(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 750 302**

(51) Int. CI.:

G06F 21/31 (2013.01)
G06F 21/62 (2013.01)
G06F 21/64 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **04.05.2015 E 15166199 (8)**

(97) Fecha y número de publicación de la concesión europea: **10.07.2019 EP 2983100**

(54) Título: **Protección de datos de un control numérico**

(30) Prioridad:

04.08.2014 DE 102014215310

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
25.03.2020

(73) Titular/es:

DR. JOHANNES HEIDENHAIN GMBH (100.0%)
Dr. Johannes-Heidenhain-Strasse 5
83301 Traunreut, DE

(72) Inventor/es:

RUTKOWSKI, CHRISTIAN

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Protección de datos de un control numérico

ÁMBITO DE LA INVENCIÓN

La presente invención se refiere a un procedimiento para la protección de datos de un control numérico para máquinas herramienta, si esos datos están archivados en formato tabular en el sistema de archivos de controles numéricos. En este caso, a menudo se desea proteger, al menos una parte de los datos, que pueden concernir a los más diferentes aspectos del control o de la máquina herramienta, contra modificaciones accidentales o no autorizadas.

ESTADO DE LA TÉCNICA

En los datos del control numérico están archivadas informaciones, con las que el control se adapta a un tipo determinado de máquina herramienta o, también, a una máquina herramienta muy concreta.

El documento EP 1914612 B1 describe un ejemplo para datos archivados en formato tabular. Los datos conciernen aquí a la cinemática de una máquina herramienta, al describir consecutivamente los diferentes ejes de la máquina, que conducen desde el punto central de la máquina hasta la bancada de la máquina. Estos datos son iguales para todas las máquinas de un tipo. Sin embargo, también se configuran determinados errores del eje y se archivan en formato tabular, que son específicamente para un máquina muy concreta. De ello, resulta la necesidad de permitir a diferentes encargados y en diferentes momentos, editar los datos contenidos en una tabla así. Además es deseable proteger determinadas entradas en tales tablas de configuración contra modificaciones accidentales o no autorizadas.

Por el documento US 6725240 B1 es conocido un procedimiento con el que se pueden reconocer las modificaciones posteriores de datos del registro archivados de manera tabular. Para ello, a la tabla se le añade una columna adicional de seguridad en la que se registra, respectivamente, un valor de huella digital de las otras celdas de una fila de la tabla. Mediante este valor de huella digital se pueden reconocer modificaciones realizadas posteriormente, cuando al leer los dataos de un fila de la tabla se calcula de nuevo su valor de huella digital y se compara con el valor de huella digital registrado en la columna de seguridad de esa fila. Con este procedimiento de hecho se pueden reconocer modificaciones, pero no se pueden evitar.

Por el documento US 7155612 B2 es conocido ajustar, por medio de un sistema de base de datos protegida completo, para la administración de derechos de acceso de usuario individuales, tanto el acceso de lectura como de escritura a determinadas partes de una base de datos existente en formato tabular. Un sistema de este tipo sería, sin embargo, demasiado costoso para un control numérico.

Por el documento US 2014/0165166 A1 es conocido un procedimiento, con el que se controla el acceso a un objeto almacenado digitalmente por medio de una contraseña y una función de huella digital. En este caso, un contador detecta la cantidad de los accesos. La cantidad se tiene en cuenta en la función de huella digital, de modo que tras una determinada cantidad de accesos ya no es posible otro acceso.

COMPENDIO DE LA INVENCIÓN

Es por ello misión de la invención, especificar un procedimiento para la protección de datos de un control numérico, con el que se pueden proteger, de manera particularmente sencilla, datos archivados en formato tabular contra modificaciones no autorizadas o accidentales. En este caso, debe ser posible que los datos se puedan procesar y proteger por diferentes instancias.

Esta misión se resuelve mediante un procedimiento de acuerdo con la reivindicación 1. Detalles ventajosos de este procedimiento resultan de las reivindicaciones dependientes de la reivindicación 1.

