,

상기 적어도 하나의 센서는 방사선 및/또는 음향 및/또는 진동 및/또는 압력 및/또는 유량 및/또는 속도 및/또는 온도 센서인 것을 특징으로 하는, 방법.

청구항 9

청구항 1 내지 청구항 8 중 어느 한 항에 있어서,

상기 단계 (iv)는 상기 펌프 유닛의 컴포넌트들, 특히 유닛(9)을 컴퓨터 네트워크로부터 분리하는 것 및/또는 상기 펌프 유닛의 자율적 작동을 포함하는 것을 특징으로 하는, 방법.

청구항 10

청구항 1 내지 청구항 9 중 어느 한 항의 방법을 수행하기 위한 유닛(9)으로서,

상기 유닛(9)은 유체 전달 기기(2), 구동기 및 제어 시스템을 갖는 펌프 유닛을 보호하도록 설정되며,

상기 유닛(9)은 바람직하게는 상기 컴퓨터 네트워크에 연결되며, 그리고 상기 적어도 하나의 제1 신호를 평가함으로써 상기 펌프 유닛의 의도적으로 야기된 불법 작동이 결정될 때 상기 컴퓨터 네트워크의 링크를 자동으로 차단하도록 설정되는 것을 특징으로 하는, 유닛(9).

청구항 11

청구항 10에 있어서,

상기 유닛(9)은 상기 적어도 하나의 제1 신호를 처리하기 위한 신호 처리 모듈(11), 상기 적어도 하나의 제1 신호를 평가하기 위한 평가 모듈(14), 상기 유체 전달 기기(2) 및/또는 상기 구동기 및/또는 상기 제어 시스템의 데이터를 갖는 메모리(15), 그리고 바람직하게는 입/출력 유닛(16)을 갖는 것을 특징으로 하는, 유닛(9).

청구항 12

청구항 10 또는 청구항 11에 있어서,

상기 유닛(9)은 상기 펌프 유닛을 제어-적합한 작동으로 변경하고 그리고 현재 및/또는 추가 사이버 공격들로부터 보호되는 상태로 변경하기 위해, 상기 적어도 하나의 제1 신호를 평가함으로써 상기 펌프 유닛의 의도적으로 야기된 불법 작동이 결정될 때 상기 펌프 유닛의 컴포넌트들의 구동/조절을 자동으로 수행하도록 설정되는, 유닛(9).

발명의 설명

기술 분야

[0001] 본 발명은 사이버 공격으로부터 펌프 유닛, 특히 원심 펌프 유닛(centrifugal pump unit)을 보호하기 위한 방법 및 장치에 관한 것이다.

배경 기술

[0002] 타겟팅된 원심 펌프에 영향을 미치거나 파괴하는 것은 사이버 공격 수단 중 하나이다. 사이버 공격은 외부에서

중요한 컴퓨터 네트워크의 특정 인프라에 대한 공격이다. 이러한 컴퓨터 네트워크는 또한 시스템 제어에 점점 더 많이 사용되고 있다.

