NCFirewall™ — Secure File Exchange Firewall for CNC Environments

Developed by Utah Informatics LLC, Salt Lake City, UT, USA

Utah Informatics, LLC
Kimberly von Zweydorff
570 S 300 W Unit S646
Salt Lake City, UT 84101
USA
Phone: (702) 728-8692
e-Mail: info@utahinformatics.com

1. Executive Summary

Modern CNC controllers cannot safely join a corporate domain. NCFirewall™ bridges that gap—providing a compliant, auditable, and secure way to exchange NC files between servers and CNC machines, closing multiple high-value NIST controls and accelerating CMMC compliance.

NCFirewall™ is a secure, auditable file-exchange gateway that bridges the gap between IT-managed servers and CNC controllers in manufacturing environments.
It was developed to fully comply with **CMMC** and **NIST 800-171 Rev. 2** requirements, enabling manufacturers to safely transfer NC program files while keeping vulnerable CNC systems isolated from the corporate network.

NCFirewall™ eliminates the need for USB drives or unsecured network shares. Only validated, authorized, and traceable files are exchanged to and from the machines.

It combines modern Windows architecture, compliance-oriented design, and shop-floor usability, making it the first complete solution for compliant CNC file exchange.

2. Background and Motivation

CNC machines form the operational core of precision manufacturing but operate on operating systems and software stacks that differ radically from enterprise IT.
Many controllers still rely on **Windows XP Embedded**, **Windows 2000**, **Windows 7**, or **Windows 10 LTS**, and cannot support modern security tools such as antivirus, patch management, or group policy enforcement.
Connecting such systems directly to a **domain controller (DC)** is **unsafe, unsupported, and non-compliant**.
NCFirewall™ was conceived specifically to solve this challenge: enabling secure, compliant, and auditable data transfer between modern IT infrastructure and legacy or OEM-locked CNC systems.

3. Solution Overview

NCFirewall™ acts as a **controlled intermediary firewall** between the secure server environment and isolated CNC controllers.
It enforces file-transfer policies, validates each file's authenticity, and maintains a tamper-resistant audit log of every event.

Core Capabilities

- **Secure file handling:** strict validation and policy enforcement
- **Audit trail:** complete transaction history in SQLite
- **User feedback:** machinist notifications for transfer success/failure
- **Network segmentation:** CNC systems reside on a protected subnet
- **Effortless IT integration:** operates as a regular domain user within Active Directory

4. Key Features and Advantages

- **CMMC / NIST 800-171 Compliance:** implements boundary control and logging required for certification.
- **Zero-Trust File Management:** each NC file must pass structural and syntax validation before release.
- **Centralized Audit Trail:** every transfer is timestamped, user-linked, and exportable.
- **Machine-Level Configuration:** per-machine directories, post-back options, and allowed extensions.
- **Secure Quarantine:** isolates non-compliant or failed transfers.
- **Operator Awareness:** desktop notifications confirm every action.
- **Hardware Option:** optional 5" industrial display shows live status on the shop floor.

5. Technical Architecture

NCFirewall™ is a **modern Windows/.NET application** built with security, maintainability, and compliance at its core.

- **Maintainable architecture** with modular service layers for file monitoring, validation, and auditing
- **Audit-friendly design**—immutable SQLite logging and timestamping for compliance evidence
- **Windows Server / Active Directory integration**—authenticated domain user with restricted permissions
- **Isolated machine network**—NCFirewall™ hosts an independent subnet for CNC controllers
- **Lightweight and robust**—runs continuously with minimal system load

6. Compliance Alignment (NIST 800-171 Rev. 2 & CMMC)

Control Family	Requirement	NCFirewall™ Measure
AC – Access Control	3.1.3 – Control CUI flow	Restricts NC-file movement to validated, authorized destinations.
AU – Audit & Accountability	3.3.1–3.3.8	Full audit logs with timestamps and export capability.
CM – Configuration Management	3.4.8 – Prevent unauthorized changes	Detects unverified or altered NC files and quarantines them.
MP – Media Protection	3.8.9 – Protect CUI on removable media	Replaces USB transfer methods entirely.
SC – System & Communications Protection	3.13.11 – Prevent unauthorized transfer	Enforces strict IT/OT network segregation.