Se describe un procedimiento para la protección de datos almacenados en una tabla de un control numérico para máquinas herramienta contra modificaciones no autorizadas o accidentales, de acuerdo con el que en una columna de seguridad de la tabla está archivada una información sobre la protección de los datos contenidos en una fila seleccionada, con los siguientes pasos:

- primera introducción de una contraseña en una celda actual, que se encuentra en la fila seleccionada, de la columna de seguridad,

- cálculo de un nuevo valor de huella digital de la contraseña y almacenamiento de este valor de huella digital en la celda actual como valor de huella digital almacenado,

en donde, en caso de acceso de nuevo de escritura en una fila seleccionada así protegida, se introduce nuevamente la contraseña en la celda actual de la columna de seguridad y se calcula el nuevo valor de huella digital de la contraseña de nuevo introducida y se compara con el valor de huella digital almacenado en la celda actual de la

columna de seguridad, liberándose solo el acceso de escritura en la fila seleccionada, cuando el nuevo valor de huella digital coincide con el valor de huella digital almacenado.

La primera introducción de una contraseña en la celda actual de la columna de seguridad significa, por lo tanto, que esta contraseña no se escribe directamente en la tabla, sino que, en primer lugar, se genera un valor de huella digital, que entonces se archiva en la tabla. Dado que a partir de un valor de huella digital de este tipo no se puede calcular la contraseña inicial o solo con alto costo, el valor de huella digital en la tabla se puede leer, de hecho, por medio de diferentes programas estándar (p. ej. editor de texto), sin embargo, con ello la contraseña no se da conocer.

Al visualizar una tabla en la interfaz de usuario del control numérico, en lugar del valor de huella digital se visualizan únicamente comodines, que indican inmediatamente al operador que la fila en cuestión solo puede modificarse mediante introducción de nuevo de la contraseña correcta. También, con la nueva introducción de la contraseña no se escribe directamente esta contraseña en lugar de los comodines en la tabla, sino que únicamente se crea un valor de huella digital de la contraseña introducida de nuevo, que luego se compara con el valor de huella digital almacenado.

Para hacer reconocibles de inmediato modificaciones en la tabla por medio de programas estándar fuera del software de control propiamente dicho, el control debería también crear para cada una de las filas otro valor de huella digital (incluida la contraseña almacenada como valor de huella digital) y, también, archivarlo en la columna de seguridad (o una columna separada). Por lo tanto, se puede reconocer de inmediato una manipulación de la tabla en la lectura del control y confirmarse con un correspondiente mensaje de error.

Otras ventajas y detalles de la presente invención resultan de la siguiente descripción de la invención mediante las figuras.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

En este caso, muestra

la Figura 1, una tabla con datos de un control numérico,

la Figura 2, un diagrama de flujo para el procedimiento para la protección de datos almacenados en la tabla.

DESCRIPCIÓN DE LAS FORMAS DE REALIZACIÓN

La Figura 1 muestra una tabla T, en cuyas filas y columnas están archivados datos de un control numérico. Los datos a1-h4 propiamente dichos están, en este caso, archivados en las columnas D1-D4 de datos. En una columna Z de números de fila están numeradas las filas de la tabla T, en una columna S adicional de seguridad están archivados los datos importantes para el procedimiento de acuerdo con la invención.

La tabla T se almacena en el sistema de archivos del control numérico, preferiblemente, en un formato de texto con formato fijo, o en otro formato legible por programas de PC habituales. Esto posibilita modificar los datos de manera no autorizada con programas no previstos para ello, p. ej., un editor de texto. Además, los datos almacenados pueden falsearse por un defecto del medio de almacenamiento.

El control numérico visualiza a un usuario la tabla T de la manera representada en la Figura 1. El usuario puede seleccionar una fila y, entonces, introducir y/o modificar los datos individuales contenidos en esa fila. En la Figura 1 está enmarcada la fila N seleccionada actualmente para el procesamiento.

Si en una fila N seleccionada en la celda X actual de la columna S de seguridad se visualizan comodines P, de esta manera, esto indica al usuario que las modificaciones son solo posibles cuando se introduce una contraseña en lugar de los comodines P. Un valor H1 de huella digital de esta contraseña está almacenado en la columna S de seguridad en cada una de las filas protegidas. Si no hay asignado un valor de huella digital en un fila, de esta manera, los datos en esa fila pueden modificarse sin la introducción de una contraseña. Si, sin embargo, en una fila de este tipo se introduce una contraseña, de esta manera, se crea un nuevo valor H2 de huella digital de esa contraseña y se almacena en la columna de seguridad (y, por lo tanto, al valor H1 de huella digital almacenado), de modo que esa fila de inmediato está protegida contra modificaciones con aquella contraseña y se visualizan los comodines P en la columna S de seguridad.