- [0003] 펌프, 모터, 제어 전자 장치 및 필요한 경우 제어 밸브를 포함하는 원심 펌프 및 특히 원심 펌프 유닛은 생산 시스템에서 중요한 역할을 한다. 일반적으로, 원심 펌프는 조절되거나 조절되지 않은 전기 모터에 의해 구동된다.
- [0004] 해커가 사이버 공격을 통해 산업 시스템을 공격하는 경우 전원 공급 장치가 바로 중단되는 경우가 종종 있다. 그 결과, 생산 중단이 발생한다. 일반적인 섯다운보다 더 차별화된 방식으로 동작하는 공격에 대해서는 보다 복잡한 절차가 필요하다. 특정 프로세스들을 타겟팅하는 경우, 그것들의 구조 및 제어에 대한 정확한 지식이 필요하다. 이로 인해 특정 프로세스에 대한 공격이 더 어려워진다. 그러나, 유체를 사용하는 모든 프로세스들에는 다소 표준화된 설계의 유체 전달 기기가 있으며, 이는 전체 프로세스들보다 광범위하게 더 식별 가능하고 더 구조화된 방식으로 공격될 수 있다.
- [0005] 예를 들어, 원심 펌프의 속도는 사이버 공격에 의해 조작될 수 있다.
- [0006] 상기 조작의 결과로, 원심 펌프는 덜 유리한 효율 범위로 이동될 수 있으며, 이는 높은 추가 운영 비용을 야기시킨다. 또한, 원심 펌프의 구동 또는 원심 펌프 자체 또는 시스템의 다른 부분들을 부분적으로 또는 완전히 파괴할 수 있다.
- [0007] 펌프들은 시스템의 특정 용도에 맞게 정확하게 설계되고 구성된다. 일부 펌프는 손상이 발생한 후 교체 부품 또는 교체 펌프가 준비될 때까지 몇 주 또는 몇 달이 경과할 수 있도록 맞춤 설계된다. 최악의 경우 시스템은 그 때까지 정지 상태를 유지한다. 따라서, 유체 이송 기기에 대한 이러한 공격의 결과로 높은 생산 중단이 발생할 수 있다.
- [0008] 최악의 경우, 그러한 조작으로 인해 폭발이 발생할 수도 있다. 화학 시스템의 경우 그 결과는 치명적일 것이다. 석유 또는 가스 전달 시스템에서는 환경에 매우 큰 영향을 미칠 수 있다.
- [0009] 원심 펌프에서, 제어되는 속도 조절은 지정된 속도 조절이다. 이 제어는 펌프 속도를 작동에 필요한 값(출력 데이터)에 에너지 효율적으로 적용하는데 사용된다. 주파수 변환기를 사용한 속도 제어는 가변 유량 요구사항에 맞게 펌프 출력을 조정하는 가장 효율적인 방법이다.
- [0010] 속도가 제어되는 펌프는 특정 작업에 필요한 양의 에너지 만 사용한다. 주파수-제어 속도 제어는 다른 제어 방법들과 비교하여 최고의 시스템 효율을 제공하므로, 특정 목적을 위한 가장 효율적인 에너지 활용을 제공한다.
- [0011] 속도 제어되는 펌프들은 최대 작동점에 대한 고정 속도 펌프의 일반적인 절차를 대체하며, 최대 작동점으로부터의 초과 출력은 밸브에 의해 조절(throttling)된다. 이 제어 밸브는 펌프의 속도 제어의 결과로 필요하지 않더라도 작은 변경 및 공정 제어를 위해 여전히 사용할 수 있다.
- [0012] 원심 펌프의 속도는 예를 들어 사용되는 3상 비동기 모터의 주파수 및 전압 변화에 의해 설명된 주파수 변환기로 제어된다. 이 방법은 비교적 적은 비용과 높은 효율로 최적의 이점을 제공한다. 주파수 변환기는 모터가 다른 속도로 작동될 수 있도록, 사전 정의된 패턴에 따라 주 전원 공급 장치의 전압과 주파수를 변환한다. 이 유형의 주파수 제어에서는 다음과 같은 문제가 발생할 수 있다.
- [0013] - 모터의 소음(간혹 간접 소음으로서 시스템에 전달됨)
- [0014] - 모터에 대한 주파수 변환기의 출력에서 고전압 피크.
- [0015] 예를 들어 프로세스 자동화 및 대형 시스템 모니터링을 위해 시퀀스들을 측정, 제어 및 조정하기 위해, 많은 산업 분야에서 소위 산업용 제어 시스템들(industrial control system; ICS)이 사용된다. 이들은 생산 산업에서 자주 사용된다. 예를 들어, 펌프의 속도 또는 흐름을 제어하는 밸브의 위치는 이러한 시스템에 의해 영향을 받을 수 있다.
- [0016] 과거에는 ICS가 다른 IT 시스템 및 네트워크와 물리적으로 분리되어 외부 영향으로부터 보호되었다. 따라서 IT 보안의 중요성이 떨어졌다.
- [0017] 사무실 환경에 IT 시스템이 도입되고 ICS의 네트워킹이 증가함에 따라, 이러한 시스템들은 현재 기존 회사 IT의 시스템과 유사한 위협에 노출되어 있다.
- [0018] 공격자의 절차는 타겟에 따라 다르다. 인터넷을 통해 직접 접근할 수 있는 시스템에서는, 시스템에 대한 타겟팅

