CERIAS

# Securing the Manufacturing Environment using Biometrics

**S.K.Modi, B.C.Harriger, S.J.Elliott, Ph.D, & M.R. Young**

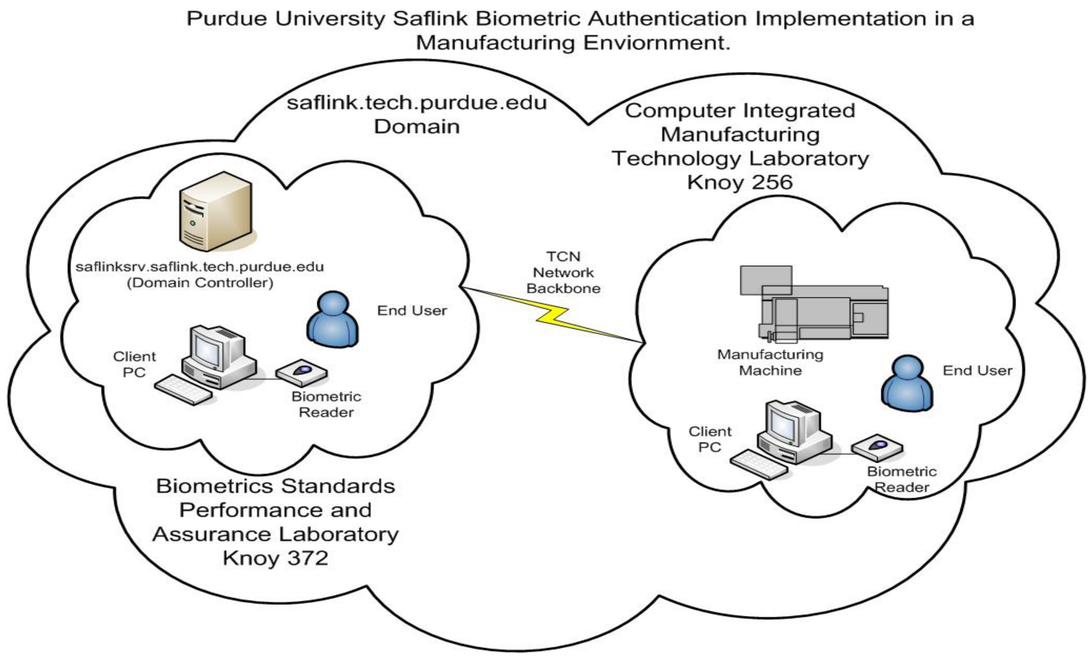
## Abstract

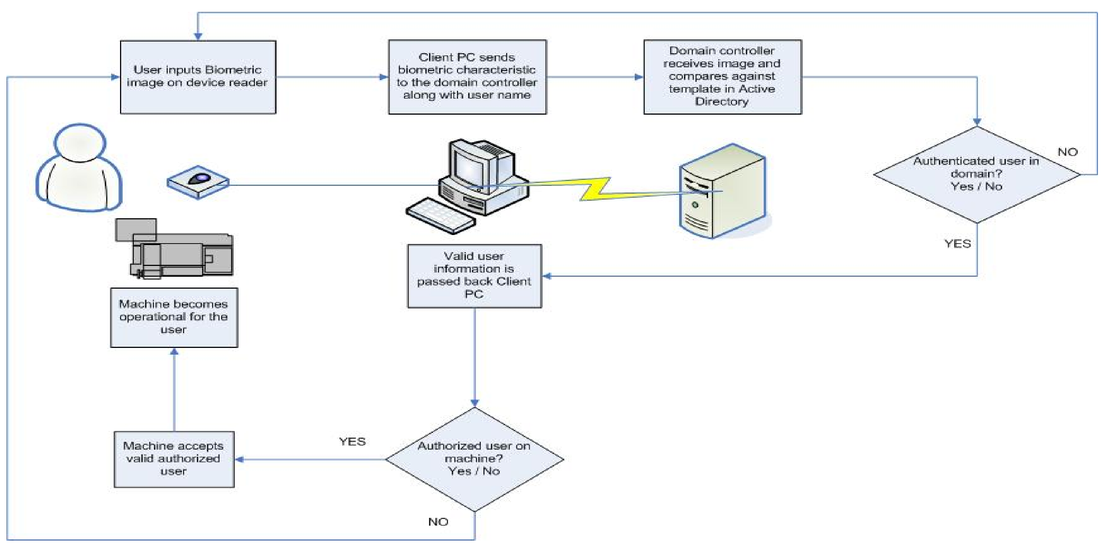
Computer integrated manufacturing systems have changed the interaction of industrial manufacturing equipment with different systems within and outside the manufacturing environment. The increase in the sophistication of the manufacturing equipment, along with increased connectivity with internal and external systems has changed the way that manufacturing security is designed. As manufacturers move towards a more connected collaborative environment in order to compete in global businesses and geographically disparate facilities, concerns that their proprietary manufacturing processes and intellectual property could be exposed to damaging compromise on a worldwide scale are increasing. The US government has also passed several regulations so that companies take into account general concerns like physical and logical security. The Sarbanes-Oxley Act of 2002 and FDA's 21 CFR Part 11 are two such regulations which require that companies have specific controls to ensure authenticity, integrity and auditability of electronic records. As part of the compliance guidelines, biometrics is indicated as a preferred means of security. The general problem that the manufacturing environment is facing is that operation of most industrial manufacturing equipment does not require any strong form of authentication or identification when some transaction related to product manufacturing takes place. Most manufacturing systems require a password to log onto the system, after which the system is open to anyone on the manufacturing floor to operate. The manufacturing systems are sophisticated enough to provide remote operation capability, but the only form of authentication is a password. There are no means to ascertain who was operating the machine and if they were authorized to do so. In an event of a malfunction or accident, the audit trail does not provide adequate information. Biometrics can solidify the authority checks and operator entry checks since the authentication is no longer based only on passwords or security cards/tokens. The main aim of this project is to demonstrate the integration of several biometric technologies into the manufacturing environment. This project proposes a unique application of biometrics and computer integrated technology as part of providing an applied solution for the problems of security and auditability in the manufacturing environment.