NCFirewall™ helps manufacturers achieve and maintain **CMMC Level 2–3** readiness by satisfying multiple high-value controls in a single deployment.

7. Business and Operational Benefits

- **Compliance assurance:** built-in alignment with CMMC and NIST standards
- **Data integrity:** prevents execution of corrupt or incomplete NC programs
- **Cybersecurity:** isolates unpatched CNC systems from enterprise networks
- **Audit readiness:** instant evidence of data control for assessors
- **Ease of adoption:** minimal training, quick deployment
- **Low cost of ownership:** no external database or heavy infrastructure

8. Commercial Model and Pricing

Ownership

Utah Informatics LLC holds all intellectual-property rights.

Pricing

Component	Price
Per-Machine License (initial)	$999.00 one-time
Annual Shop Base License	$1,999.00 per year
Annual Per-Machine Maintenance	$499.00 per year
Optional Hardware Appliance	$3,999.00 incl. 12-month warranty
Extended Warranty	$300 / year (up to 5 years)

9. Proven Field Deployment

Deployed and validated at **Paramount Machine** on a diverse fleet of controllers:

Machine Type	Manufacturer	Operating Environment
5-Axis Mills (NMV, NHX)	Mori-Seiki / DMG-Mori	Windows XP → 10 LTS
Wire / Sinker EDM	Sodick	Windows 2000 / 7 Embedded
Horizontal Mills	Kitamura / Kiwa	Windows 10 LTS
Swiss & Screw Machines	Tsugami / Hanwha	Windows-based HMI
Inspection Systems	Zeiss / Keyence / Mahr	Windows 10 Embedded / Pro

Demonstrated compatibility across **legacy and current controllers** without OEM modification.

10. System Isolation Justification

Nearly all CNC controllers—DMG-Mori, Mori-Seiki, Kitamura, Sodick, Tsugami, Hanwha—**cannot safely join** a Windows Domain because:

1. **Outdated or Locked OS Images:** no patches, missing antivirus, frozen OEM builds.
2. **OEM Restrictions:** vendors forbid third-party software on timing-critical systems.
3. **Security Risks:** unpatched controllers expose the corporate domain if networked directly.

NCFirewall™ solves this by functioning as a **domain-managed endpoint** on the IT side while creating an **isolated OT subnet** for the machines.
This design fulfills the NIST 800-171 controls for boundary protection, CUI flow, and media protection.
To date, **no comparable compliant solution** exists—NCFirewall™ is the **first practical implementation** of this requirement.

11. Compliance Point-Benefits: With vs Without NCFirewall™

CMMC Scoring Overview

CMMC Level 2 audits evaluate ~110 NIST 800-171 controls. Each control carries 1–5 points; deductions reduce a shop's score from a possible 110. A passing score typically falls near 88.

Impact of NCFirewall™

Control Family	Requirement ID	Typical Points	Without NCFirewall™	With NCFirewall™
AC – Access Control	3.1.3	5	Uncontrolled file flow → −5 pts	Validated, restricted flow → 0 deduction
AU – Audit & Accountability	3.3.1	5	No audit trail for CNC files	Comprehensive logging → 0 deduction
MP – Media Protection	3.8.9	5	USB transfer risk	USB eliminated → 0 deduction
SC – System & Comms Protection	3.13.11	5	No boundary protection	Dedicated OT firewall → 0 deduction
CM – Configuration Mgmt	3.4.8	3	Unverified file changes	Automatic quarantine and validation → 0 deduction

Potential Improvement:
Shops typically lose **20–25 points** across these high-value controls. Deploying NCFirewall™ restores those points—often the difference between failing and passing **CMMC Level 2**.