된 공격이 시작된다. 따라서 공격받은 시스템의 취약점이 직접 사용된다. 운영 체제 또는 서비스 응용 프로그램과 관련이 있을 수 있다.

- [0019] 최근에 알려진 많은 공격들에서, 회사로의 진입으로서 소위 스피어-피싱 공격(spear-phishing attack)이 사용된다. 이런 식으로, "교두보(bridgehead)" 유형은 회사의 컴퓨터를 대상으로 한다. 이 교두보에서 네트워크가 탐색되고 추가 시스템이 식별된다. 공격자가 실제 타겟 시스템에 도달하면, 그로부터 발견한 정보를 추출하고 조작을 수행한다. 공격자가 타겟에 도달하면, 자신의 발자취(track)를 가리고 미발견 상태를 유지하려고 시도한다.
- [0020] 다른 공격은 폐쇄형 시스템에 부주의하게 연결된 모바일 데이터 저장 수단을 통한 전파에 의해 폐쇄형 시스템을 목표로 한다. 루틴 자체는 모바일 데이터 저장 수단으로부터 관독됨으로써 설치된다.
- [0021] 산업 제어 시스템을 위한 사이버 보안 관리를 위한 컴퓨터 구현 방법은 EP 2 279 465 B1에 기재되어 있다. 여기에는 중앙 집중식 시스템 보안 관리자 프로그램 모듈이 제공된다. 이것은 처리 장치를 통해 도입될 수 있다. 중앙 집중식 시스템 보안 관리자 프로그램 모듈은 모니터링, 제어 및 데이터 수집 유닛의 통합 명령 및 제어 사용자 인터페이스에 통합된다.
- [0022] EP 2 500 579 A1은 전기 모터에 의해 구동되는 원심 펌프를 모니터링하는 방법을 기술한다. 전기 모터의 전력 소비 및 부하 전류는 토크 형성에 중요하다고 설명된다. 모터 제어 시스템에는 일반적으로 전력 소비 또는 부하 전류의 값들이 존재하기 때문에, 원심 펌프를 모니터링하기 위해 추가 센서가 필요하지 않다.
- [0023] EP 2 433 010 B1은 작업 기계의 작동점을 결정하기 위한 방법 및 장치를 설명한다. 작업 기계가 소비하는 전력량과 그 전달 속도는 작동점을 특징짓는다. 이 방법에서, 작업 기계의 작동점-의존 측정 변수는 센서에 의해 검출된다. 측정된 값들은 작동 중에 저장 및 평가된다.

