ZEISS Predictive Service

Technologieinformationen zu unserem Remote-Service-Angebot

ZEISS Predictive Service

Technologieinformationen zu unserem Remote-Service-Angebot

Autor: Dr. Christian Schwindling, Marcus Jacob
Carl Zeiss Microscopy GmbH, Deutschland

Datum: Januar 2022

Dieses Dokument enthält eine Beschreibung der Architektur und der Sicherheitsmerkmale von ZEISS Predictive Service.
Es zeigt Ihnen als Entscheidungsträger im IT-Bereich, wie ZEISS Predictive Service in Ihrer Umgebung funktioniert und wie es Ihre technischen Sicherheitsanforderungen erfüllt. Außerdem behandelt es wichtige Themen wie die Kommunikation über Firewalls und Netzwerksicherheit.

Konnektivität

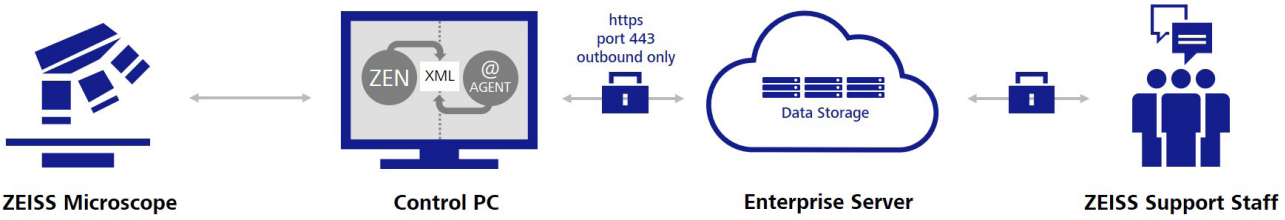


Abbildung 1 *Konnektivität*

Zentrales Element der Netzwerkkonnektivität ist der sogenannte Agent, ein kleines Softwarepaket, das auf dem Steuerungs-PC des Mikroskops installiert ist.
Es ist so konfiguriert, dass es als Windows-Dienst mit lokalen Systemrechten als „ZEISS Predictive Service Agent" ausgeführt wird. Während der Ausführung versucht der ZEISS Predictive Service Agent eine Verbindung zum ZEISS Enterprise Server unter predictive-service.zeiss.com mittels des HTTPS-Protokolls über den TCP-Port 443 und mit 256-Bit-TLS (Transport Layer Security) End-to-End-Verschlüsselung herzustellen.
Diese Verbindung ist ausschließlich ausgehend.
Das bedeutet, dass der Kommunikationskanal immer vom Agent initiiert wird, sodass der Agent Nachrichten lediglich über eine hergestellte Verbindung erhalten kann.
Dabei ist wichtig zu wissen, dass der ZEISS Predictive Service Agent niemals als Server fungiert und Ports für eine eingehende Verbindung öffnet, wodurch ein typischer Angriffsweg effektiv vermieden wird.

Wenn das lokale Netzwerk einen Proxyserver benötigt, kann die Serveradresse konfiguriert werden. Ist ein Benutzername und Passwort erforderlich, so wird das Passwort mittels der starken AES-256-Bit-Verschlüsselung im Installations-verzeichnis des ZEISS Predictive Service Agents gespeichert.
Meist ist es nicht nötig, die Firewall-Einstellungen zu verändern, wenn ausgehende HTTPS-Verbindungen zu predictive-service.zeiss.com bereits bewilligt sind.
Der Enterprise Server predictive-service.zeiss.com wird mittels der Microsoft Azure Cloud-Infrastruktur gehostet, die gemäß internationalen Standards (z. B. ISO 27001, HIPAA, FedRAMP, SOC1 und SOC2) zertifiziert und geprüft ist.
Die auf dem Enterprise Server ausgeführte Anwendung basiert auf PTC ThingWorx, das unter anderem die folgenden branchenüblichen Sicherheitsfunktionen beinhaltet: HTTP-Authentifizierung und -Autorisierung, Sub-Systeme mit Sicherheitsprotokollierung, verschlüsselte Speicherung aller sensiblen Daten (Login-Daten) und Unterstützung von