## Setup

Enrollment of all users of the system will take place at the administrator's machine. The administrator's machine is secured using single-sign-on using fingerprint scanner's provided by Precise Biometrics. The middleware software is provided by SAFlink. The logon for Human Machine Interface (HMI) is secured using face recognition. As part of securing the manufacturing environment, physical access to the facilities is also an important factor. This is done using hand readers provided by Recognition Systems. The verification process of the hand readers is tied in with the authentication process that takes place when an operator logs onto a HMI. If an operator did not enter the physical facilities using the hand reader, then the HMI will not allow the operator to log on until they have been authenticated using the hand reader at the entrance of the physical facilities. Along with authentication at the operating system level of the HMI, the HMI operators will also be authenticated at the application level. Different profiles can be set up for different operators, thus allowing separation of duties for using the manufacturing systems. Manufacturing systems allow for remote access for maintenance and production purposes. Using middleware software provided by SAFlink, an operator will be authenticated using iris recognition software provided by Iridian Technologies. This provides a strong form of authentication for remote operators, instead of just a generic password. All the biometric templates will be stored on central database which will be under the control of the system administrator. This allows for easier data management and authentication from multiple locations.

## Conceptual Design




## Sponsors

**Purdue:**

- Department of Industrial Technology
- Department of Computer Integrated Technology
- Center for Advanced Manufacturing
- Discovery Park

**Industry Support:**

Recognition Systems. · Rockwell Automation · saflink CORPORATION · PRECISE BIOMETRICS · iridian technologies · CHERRY · intel · identix Empowering Identification™

PURDUE UNIVERSITY · CERIAS · Discovery Park e-Enterprise Center