발명의 내용

- [0024] 본 발명의 목적은 유체 전달 기기, 특히 원심 펌프, 모터, 제어 전자 장치, 그리고 필요한 경우 제어 밸브를 포함하는 진술한 펌프 유닛들, 특히 원심 펌프 유닛에 대한 사이버 공격이 효과적으로 방지될 수 있는 방법 및 장치를 제공하는 것이다. 펌프 유닛 자체의 컴포넌트들, 그리고 시스템에서 사용된 모든 컴포넌트들을 안정적으로 보호해야, 시스템 고장을 방지 할 수 있다. 상기 방법 및 장치는 시스템에서 구현하기가 간단해야 하며, 이로써, 기기 또는 개장(refitting)은 제조업체 및 운영자의 비용에 대한 가능한 최저 비용과 관련이 있다.
- [0025] 본 발명에 따르면, 이 목적은 청구항 1의 특징을 갖는 사이버 공격으로부터 펌프 유닛을 보호하는 방법 및 청구항 12의 특징을 갖는 방법을 수행하기위한 유닛에 의해 달성된다. 종속항, 설명 및 도면으로부터 바람직한 변형이 수집될 수 있다.
- [0026] 따라서, 먼저 사이버 공격 중에, 속도 제어되는 유체 전달 기기, 특히 원심 펌프, 구동기 및 제어 시스템을 포함하는 펌프 유닛을 보호하기 위한 방법이 제안된다. 본 발명에 따르면, 먼저 유체 전달 기기의 속도 및/또는 속도 제어와 관련된 적어도 하나의 제1 신호가 검출된다. 제1 신호의 검출은 또한 옵션으로 센서들에 의해 수행될 수 있다.
- [0027] 적어도 하나의 제1 신호는 유닛으로 포워딩되거나 유닛에 의해 획득되어 평가된다. 이 유닛에서, 평가의 맥락 내에서, 제1 신호로부터 유도된 적어도 하나의 타겟 변수 및 적어도 하나의 실제 변수는 서로 비교된다. 상당한 편차가 있거나 사전 정의된 제한값이 초과(overshooting) 또는 미달(undershooting)된다면, 유닛은 펌프 유닛에 대한 사이버 공격, 예를 들어 유체 전달 기기의 구동기 또는 유체 전달 기기에 연결된 다른 컴포넌트에 대한 사이버 공격이 발생했는지 여부를 판단할 수 있다.
- [0028] 이 평가 과정에서 유닛이 펌프 유닛(특히 구동기), 제어 시스템 및/또는 유체 전달 기기의 고의적인 불법 작동을 결정하는 경우, 적어도 하나의 제2 신호를 출력하여 반응하며, 그 결과, 펌프 유닛을 안전한 상태로 만들며, 이에 의해, 현재 및/또는 미래의 사이버 공격이 효과적으로 차단된다. 동시에, 상기 적어도 하나의 제2 신호에 대한 반응에서, 유체 전달 기기는 적절하게 조정되는 유체 전달 기기 및/또는 제어 시스템 및/또는 구동기의 컴포넌트들에 의해 제어-적합 작동(control-conformant operation)으로 변경된다.
- [0029] 바람직하게는 상기 유닛은 속도 제어식 유체 전달 기기 및 제어 시스템에 의해 수신된 신호들을 분석한다. 특히 다음 현상은 사이버 공격을 가리킬 수 있다 :
- [0030] - 제한 속도에 대한 체계적 접근