En lugar de los comodines P, por supuesto, también podría visualizarse el propio valor H1 de huella digital. Dado que éste, sin embargo, no contiene información útil para el usuario (aparte de que la respectiva fila está protegida), se prefiere la visualización de un comodín P.

Para un usuario es por lo tanto fácil de reconocer mediante el comodín P, qué filas de la tabla T están protegidas con una contraseña. Además, el usuario puede proveer con una contraseña de manera muy sencilla a una fila no protegida. Dado que cada una de las filas puede protegerse con una contraseña propia, por consiguiente, una contraseña tiene efecto fundamentalmente en relación con una fila, las filas pueden protegerse por diferentes instancias.

De esta manera, en el ejemplo arriba mencionado de una tabla cinemática, se pueden proteger por el fabricante de la máquina aquellas filas que describen la construcción fundamental de un tipo de máquina herramienta a ser controlada. Las filas que describen la cinemática específica de la máquina, debido a desgaste, eventualmente, incluso errores de la cinemática que cambian con el tiempo, se pueden medir más tarde por un técnico de servicio en una máquina herramienta concreta, se introducen en la tabla T y se protegen. Un operador de esa máquina herramienta, que todavía debe introducir en la tabla T, eventualmente, los datos de una situación de montaje concreta, no puede modificar los datos detectados anteriormente y registrar sus datos solo válidos para un proceso de procesamiento sin protección en la tabla T.

Para la modificación o la edición de una fila también hay que tener en cuenta el borrado de una fila. También, para ello, en una fila protegida es necesaria la introducción de la contraseña correcta.

Se puede volver a borrar una contraseña, de modo que la fila después ya no está protegida. Para ello, por ejemplo, se puede especificar un símbolo que esté prohibido como primer símbolo para una contraseña o bien se ignora. Pues bien, si se introduce este símbolo seguido de la contraseña correcta en la columna S de seguridad de la fila hasta ahora protegida, de esta manera se borra la contraseña.

Para proteger adicionalmente los datos contra manipulaciones, se crea otro valor H3 de huella digital sobre el contenido de todas las celdas de una fila, que también tiene en cuenta el valor H1 de huella digital de la contraseña de una fila. Las modificaciones de los datos por medio de un editor de texto sencillo u otro programa de PC, sin embargo, también mediante modificaciones causadas por errores de lectura/escritura, se pueden reconocer, de esta manera, por el control al leerse y confirmarse con un mensaje de error. La creación y el almacenamiento de otro valor H3 de huella digital de este tipo, es también ventajoso para filas desprotegidas, sin embargo, ni conduce a la visualización de comodines P ni se protege cada una de las filas con ello. Este otro valor H3 de huella digital puede archivarse junto con el valor H1 de huella digital almacenado en la columna S de seguridad, o en una columna separada.

Dado que todas las filas se diferencian al menos por su número de fila almacenado en la columna Z de número de fila, tampoco es posible copiar una fila junto con contraseña e insertarla en otro lugar, dado que el valor de huella digital de esta fila copiada ya no coincide con el nuevo número de fila.

La Figura 2 muestra un diagrama de flujo para la modificación de datos a1-h4 almacenados en una tabla T de un control numérico. A continuación, se explican los pasos individuales.

Paso 1:
En el paso 1 se selecciona una fila N de la tabla T para el procesamiento. Procesamiento significa que los datos e1, e2, e3, e4 de esa fila se introducen nuevos o se modifican, o que se configura o se anula la protección por contraseña de la fila. En este paso, en primer lugar, todas las entradas deseadas se realizan por el operador, que en los siguientes pasos se procesan adecuadamente por el control. A ello, pertenece también la introducción de una contraseña en la celda X actual de la celda seleccionada. Esta contraseña no se registra, en este caso, en la tabla T, sino que se almacena de manera intermedia para el procesamiento adicional.

Paso E1 ramificado:
En el subsiguiente paso E1 ramificado, el control comprueba si para esa fila ya hay una contraseña establecida, por lo tanto, si en la celda X actual de la columna S de seguridad para esa fila N está contenido un valor H1 de huella digital almacenado de una contraseña introducida en el pasado. Si este no es el caso, el procedimiento se ramifica al paso E2 ramificado, en otro caso al paso 3.