Transport Layer Security. Dadurch wird sichergestellt, dass alle Datenübertragungen verschlüsselt sind (TLS 1.2 mit Advanced Encryption Standard (AES) 256-Bit). Die Kommunikation zwischen dem ZEISS Enterprise Server und dem Agenten erfolgt entsprechend dem Secure-WebSocket-Standard.
In der Initialisierungsphase, in der der Agent eine sichere Verbindung zum Enterprise Server über HTTPS aufbaut, wird ein Web-Socket-Upgrade durchgeführt, um eine bidirektionale Kommunikation zwischen dem Agenten und dem ZEISS Enterprise Server zu ermöglichen.
Nach der Initialisierungsphase leitet der Agent die spezifischen Datenwerte, welche für die Überwachung der Daten zur Geräteintegrität oder die Erstellung von Kundenberichten wichtig sind, weiter.
Datenwerte können beispielsweise Betriebsstunden, Spannungen auf Komponentenebene oder Verbindungszustände sein. Die Protokolldateien werden ebenfalls über dieselbe bestehende Verbindung übertragen.
Jede Datenübertragung erfordert einen bestehenden Kommunikationskanal, der immer vom Agent initiiert wird.

Der Enterprise Server kann daher Daten nur über eine bestehende sichere Verbindung anfordern. Sobald die Verbindung aufgebaut wurde bleibt sie erhalten, bis aufgrund eines Verbindungsverlusts der Aufbau einer neuen Verbindung notwendig ist.

Zusammenfassung der Konnektivität

- ZeissPredictiveServiceAgent.exe läuft als Windows-Service
- Nur ausgehende, gesicherte Verbindungen über HTTPS und Port 443 mit 256-Bit-TLS/SSL-Verschlüsselung
- Keine offenen Ports für eingehende Verbindungen
- Unterstützung von Proxyservern
- Vorwiegend keine Änderungen der Firewall-Einstellungen
- Microsoft Azure Cloud-Infrastruktur, zertifiziert und geprüft gemäß internationalen Standards (ISO 27001, HIPAA, FedRAMP, SOC1 und SOC2)

Zustandsüberwachung

Dieser Abschnitt beschreibt den Anwendungsfall der Zustandsüberwachung, der auf dem oben beschriebenen Konnektivitätsmodell basiert. Die Zustandsüberwachung ist der systematische Abruf relevanter Informationen zur Geräteintegrität und deren serverbasierte Verarbeitung.
Ziel ist die Erkennung von Abweichungen bei der Geräteleistung, bevor sich diese auf die Versuchsergebnisse auswirken oder zu ungeplanten Ausfallzeiten führen.
Ein typisches Beispiel hierfür ist der vorbeugende Austausch einer mechanischen Komponente, die die maximale Anzahl von Bewegungszyklen erreicht hat. Zu den Informationen der Geräteintegrität gehören unter anderem Betriebsstunden, Bewegungszyklen motorisierter Komponenten, Spannungen auf Komponentenebene, Firmwareversionen und Fehlermeldungen. Der genaue Umfang ist gerätespezifisch.
Alle relevanten Daten werden von der Systembetriebssoftware des ZEISS Mikroskops gesammelt und in separaten Protokolldateien gespeichert (siehe Tabelle 1). Diese Dateien können mit einem Textviewer geöffnet werden.
Die Protokolldateien werden laufend von der Agent-Software überwacht. Wenn neue Daten gespeichert werden, analysiert der Agent die Protokolldatei und überträgt die Datenelemente über die bestehende Verbindung an den Enterprise Server.