- [0031] - 신속한 시작 및 중지 사이클
- [0032] - 속도가 증가 또는 감소되는 고속 램프(fast ramp)
- [0033] - 진동의 가진(excitation of vibration)
- [0034] - 일반적인 행동과 비교하여 활성화의 이상.
- [0035] 적절한 입력 데이터를 분석한 후, 이 유닛은 펌프 유닛의 컴포넌트들로 신호를 보내, 사이버 공격으로부터 보호되는 안전 상태를 유지한다. 본 발명에 따른 방법은 중앙 네트워크에 대한 사이버 공격을 차단하고 펌프 유닛의 개별 컴포넌트들에 대한 사이버 공격을 차단하는데 적합하다.
- [0036] 제어 전자 장치 이외에, 하나 이상의 제어 컴포넌트, 예를 들어 제어 밸브는 또한 본 발명에 따른 펌프 유닛의 제어에 속할 수 있다.
- [0037] 본 사례에서 사이버 공격이라는 용어는 외부에서 불법 작동을 고의적으로 부과하는 행위를 나타낸다.
- [0038] 본 발명의 특히 유리한 변형에서, 유닛은 모니터링 모듈을 갖는다. 모니터링 모듈은 평가 유닛을 가질 수 있다. 그 다음, 평가 유닛은 메모리에 연결될 수 있다. 또한, 모니터링 모듈은 입력 유닛 및 출력 유닛을 갖는 것이 바람직하다.
- [0039] 본 발명의 유리한 변형에서, 모니터링 모듈은 모터 모듈에 연결된다. 모니터링 모듈 및 모터 모듈은 프로세스 제어 시스템 또는 네트워크로부터 완전히 분산(decentralized)될 수 있거나, 대안적인 변형으로, 프로세스 제어 시스템 또는 네트워크의 일부일 수도 있다. 모니터링 모듈이 펌프 유닛을 완전히 독립적으로 모니터링 할 수 있도록, 이를테면 안전 상태를 개시하고 적절한 경보를 출력할 수 있도록, 어떤 종류의 링크도 없는 것이 중요하고, 심지어 분리가 엄격해야 한다.
- [0040] 바람직하게는, 모터 제어 기기는 모터 모듈, 모니터링 모듈의 평가 유닛 및 구동기에 연결되며, 바람직하게는, 구동기는 전기 모터로서 형성된다.
- [0041] 펌프 유닛 또는 전체 시스템을 보호하기 위해, 펌프 유닛의 작동 파라미터들은 평가, 제어 및 조절 유닛에 의해 변화되며, 이로써, 유체 전달 기기의 구동기가 안정 상태로 진입하고 효과적으로 보호된다.
- [0042] 적절한 경우, 개별 단계들 또는 단계 시퀀스들 또는 전체 방법이 한 번 또는 여러 번 반복되는 반복 방법이 적용된다.
- [0043] 가능한 사이버 공격은 작동 파라미터들의 분석을 통해 검출된다. 이를 위해, 측정된 값들은 모터 제어 기기에 저장된 다수의 작동 상태 패턴들과 비교된다. 저장되지 않은 작동 상태가 펌프 유닛에서 감지되면 비상 상태가 자동으로 개시된다. 그 후, 바람직하게는, 구동기 및 유체 전달 기기 또는 전체 펌프 유닛은 사이버 공격이 수행된 네트워크로부터 분리되며, 이로써, 더 이상의 사이버 공격이 불가능하다. 이러한 방식으로, 의도하지 않은 작동 오류로 인한 오용을 피할 수 있습니다.
- [0044] 일 실시예에서, 구동기는 전기 모터가 되고, 유체 전달 기기의 속도 제어는 구동기에 연결된 주파수 변환기에 의해 수행된다. 바람직하게는, 이 경우에 적어도 하나의 제1 신호는 주파수 변환기의 상태 또는 작동 파라미터와 관련된다.
- [0045] 본 발명의 변형에서, 유닛은 분산 제어 및/또는 조절 장치이다. 이 유닛은 유체 전달 기기, 제어 시스템 또는 구동기에 또는 그 내부에 직접 부착될 수 있다. 상기 분산 유닛에 의해, 전체 프로세스 제어 시스템 또는 네트워크가 사이버 공격에 의해 이미 감염된 경우에도 사이버 공격으로부터의 보호가 가능하다. 독립적인 분산 유닛은 구동기 또는 유체 전달 기기의 적합하지 않은 작동 상태를 감지하여 사이버 공격을 감지할 수 있다. 또한, 상기 분산 유닛은 사이버 공격이 차단될 때까지 구동기, 유체 전달 기기 또는 펌프 유닛의 하나 이상의 다른 컴포넌트들을 네트워크 또는 프로세스 제어 시스템으로부터 분리할 수 있다.
- [0046] 본 발명의 바람직한 변형에서, 유닛은 명령 구조에서, 프로세스 제어 시스템, 또는 펌프 유닛 또는 이의 특정 컴포넌트들이 연결되는 네트워크와 비교하여 지배적인 방식으로 설정된다. 유닛이 사이버 공격을 감지하면, 펌프 유닛의 해당 컴포넌트들(예를 들어, 구동기 또는 제어 시스템의 일부들)을 프로세스 제어 시스템 또는 네트워크에서 완전히 분리하여, 펌프 유닛을 현재 공격과 추가 공격으로부터 보호한다.
- [0047] 보안 상태를 유지하는 것 외에도, 유닛은 추가적으로 또는 대안적으로 경고 메시지들을 개시할 수 있으며, 이로써, 조작자에게 탐지된 사이버 공격을 알린다.