Paso E2 ramificado:
En el paso E2 ramificado, el control comprueba si en el paso 1 se registró una nueva contraseña en la columna S de seguridad para la fila N. Si este es el caso, el procedimiento se ramifica al paso 5, en otro caso al paso 2.

Paso 2:
En el paso 2 se asumen todas las modificaciones en los datos e1, e2, e3, e4 y, dado el caso, en el valor H1 de huella digital almacenado.

Paso 5:
En el paso 5 se calcula un nuevo valor H2 de huella digital de la contraseña introducida en el paso 1 y se almacena en la celda X actual de la columna S de seguridad en la fila N procesada. El nuevo valor H2 de huella digital se convierte, con ello, en el valor H1 de huella digital almacenado y, de ahora en adelante, la fila N seleccionada está protegida. La contraseña introducida en el paso 1 se descarta. Después sigue el paso 2.

Paso 3:
En el paso 3 se calcula un nuevo valor H2 de huella digital de la contraseña introducida en el paso 1 y, entonces, el procedimiento continúa con el paso E3 ramificado. En el cálculo no se tiene en cuenta un símbolo eventualmente antepuesto, prohibido para el comienzo de una contraseña.

Paso E3 ramificado:
En el paso E3 ramificado se comprueba si el nuevo valor H2 de huella digital de la contraseña introducida en el paso 1 coincide con el valor H1 de huella digital almacenado para esa fila. Si este no es el caso, se ramifica al paso 4. En caso de que los valores H1, H2 de huella digital coincidan, se ramifica al paso 6.

Paso 4:
En el paso 4 se descartan todas las entradas y modificación en la fila N, dado que no se introdujo una contraseña correcta.

Paso 6:
En el paso 6 todavía se comprueba si se encontraba el símbolo prohibido para una contraseña al comienzo de la contraseña introducida en el paso 1 y, en caso de que sea verdad, se borra el valor H1 de huella digital de la contraseña almacenado para la fila N. El procedimiento continúa, entonces, con el paso 2.

En el caso más sencillo, por lo tanto, para la modificación de una fila no protegida, en el paso 1 se selecciona esa fila y, p. ej., se sobrescribe la fecha e3 de configuración, sin introducir en este caso una contraseña. A través de los pasos E1 y E2 ramificados se pasa entonces al paso 2, la fecha modificada se almacena en la tabla T.

Si, en este caso, se introdujo una nueva contraseña en la columna S de seguridad, se ramifica a través de E1 y E2 todavía antes al paso 5. Con la introducción del nuevo valor H2 de huella digital de la nueva contraseña en la columna S de seguridad, de ahora en adelante, la fila N procesada está protegida, el nuevo valor H2 de huella digital se convierte en el valor H1 de huella digital almacenado.

Al procesar una fila N ya protegida, se debe introducir la contraseña correcta, cuyo nuevo valor H2 de huella digital calculado en el paso 3 se compara con el valor H1 de huella digital ya almacenado. Si coinciden los dos valores H1, H2 de huella digital, se llega finalmente al paso 2, en el que se asumen todas las modificaciones. Si no coinciden los valores H1, H2 de huella digital, se descartan las modificaciones en el paso 4.

El procedimiento aquí descrito para la protección de datos está implementado de tal manera que todas las informaciones necesarias están archivadas en la propia tabla T a ser protegida. La protección está contenida, p. ej., en copias de seguridad de la tabla T y son efectivas de inmediato tras una restauración de esa copia de seguridad. No es necesaria una administración costosa de permisos de usuario como en el estado de la técnica.

El valor de huella digital de la contraseña o del contenido de la fila se puede calcular con cualquier procedimiento, que ofrezca suficiente seguridad contra el descubrimiento de la contraseña mediante prueba o cálculo. Ejemplos para procedimientos conocidos para la creación de valores de huella digital de este tipo son CRC, MD5 o SHA.