Informationen zum Betriebssystem und zur Systembetriebssoftware (z. B. ZEN, SmartSEM) werden über die Registry und Windows Management Instrumentation (WMI) abgerufen. Diese Daten können die Version des Betriebssystems, die Seriennummer des PCs und die Festplattennutzung beinhalten.
Neben dem Durchforsten der Protokolldateien (Parsing) werden auch komplette Protokolldateien an den Server übertragen, um die ZEISS Supportmitarbeiter bei der schnellen Diagnose von Systemfehlern ohne manuellen Abruf der jeweiligen Protokolldateien zu unterstützen. Basierend auf unseren Tests erwarten wir einen durchschnittlichen Netzwerkverkehr von unter 2 MB pro Tag. Protokolldateien werden in der Regel einmal täglich hochgeladen, nachdem alle potenziellen personenbezogenen Daten anonymisiert wurden. Diese Schätzungen hängen stark von der Systemnutzung ab. Bei der erstmaligen Installation des Agenten wird während des Uploads historischer Daten ein überdurchschnittlicher Netzwerkverkehr erwartet. Nachfolgend finden Sie eine Liste aller Protokolldateien mit den dazugehörigen Speicherorten auf dem Systemsteuerungs-PC des Kunden.
Daten werden auf dem Server mit einem Zeitstempel gespeichert und auf vordefinierte Regeln überprüft.

Im Fehlerfall können so Aktionen ausgelöst werden, wie z.B., eine Benachrichtigung an den ZEISS Service. Daraufhin kann sich trainiertes und autorisiertes ZEISS Service Personal auf dem Enterprise Server anmelden, um den kompletten Datensatz und seinen Verlauf zu Diagnosezwecken zu prüfen. Aufgenommene Ergebnisse des Mikroskopbenutzers, wie Rohbilder oder verarbeitete Bilder, werden in diesem Datenstrom zu keiner Zeit übertragen, es sei denn der Nutzer erlaubt explizit eine Übertragung, z.B.: im Rahmen der ZEN Funktion "Automatic image upload".

Zusammenfassung der Zustandsüberwachung

- Es werden nur Protokolldateien von speziellen Protokolldatei-Speicherorten übertragen (siehe Tabelle 1). Diese Dateien sind vollständig transparent und als Klartext lesbar
- Benutzerspezifische Informationen oder Dateien sind von der ständigen Überwachung ausgenommen

Gerätetyp	Name der Protokolldatei	Beschreibung	Pfad
Elektronen-mikroskope	EM Server.log	Informationen zum EM Server	C:\ProgramData\Carl Zeiss\SmartSEM\Log\EM Server.log
Elektronen-mikroskope	Protokollordner	Beinhaltet SmartSEM Logs (GIS, FIB,…)	C:\ProgramData\Carl Zeiss\SmartSEM\Log
Elektronen-mikroskope	Ordner Momentaufnahme	Beinhaltet Capella System Momentaufnahmen	C:\ProgramData\Carl Zeiss\Capella\SystemBackups
Elektronen-mikroskope	Log Ordner	Datenüberwachung des EM Service Centers Software	C:\ProgramData\Carl Zeiss Microscopy GmbH\EmServiceCenter\DataMonitoring\External D:\EmServiceCenter\DataMonitoring\External
Licht-mikroskope	remote service.log.xml	Bereits geparste Informationen aus ZEN.log.xml und ZENCore.log.xml	C:\ProgramData\Carl Zeiss\Remote Service\remote service.log.xml
Licht-mikroskope	ZEN.log.xml	Informationen zur ZEN-Software	C:\ProgramData\Carl Zeiss\Logging
Licht-mikroskope	ZENCore.log.xml	Informationen zu ZEN core Software	C:\ProgramData\Carl Zeiss\Logging
Röntgen-mikroskope	XradiaAppn.log wobei n=1,2,….N verwendet bei System-Software v11.1 XradiaApp_n.log wobei n=1,2,….N verwendet bei System-Software v12	Informationen zu Versa-Systemparametern	C:\Program Files\Carl Zeiss X-ray Microscopy\Xradia Versa\XX.X.XXXX.XXXXX\Log Files

Tabelle 1: *Übersicht der Protokolldateien*

Optionaler Bild-Upload

Sie haben die Möglichkeit, die optionale Bild-Upload-Funktion für den automatischen Sample Finder zu wählen. Diese Option kann während des Aktivierungsprozesses oder im Anschluss daran im Einstellungsmenü des Predictive Service auf Ihrem System an- oder abgewählt werden. An diesen Stellen können die entsprechenden Allgemeinen Bedingungen dieser Funktion jederzeit eingesehen werden. Dieser automatische Sample Finder Bild-Upload hilft ZEISS hauptsächlich bei der Verbesserung von Machine-Learning-Modellen, um die Funktionen und die Effizienz des Sample Finders weiter zu verbessern.