- [0048] 본 발명의 변형에서, 유닛은 데이터 메모리를 갖는다. 데이터 메모리는 구동기 및/또는 유체 전달 기기 및/또는 제어 시스템 및/또는 펌프 유닛의 추가 컴포넌트들의 기술 데이터를 검출하고 저장하는데 사용된다.
- [0049] 바람직하게는, 유닛은 센서를 위한 적어도 하나의 단자를 갖는다. 특히, 진동, 압력, 유량 또는 온도 센서들은 사이버 공격 탐지에 적합하다.
- [0050] 구동기를 빠르게 켜고 끄는 것을 피하고 결과적으로 사이버 공격을 차단하기 위해, 예를 들어 배터리 또는 커패시터 조합으로서 구현될 수 있는, 에너지 저장 유닛이 사용될 수 있다.
- [0051] 또한, 유체 전달 기기 또는 구동기 내 진동의 가진(excitation)을 피해야 한다. 유발된 부하 변화에 의해, 예를 들어 (특히 원심 펌프 유닛으로서의 구성에서) 펌프 유닛의 임펠러와 가이드 휠 간의 상호작용, 또는 다른 컴포넌트들 간의 상호 작용은 유체 전달 기기 또는 전체 시스템 내에서 공진을 경험할 수 있는 압력 변동을 야기할 수 있다. 이들 공진 주파수의 타겟된 가진(excitation)의 경우, 유체 전달 기기의 또는 펌프 유닛이 배열된 전체 시스템의 손상, 심지어는 파괴를 초래할 수 있는 진동 진폭이 생성될 수 있다.
- [0052] 상기 상태들은 원심 펌프 유닛들의 제어 기기에 이미 알려져 있는데, 이는 시스템들을 시동 및 가동시킬 때, 손상을 입히지 않기 위해 가능한 빨리 이러한 작동 상태들을 극복해야 하는 문제이기 때문이다. 이미 알려진 시스템 데이터를 사용하여 사이버 공격 또는 인적 오류와 관련하여 타겟팅된 피해를 피할 수도 있다.
- [0053] 본 발명의 변형에서, 무정전 전원 장치(uninterruptible power supply; UPS)가 사용된다. 결과적으로, 사이버 공격 중에, 구동기 또는 펌프 유닛의 다른 부분들의 전원 공급이 보장될 수 있다.
- [0054] UPS의 또 다른 중요한 특징은 배터리 용량에 따라 달라지는 최대 바이패스 시간이다. 필요에 따라 몇 초 또는 몇 시간일 수 있다. 전력 및 바이패스 시간에 대한 수요가 높은 경우, 배터리를 재충전하기 위한 전력 생성 유닛들이 또한 사용될 수 있다.
- [0055] 본 발명은 또한 본 발명에 따른 방법을 수행하기 위한 유닛에 관한 것으로, 사이버 공격 동안 청구항 1의 프리앰블에 따라 펌프 유닛을 보호하도록 설정된다. 여기서, 본 발명에 따른 방법에서와 동일한 장점들 및 특성들이 발생한다는 것이 명백하며, 그 이유로, 이시점에서 반복되는 설명은 생략될 것이다.
- [0056] 바람직하게는 유닛은 컴퓨터 네트워크에 연결되고, 그리고 펌프 유닛의 의도적으로 야기된 불법 작동이 적어도 하나의 제1 신호를 평가함으로써 결정될 때 자동으로 컴퓨터 네트워크에 대한 연결을 차단하도록 설정된다.
- [0057] 일 실시예에 따르면, 유닛은 적어도 하나의 제1 신호를 처리하기 위한 신호 처리 모듈, 상기 적어도 하나의 제1 신호를 평가하기 위한 평가 모듈, 유체 전달 기기의 데이터를 갖는 메모리 및/또는 구동기 및/또는 제어 시스템 및 바람직하게는 입/출력 유닛을 갖는다.
- [0058] 유리하게는, 유닛은 펌프 유닛을 제어-적합한 작동으로 변경하고 그리고 현재 및/또는 추가 사이버 공격들로부터 보호되는 상태로 변경하기 위해, 적어도 하나의 제1 신호를 평가함으로써 펌프 유닛의 의도적으로 야기된 불법 작동이 결정될 때 펌프 유닛의 컴포넌트들의 구동/조절을 자동으로 수행하도록 더 설정된다.

