SaveGarde

Functional Safety in Manufacturing Processes

with the SaveGarde Production Suite:

FROST & SULLIVAN

2010 BEST PRACTICES AWARD

World Biometrics
Product Quality Leadership Award

Functional safety for people, achines and the environment

More than 30 Million people verified …
More than 40 trillion comparisons made …

Why Iris-Recognition?

The SaveGarde Production Suite provides the intelligent solution to the ever-increasing demand for functional safety in machines and plants. It reliably protects people, machines and the environment, while fulfilling current and future efficiency and flexibility requirements.

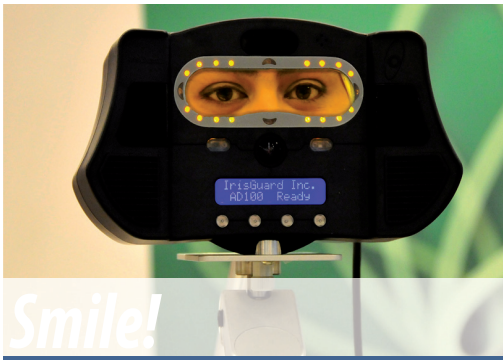
The Production Suite is designed to provide personated and traceable access control. Fields or applications are endless, such as in critical sections of automated systems or in safety relevant processes. Critical features are e.g. quality verification tasks, or any task with high financial impact in case of failure. Examples for safety relevant features are operations in petro-chemical production or handling fast moving units like robots. Lastly, contact-free identification is of advantage in dusty environments. The operator is biometrically identified and his release decision is automatically documented, mapped with a time stamp and his assessor number. The system communicates with all leading Quality Control systems and your verification process becomes faster, tangible and less susceptible to forgery than processes without time-stamped identification

Being *"... the first devices tested under IBG's cross- comparative methodology to achieve perfect transactional matching error rates (0.00% …)"*, our award-winning iris-recognition solutions are designed in support of a humane environment, where technology creates unprecedented levels of security while being non intrusive to the assessor.

The methodology is not DNA based, emits no radiation, is non-invasive, contact-free (no communicable diseases) and 10-times more accurate than fingerprints.

How does it work?

The assessor is enrolled once in an enrollment station, and mapped with his corporate assessor code. At the moment of any quality decision, the assessor is identified; a log file with assessor code and time stamp is passed to the production system. The cameras have an incorporated eye-finding mechanism, optimize light and focus (we learned from 24 million trial runs), detects glasses or lenses and can handle them, and verifies the eye's liveliness. The system can handle safety glasses and can operate in environments of dust and suboptimal illumination.



Iris Recognition is non-invasive, contact-free and emits no radiation

Technical Data on the Camera System:

Very Fast:
- 580,000 Comparisons/Second

Perfect Focus
- Auto focus
- Fine Focus
- Focus QC

Pupil Dilation
- Pupil/Iris ratio detection
- Flash tickler
- Eye Openness
- Openness QC

Specular reflections
- Glass neutralization

Ambient conditions
- Auto saturation
- Auto shutter speed
- Tolerant of lighting

Motion blur
- Auto shutter speed

Interfaces for 'solution in a box' application:
- Industrial quality server for continuous operation
- Scalable from small user sizes up to millions of users
- Operates as intra- and inter-corporate device
- Local or Web based Iris bank solutions
- Customer special surface with easy to use functions for enrollment, recognition and evaluation in combination with a reaction to the customer own automation and process level
- RJ45 (Gigabit) connection ports, USB ports
- Output data can be integrated in all relevant factory automation systems such as the SIMATIC Communication Processes, WinCC etc.
- Interfaces to PROFIBUS DP, PROFINET, CANBUS, DEVICENET, ETHERNET, TCP/IP etc
- IG-AD100 Camera
- Possible additional enrollment and recognition components as Chipcard reader, Passport reader

The security Model:

Imager USB protection
- 24 Byte OTP
- Two 3DES Keys
- SHA2 signature

Client-server-client protection
- Expiring OTP (5 seconds)
- SHA2 signature
- 3DES key (site specific)

Attack detection
- Client lockdown after 3 failed:
  - Recognitions
  - Acquisitions
  - Inquiries

Tamper-detection of:
- User Data
- Iris templates
- System logs

Template protection
- 3DES key (site specific)
- SHA2 signature
- Template never returned to caller.

Key generation
- Client generated
- Three keys (storage, transmission and images)
- 3DES-based
- Templates permutated

Client Authentication
- Username/password
- Username/password & Iris logon
- Username/MacID
- Username/MacID & Iris logon

Client Authorization
- Separate business and IT management
- Enroll, modify, delete, Recog and activate privileges.

Network separation
- Web servers and Database and Application servers can be on different segments

Data-Security Standards used:

Triple DES Encryption that complies with:
- FIPS PUB 46-3, Data Encryption Standard (DES), [FIPS46].
- FIPS PUB 74, Guidelines for Implementing and Using the NBS Data Encryption Standard, [FIPS74].
- FIPS PUB 81, DES Modes of Operation, [FIPS81].
- NIST Special Publication 800-20 Modes of Operation Validation System for the Triple Data Encryption Algorithm [TMOVS].

SHA-256 Digital Signature algorithms that complies with:
- FIPS PUB 180-2 Secure Hash Standard, [FIPS180].

The OTP random number generator that complies with:
- ANSI X9.31 Appendix A [AX931] (which replaces X9.17 Appendix C).
- FIPS PUB 140-2, Security Requirements For Cryptographic Modules [FIPS140] (as updated on 3 December 2002).
- Implementation Guidance for FIPS PUB 140-1 and the Cryptographic Module Validation Program [FIPS140IG].