12. NCFirewall™ vs. "NC Program/DNC" Tools (CMMC/NIST Compliance Lens)

The compliance problem we must solve

CMMC Level 2 requires implementing **all 110 NIST SP 800-171 Rev.2 requirements** across applicable systems—especially **boundary protection** and **controlled information flow** between IT and OT networks. Shops can *limit scope* and meet these controls by **isolating** CNC systems in **separate subnetworks with firewalls and information-flow mechanisms**.

Key need: a **domain-integrated middle layer** that (1) keeps controllers off the corporate domain, (2) **segments** the machine network, (3) **validates** and **audits** every file transfer, and (4) eliminates **USB/uncontrolled shares**.

What "NC program/DNC" tools actually do

- **CIMCO NC-Base / DNC-Max** – NC program/document management and DNC communications (RS-232/Ethernet), including program transfer and versioning. They **send programs** to machines; documentation does not claim controller network isolation or AD-integrated boundary enforcement.
- **ProShop ERP** – ERP/MES/QMS platform for scheduling, job docs, and quality. Strong shop-management features, **not** a boundary-protection/segmentation solution for CNC controllers.
- (Similar DNC tools exist—Predator DNC, ProEZDNC, etc.—focused on comms/transfer, not network segmentation or compliant boundary control.)

Why that's insufficient for CMMC/NIST 800-171

Typical DNC/ERP tools assume the machine is simply reachable (RS-232/FTP/Ethernet) and live on the same routable network—or reachable via adapters—without **guaranteeing**:

- **Network isolation / separate OT subnet** with a managed, auditable **firewall boundary**,
- **Active Directory–integrated mediation** (machine stays off the domain; the mediator is the domain principal),
- **File-validation + quarantine** before a program can reach the controller,
- **Complete transfer audit trail** bound to identity/time/machine for **assessment evidence**.

NIST explicitly points to **isolation via subnetworks and firewalls** and **information-flow control** as the way to bound scope around CUI systems—merely moving files via DNC/FTP does **not** establish this architectural separation.

Capability (what auditors look for)	NCFirewall™	CIMCO NC-Base / DNC-Max	ProShop ERP
Keeps controllers **off the domain** while the mediator is a **domain user**	✔ Designed for AD integration on IT side; machines on isolated OT subnet	❌ Not documented as a boundary/segmentation control	❌ Not a network boundary product
Network segmentation / **firewall** between IT and CNC (information-flow control)	✔ Purpose-built mediator/firewall layer	❌ Focus on program mgmt/DNC comms; no claimed boundary segmentation	❌ ERP/MES scope, not network security
Validated transfer (syntax/structure), **quarantine on fail**	✔ Built-in validation & quarantine	◑ Versioning/quarantine of changed programs exists, but not a security validation gate for OT isolation	❌ Not applicable
Full, exportable audit trail per machine/file/event	✔ Audit-oriented logging for assessments	◑ Program/document logs (not positioned as a compliance boundary log)	◑ ERP activity logs (not machine-transfer boundary logs)
Eliminates **USB / uncontrolled shares**	✔ Yes (policy-enforced gateway)	◑ Can reduce, but still relies on shop's network posture	◑ Out of scope
Aligns directly to **NIST 800-171** boundary/media/audit controls (e.g., 3.13.1/3.13.11, 3.8.9, 3.3.x)	✔ Designed for those controls	❌ Not documented as meeting boundary controls	❌ Not documented as meeting boundary controls

Sources:

CIMCO product pages/brochures; ProShop ERP overview; NIST SP 800-171; DoD CMMC alignment.

Bottom line

- **Other tools** manage programs and push files—but they **do not** provide the **architectural isolation** and **AD-integrated mediation** that NIST/CMMC expect for sensitive controller environments.
- **NCFirewall™** is (to our knowledge and based on public documentation) the **only solution** purpose-built to act as a **true middle-man**: an **IT-side domain principal** enforcing **policy, validation, quarantine, and full audit**, while maintaining a **separate OT subnet** for machines—exactly the isolation approach NIST describes.

If a shop is doing aerospace work today **without** this kind of boundary, they may be moving code—but they have **not closed** the controls auditors care about for **CMMC Level 2** (and they risk deductions).