도면의 간단한 설명

[0059] 본 발명의 추가 특징들 및 장점들은 도면을 사용함으로써 예시적인 실시예들의 설명으로부터 그리고 도면 자체로부터 수집될 수 있다 :

- 도 1은 원심 펌프 장치를 도시한다.
- 도 2는 사이버 공격을 차단하는 유닛의 블록도를 도시한다.

발명을 실시하기 위한 구체적인 내용

- [0060] 도 1은 원심 펌프로서 구현되고 샤프트(3)를 통해 구동기(4)에 연결된 유체 전달 기기(2)를 갖는 장치(1)를 도시한다. 예시적인 실시예에서, 구동기(4)는 원심 펌프(2)를 구동하는 비동기 모터(asynchronous motor)로서 구현된다. 구동기(4)는 주 공급 라인(5)으로부터 공급된다. 원심 펌프(2)의 압력 커넥터(6)에는 원심 펌프(2)의 가압측 압력 또는 최종 압력을 측정하기 위한 센서(7)가 배치된다. 센서(7)는 라인(8)을 통해 유닛(9)에 연결된다.
- [0061] 유닛(9)은 라인(22)을 통해 구동기(4)에 더 연결된다. 유닛(9)은 구동기(4) 및/또는 센서(7)로부터의 신호들을 평가하고, 결과적으로, 중요한 작동 상태들을 분석할 수 있으며, 이는 구동기(4)에 대한 사이버 공격에 대한 결

론이 도출될 수 있게 한다. 이를 위해, 유닛(9)은 본 발명에 따른 방법을 사용한다.

- [0062] 바람직하게는, 본 발명에 따른 방법을 수행하기 위해, 예를 들어 공칭 출력과 같은 구동기(4)의 특성 변수들이 사용된다. 이러한 파라미터들로부터 다른 파라미터들을 도출하거나 계산할 수도 있다. 유닛(9)은 센서들(7)로부터의 신호들을 검출하기 위한 적합한 단자들(10)을 갖는다. 단자들(10)은 예시적인 실시예에서 신호 입력들로서 구현된다.
- [0063] 예시적인 실시예에서, 유닛(9)은 신호 처리 모듈(11)을 갖는다. 신호 처리 모듈(11)은 예를 들어 비교적 높은 정확도로 회전음 주파수(rotational sound frequency)를 결정할 수도 있다.
- [0064] 유닛(9)에서 진행되는 방법은 컴퓨팅 모듈(12)에 의해 제어되고 조정된다. 또한, 유닛(9)은 바람직하게는 디스플레이 및 작동 요소(13)를 갖는다.
- [0065] 상기 장치에서, 예를 들어 펌프 흡입 압력을 검출하는데 사용되는, 추가 압력 센서 단자(도시되지 않음)가 제공될 수 있다. 또한, 장치는 추가 신호 입력들(도시되지 않음) 및/또는 예를 들어 파라미터들을 입력 또는 관측하기 위한 직렬 버스 인터페이스를 가질 수 있다.
- [0066] 도 2는 블록도를 도시하고 원심 펌프(2)를 제어하고 그리고/또는 조절하는 유닛(9)을 도시한다.
- [0067] 도 2에 따른 예시에서, 유닛(9)은 평가 모듈(14), 평가 모듈(14)에 연결된 메모리(15) 및 마찬가지로 평가 모듈(14)에 연결된 입/출력 유닛(16)을 갖는다.
- [0068] 유닛(9)은 모터 모듈(17)에 연결된다. 유닛(9) 및 모터 모듈(17)은 프로세스 제어 시스템(18)의 일부일 수 있지만 반드시 그럴 필요는 없다. 모터 제어 기기(19)는 모터 모듈(17), 원심 펌프(2)의 유닛(9) 및 구동기(4)에 연결된다. 원심 펌프(2)에는 공급 라인(20)을 통해 전달될 액체 매체가 공급되고 배출 라인(21)을 통해 전달될 매체를 펌핑한다. 위에서 언급한 컴포넌트들 간의 데이터 트래픽은 화살표로 표시된다.