Installation

Nach der Freigabe von Predictive Service durch Sie und Ihre IT-Abteilung gibt es zwei Optionen, um Ihr ZEISS Mikroskop an Predictive Service anzubinden. Voraussetzung für beide Optionen ist, dass Ihr System mit allen nötigen Sicherheitsmaßnahmen (z. B. Antivirus-Software) ausgestattet und mit dem Internet verbunden ist. Siehe unsere Empfehlungen zur Datensicherheit.

1. Vorinstallation durch ZEISS

Für ausgewählte Systemtypen (LSM, Axioscan, etc.) wurde die Predictive Service Agent Software bereits im Produktionsprozess bei ZEISS vorinstalliert. Wenn Sie Ihren Systembetriebs-PC zum ersten Mal starten, erscheint ein Pop-up-Fenster der Predictive Service Software und führt Sie durch den Aktivierungsprozess (z.B. Annahme der Geschäftsbedingungen, Internet-Einstellungen).

2. Installation über Desktop-Fernsteuerung per TeamViewer

- Alle erforderlichen Informationen und Dokumente werden an ZEISS gesendet und eine Installationssitzung per Fernzugriff wird vereinbart.
  Bitte klären Sie, ob spezielle Proxy-Einstellungen notwendig sind und falls ja, halten Sie diese bitte für die Installation bereit
- Sie erhalten eine E-Mail von ZEISS Service mit einem Link zum Download der TeamViewer-Quick-Support-Software.
  Bitte beachten Sie, dass diese Software nicht dauerhaft auf Ihrem PC installiert wird
- Starten Sie die TeamViewer-Quick-Support-Software und akzeptieren Sie die TeamViewer-Sitzungsanfrage und die Anfrage zur Fernsteuerung
- Der ZEISS Tech Support installiert den ZEISS Predictive Service Agent
- Testen Sie, ob die Verbindung zwischen der Agent-Software und dem Enterprise Server herstellt wurde

Unter diesem Link finden Sie weitere Sicherheitsinformationen zu TeamViewer:
https://dl.tvcdn.de/docs/en/TeamViewer-Security-Statement-en.pdf

3. Installation durch den Servicetechniker

- Alle erforderlichen Informationen und Dokumente werden an ZEISS gesendet und ein Ortstermin wird vereinbart.
  Bitte klären Sie, ob spezielle Proxy-Einstellungen notwendig sind und falls ja, halten Sie diese bitte für die Installation bereit
- Der ZEISS Servicetechniker installiert den ZEISS Predictive Service Agent
- Test, ob die Verbindung zwischen der Agent-Software und dem Enterprise Server herstellt wurde

Sicherheitsrelevante Updates

ZEISS aktualisiert die Predictive Service Software von Zeit zu Zeit, um die neuesten Funktionen und Sicherheitsupdates bereizustellen. Diese Updates werden automatisch installiert, es sei denn, Sie lehnen die Zustimmung zu den Allgemeinen Bedingungen für Predictive Service ausdrücklich ab. Falls Sie die Zustimmung verweigern, wird Predictive Service vollständig deaktiviert.

Technische Daten

Anschlüsse	443
Protokolle	HTTPS, Secure Websocket
URL der ZEISS Servers	predictive-service.zeiss.com www.predictive-service.zeiss.com
I-Adresse	52.174.243.245
Zertifizierung der Microsoft Azure Cloud-Infrastruktur	ISO 27001, HIPAA, FedRAMP, SOC1 und SOC2
Verbindungssicherheit	TLS 1.2 mit AES 256bit
Unterstützte Proxy-Einstellungen für die Installation	- Keine Authentifizierung - Standardauthentifizierung - Digestauthentifizierung - NTLM-Authentifizierung
Mit dem ZEISS System-PC verbundenes, verfügbares und gepatchtes lokales Netzwerk	RJ-45-Steckverbindung für LAN
Gepatchte Sicherheit und Maßnahmen gemäß Ihren lokalen IT-Sicherheitsstandards	Bspw. Installation von Antivirus-Software, siehe Empfehlungen für Datensicherheitsvorschriften für ZEISS Microscopy Systeme (siehe Referenzen)
Bestehende und funktionierende ausgehende Internetverbindung	

Überblick über die Datensicherheit

Dieser Abschnitt gibt Ihnen einen Überblick über Datensicherheitsstandards und -maßnahmen im Kontext des ZEISS Predictive Service IoT Produkts.