REIVINDICACIONES

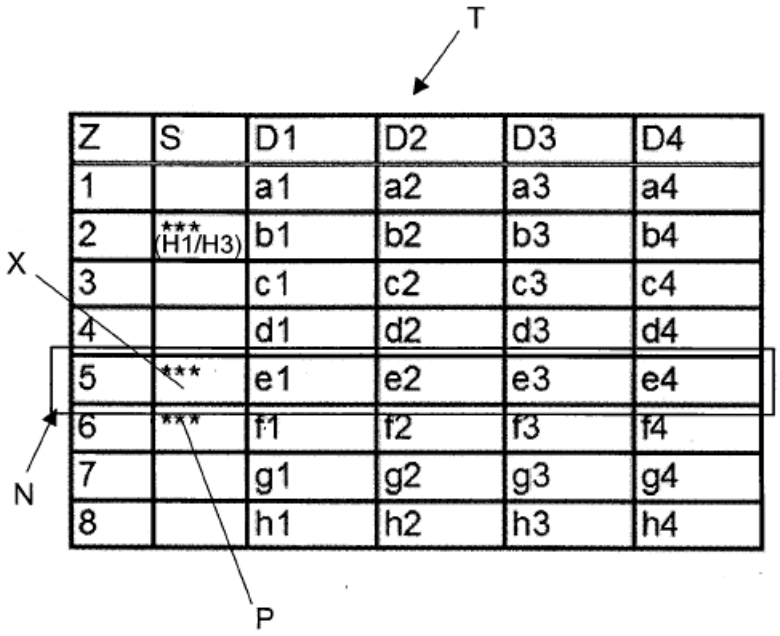
1. Procedimiento para la protección de datos (a1-h4) almacenados en una tabla (T) de un control numérico para máquinas herramienta contra modificaciones no autorizadas o accidentales, de acuerdo con el que en una columna (S) de seguridad de la tabla (T) está archivada una información sobre la protección de los datos (a1-h4) contenidos en una fila (N) seleccionada, con los siguientes pasos:

- primera introducción de una contraseña en una celda (X) actual de la columna (S) de seguridad que se encuentra en la fila (N) seleccionada,
- cálculo de un nuevo valor (H2) de huella digital de la contraseña y almacenamiento de ese valor de huella digital en la celda (X) actual como valor (H1) de huella digital almacenado,
en donde, en caso de un nuevo acceso de escritura a una fila (N) seleccionada así protegida
- se introduce la contraseña de nuevo en la celda (X) actual de la columna (S) de seguridad y se calcula el nuevo valor (H2) de huella digital de la contraseña introducida de nuevo
- y se compara con el valor (H1) de huella digital almacenado en la celda (X) actual de la columna (S) de seguridad,
en donde, solo se libera el acceso de escritura a la fila (N) seleccionada cuando el nuevo valor (H2) de huella digital coincide con el valor (H1) de huella digital almacenado y, en donde, después de cada modificación en la fila (N) seleccionada se crea otro valor (H3) de huella digital y se archiva en la fila (N) seleccionada, en donde este otro valor (H3) de huella digital se crea también sobre el valor (H1) de huella digital almacenado en la fila (N) seleccionada y, en donde, al leer una tabla (T) se crea de nuevo el otro valor (H3) de huella digital para cada una de las filas y se compara con el otro valor (H3) de huella digital almacenado por última vez, para, mediante diferentes otros valores (H3) de huella digital, reconocer modificaciones en la respectiva fila.

2. Procedimiento según la reivindicación 1, de acuerdo con el que se borra el valor (H1) de huella digital almacenado de la fila (N) seleccionada, cuando a una contraseña introducida en la celda (X) actual de la columna (S) de seguridad, se le antepuso un símbolo prohibido para el comienzo de una contraseña, que no se tiene en cuenta al calcular el nuevo valor (H2) de huella digital y cuando el nuevo valor (H2) de huella digital coincide con el valor (H1) de huella digital almacenado.

3. Procedimiento según una de las reivindicaciones anteriores, **caracterizado por que** la interfaz de usuario del control numérico visualiza la tabla (T) de tal manera que el valor (H1) de huella digital se representa con comodines (P).

Fig. 1



Z	S	D1	D2	D3	D4
1		a1	a2	a3	a4
2	*** (H1/H3)	b1	b2	b3	b4
3		c1	c2	c3	c4
4		d1	d2	d3	d4
5	***	e1	e2	e3	e4
6	***	f1	f2	f3	f4
7		g1	g2	g3	g4
8		h1	h2	h3	h4

Fig. 2