부호의 설명

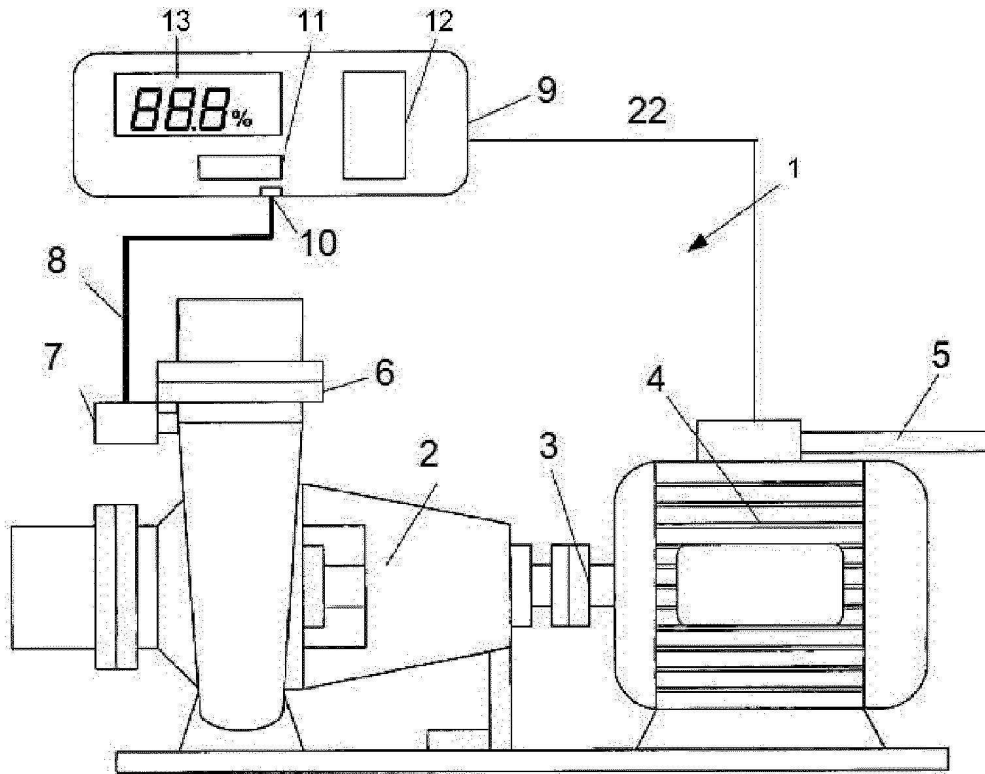
- [0069] 1 장치
- 2 유체 전달 장치(원심 펌프)
- 3 샤프트
- 4 구동기
- 5 주 공급 라인
- 6 압력 커넥터
- 7 센서
- 8 라인
- 9 유닛
- 10 단자
- 11 신호 처리 모듈
- 12 컴퓨팅 모듈
- 13 작동 요소
- 14 평가 모듈
- 15 메모리
- 16 입/출력 유닛
- 17 모터 모듈
- 18 프로세스 제어 시스템
- 19 모터 제어 기기

20 공급 라인

21 배출 라인

도면

도면1



도면2