PTC ThingWorx IoT-Plattform

- Server-Sicherheit (aus Gründen der IT-Sicherheit werden individuelle Maßnahmen hier nicht aufgeführt)
- Sichere Konstruktionsprinzipien
- Authentifizierung und Autorisierung
- Matrix-Mehrmandantenfähigkeit
- Sicherheitsprotokollierungs-Subsystem
- Verschlüsselte Speicherung aller sensiblen Daten
- Empfohlene und unterstützte Sicherungsstrategie
- Schutz gegen häufige Schwachstellen
- Unterstützung für die Sicherheit der Transportschic
- Zusätzliche Sicherheitsmerkmale
- Dateiübertragung und Anwendungstunnelung mit ThingWorx EMS
- Sichere und skalierbare On-Demand-Zentren
- Konnektivitätssicherheit
- Anforderungen des Herstellers an die Produktsicherheit
- Endkundenanforderungen für angeschlossene Produkte

Microsoft Azure Cloud-Speicher

- Zugriffs- und Berechtigungsverwaltung
    - o Sicherheitsgruppen
    - o Berechtigungsstufen
    - o Zustände der Erlaubnis
- DDoS-Schutz
- Sicher durch Design
- Sicherheit der Berechtigungsnachweise
- Live-Antwort vor Ort
- Sicherheit des Dienstes
- Allgemeine Datenschutzverordnung (GDPR)
- Datenresidenz und Souveränität

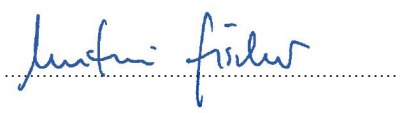
Prüfung und Validierung von Datensicherheitsmaßnahmen

- Kontinuierliche (tägliche) Prüfungen aufgrund automatisierter Tests von benutzerdefinierte implementierten Funktionen
- Auswertung von Berechtigungen für den Zugriff auf verschiedene Backend-Dienste von kundenspezifisch implementierten Funktionen
- Penetrationstests ("Pen-Tests") werden einmal pro Jahr von vertrauenswürdigen und verifizierten externen Partnern durchgeführt. Etwaige Ergebnisse werden fixiert.
- Kontinuierliche Aktualisierungen der Internet-orientierten Systeme und Kernabhängigkeiten
- Sichere Entwicklungsumgebung
    - o Zugang zum Büro
    - o Zugang zu den Systemen
    - o Trennung von Produktiv- und Testplattform
    - o Sicherung
- Versionskontrolle
- Kontrolle ändern
- Akzeptanztest
- Sichere Programmiertechniken
- Verschiedene Arten von Tests
- Keine Änderungen an Software von Drittanbietern (Ausnahme: Sicherheitslücken)
- Ausbildungsmaßnahmen von Mitarbeitern
- Kontrolle der ausgelagerten Entwicklung

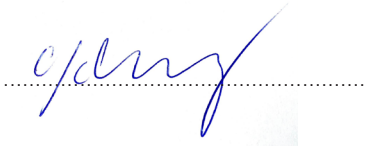
Referenzen

Empfehlungen für Datensicherheitsvorschriften für ZEISS Microscopy Systeme

AGBs Allgemeine Geschäftsbedingungen Predictive Service



Martin Fischer
Head of Global Service & Customer Care
ZEISS Research Microscopy Solutions



Dr. Christian Schwindling
Head of Remote Service & IT Support
ZEISS Research Microscopy Solutions

Carl Zeiss Microscopy GmbH
07745 Jena, Germany
Service and Customer Care
microscopy@zeiss.com
www.zeiss.com/microscopy